Accurate reachability analysis of uncertain nonlinear systems

Matthias Rungger
Hybrid Control Systems Group
Technical University of Munich
matthias.rungger@tum.de

Majid Zamani
Hybrid Control Systems Group
Technical University of Munich
zamani@tum.de

ABSTRACT

We propose an algorithm to over-approximate the reachable set of nonlinear systems with bounded, time-varying parameters and uncertain initial conditions. The algorithm is based on the conservative representation of the nonlinear dynamics by a differential inclusion consisting of a linear term and the Minkowsky sum of two convex sets. The linear term and one of the two sets are obtained by a conservative first-order over-approximation of the nonlinear dynamics with respect to the system state. The second set accounts for the effect of the time-varying parameters. A distinctive feature of the novel algorithm is the possibility to over-approximate the reachable set to any desired accuracy by appropriately choosing the parameters in the computation. We provide an example that illustrates the effectiveness of our approach.

KEYWORDS

Reachability analysis, nonlinear systems, time-varying parameters, differential inclusions, attainable set computation, convergence

ACM Reference Format:
Matthias Rungger and Majid Zamani. 2018. Accurate reachability analysis of uncertain nonlinear systems. In *HSCC '18: 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week), April 11–13, 2018, Porto, Portugal.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3178126.3178127

1 INTRODUCTION

Reachable sets are an integral part in the analysis and design of dynamical systems. Reachable sets are used in branch-and-bound frameworks to solve nonlinear optimal control problems in the construction of convex underestimators and concave overestimators, see e.g. [35, 49]. In robust model predictive control, reachable sets are useful to guarantee the recursive feasibility of the online optimization [29] or are embedded in the online optimization to guarantee constraint satisfaction under all possible disturbances [34]. Reachable sets are essential in state estimation and fault detection, see e.g. [48]. Moreover, rigorous enclosures of reachable sets are instrumental in the verification of safety properties involving nonlinear and hybrid control systems [27]. In addition, in the symbolic approach to synthesize provably correct controllers, reachable sets are employed in the construction of symbolic models [42, 54].

In general, reachable sets are infinite objects which are not computable [28], and usually over-approximations of reachable sets are employed in the respective application at hand. In this paper, we are interested in the accurate over-approximation of reachable sets of nonlinear dynamical systems with time-varying inputs, given by a parameterized differential equation of the form

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

where $\xi(t) \in \mathbb{R}^n$ is the state signal and $\omega(t) \in W \subseteq \mathbb{R}^m$ is the time-varying, bounded input signal. The differential equation (1) represents one of the most fundamental system models in control theory [50], and the time-varying inputs are often used to incorporate model uncertainties and disturbances [22].

The extensive need of reachable sets in the analysis and design of dynamical systems, paired with the inherent computational complexity of the approximation of reachable sets, resulted in a plethora of different algorithmic approaches exploiting different mathematical principles, various system properties and set representations. State space discretization based methods to approximate reachable sets associated with (1) are presented in [41] and [36], where [41] uses direct discretization methods, while in [36] the reachable set is obtained indirectly as sublevel set of the solution of a partial differential equation. Similarly, state space discretization methods are used to compute related objects such as the viability kernel [16] and the capture basin in minimum time problems [14]. Algorithms based on differential inequalities and comparison principles [53] to compute rigorous interval, polyhedral and ellipsoidal enclosures of reachable sets are developed in [47], [26], respectively, [52]. Logarithmic norms and component-wise, one-sided Lipschitz conditions are used in [30, 45], while the algorithms in [4] and [1] use a conservative linear, respectively, polynomial approximation of the right-hand-side of (1). Polynomial approximations in combination with interval remainders, so-called Taylor models [12], to over-approximate reachable sets of nonlinear systems with time-varying inputs are developed and analyzed in [55]. Also, in principle, the algorithms to compute validated solutions of initial value problems based on interval arithmetic and a Taylor series expansion of the flow function as discussed in [38] can be used to over-approximate reachable sets of (1), by modeling the system as an autonomous system (without inputs) with interval parameters. However, as those algorithms are not specifically designed to account for time-varying inputs, the performance of those approaches is expected to degenerate rapidly as the diameter of the bounded set of uncertainties W grows, e.g. see Section 7. Many of the mentioned approaches are available in modern, state-of-the-art open source software tools. Taylor models are implemented in `flow`*

HSCC '18, April 11–13, 2018, Porto, Portugal

ACM ISBN 978-1-4503-5642-8/18/04…$15.00
https://doi.org/10.1145/3178126.3178127

[17] and `Ariadne` [18]. The algorithms developed in [4] and [1] are provided as a MATLAB toolbox in `CORA` [2]. The algorithms to compute validated solutions of initial value problems as discussed in [38] are provided in `VNODE-LP` [37] and the algorithm in [30] is available in the software tool `CAPD` [15].

Another class of algorithms to approximate reachable sets of dynamical systems of the form (1) results from the numerical approximation of the set of solutions of nonlinear differential inclusions [21, 39, 51]. In this context, under rather mild assumptions, the system (1) is equivalently (see [33, Thm. 6.1]) interpreted as differential inclusion

$$\dot{\xi}(t) \in f(\xi(t), W) \tag{2}$$

and an approximation of the reachable set is obtained by numerically solving an initial value problem associated with (2). Those approaches originate from methods for the numerical solution of initial value problems associated with ordinary differential equations, and in contrast to the previously mentioned work, which concentrates on rigorous enclosures, the focus here is on the convergence of the computed approximation to the true set of solutions or reachable set. In a recent work [8], an optimization based approach has been proposed to overcome a well-known problem of the numerical approximation schemes [31, 43], namely that the convergence rates are of the form $O(h + \gamma/h)$ rendering highly accurate approximations computationally expensive. In this case, the space discretization parameter γ has to decrease quadratically with respect to the step size h in order to obtain linear convergence in h, see [13].

In this paper, we follow the *conservative approximation* methods in [4–6, 9, 19, 20] and propose a scheme in which we iteratively approximate the nonlinear dynamics (1) by a simpler differential inclusion. The repeated conservative approximation of the nonlinear dynamics by simpler systems to facilitate the approximation of reachable sets is also known as *hybridization.* Conservative approximations and hybridization methods have a rich history in the context of the verification of safety properties of hybrid dynamical systems and by now date back almost twenty years; see e.g. [27] for an early reference and [9] for a recent in-depth discussion of hybridization schemes. In this work, we propose a novel extension of the hybridization methods that have been developed for autonomous nonlinear systems [5, 6, 9, 19, 20] to nonlinear systems with time-varying inputs of the form (1). As in [4–6, 9, 19, 20, 25] the simpler, conservative approximation is given by a differential inclusion, which consists of a linear term and the Minkowsky sum of two convex sets. The linear term and one of the two sets are obtained by a conservative first-order over-approximation of the nonlinear dynamics with respect to the system state around a linearization point x. The second set is obtained by approximating the set $f(x, W)$ (with accuracy $\gamma > 0$). It accounts for the effect of the time-varying parameters. A distinctive feature of our method, compared to the alternative schemes in [1, 4], is the ability to approximate reachable sets to *any desired accuracy* – a property that the methods in [1, 4] are lacking. We illustrate this fact with the help of small examples in Section 4.

In summary, the *main contribution* of this work is an algorithm, to be presented in Section 5, to over-approximate reachable sets of nonlinear systems with time-varying inputs and uncertain initial states, together with the proof of its correctness (Theorem 6.1) and convergence (Theorem 6.3) in Section 6. It represents a novel extension of the hybridization methods developed for autonomous systems [5, 6, 9, 19, 20, 25] to systems with time-varying inputs. Compared to the schemes in [1, 4] it is guaranteed to converge under suitable assumptions. Compared to other non-hybridization based algorithms that compute rigorous enclosures *and* are guaranteed to converge in the context of nonlinear systems with time-varying inputs or nonlinear differential inclusions, our approach is not based on a computational demanding uniform discretization of the state space [41], nor is our approach limited to additive disturbances [45] or input affine systems [55].

As it is seen in Theorem 6.3, similar to the numerical approximation schemes in [31, 43], the accuracy γ of the approximation of the set $f(x, W)$ needs to decrease quadratically with the step size h in order to obtain linear convergence of the approximation error in h. However, contrary to [31, 43], the approximation of $f(x, W)$ in our approach is not necessarily based on a discretization of the state space. In the numerical example in Section 7, we use the support function representation of $f(x, W)$ for the approximation and the effect of the slow convergence in γ on the computational complexity in such a setting is a subject of current research.

2 NOTATION AND PRELIMINARIES

We denote by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$ the set of natural, integer and real numbers, respectively. For $n \in \mathbb{N}$, we use $\mathbb{R}^n$ and $\mathbb{R}^{n\times n}$ to denote the n-dimensional Euclidean vector space, respectively, the vector space of real matrices with n rows and n columns. We annotate those symbols with subscripts to restrict those sets in the obvious way, e.g. $\mathbb{Z}_{\geq 1}$ denotes the natural numbers.

The closed, open and half-open intervals in $\mathbb{R}$ with end points a and b are denoted by $[a, b]$, $]a, b[$, $[a, b[$, and $]a, b]$, respectively. The corresponding intervals in $\mathbb{Z}$ are denoted by $[a; b]$, $]a; b[$, $[a; b[$, and $]a; b]$. We extend the notation to hyper-intervals in $\mathbb{R}^n$, e.g., $[a, b]$ with $a, b \in \mathbb{R}^n$ denotes the set $[a_1, b_1] \times \ldots \times [a_n, b_n]$.

We use $|a|$ and $\|\cdot\|$ to denote the absolute value of $a \in \mathbb{R}$, respectively, the infinity norm of vectors in $\mathbb{R}^n$. We define $\mathbb{B}$ as the closed unit ball in $\mathbb{R}^n$ with respect to $\|\cdot\|$.

Given two sets $P, Q \subseteq \mathbb{R}^n$, we define the Minkowski set addition by $Q + P = \{y \in \mathbb{R}^n \mid \exists_{q\in Q}, \exists_{p\in P}\ y = q + p\}$. For $x \in \mathbb{R}^n$, we slightly abuse notation and use $x + W$ instead of $\{x\} + W$. For $\lambda \in \mathbb{R}_{>0}$, we define $\lambda P = \{\lambda x \in \mathbb{R}^n \mid x \in P\}$.

The Hausdorff distance between two sets $P, Q \subseteq \mathbb{R}^n$ is defined by $H(P, Q) = \inf\{\eta \in \mathbb{R}_{\geq 0} \mid Q \subseteq P + \eta\mathbb{B} \wedge P \subseteq Q + \eta\mathbb{B}\}$. The diameter of a set $Q \subseteq \mathbb{R}^n$ is defined to $\operatorname{diam} Q = \sup\{\|x - y\| \mid x, y \in Q\}$. The set $\operatorname{con} Q$ denotes the convex hull of Q see e.g. [44, Thm. 2.27, Ch. 2.E]. A set Q is convex iff $Q = \operatorname{con} Q$.

We use $f : X \rightrightarrows Y$ to denote set-valued maps from X into Y, whereas $f : X \to Y$ denotes an ordinary map; see [44].

For $f : \mathbb{R}^n \to \mathbb{R}$, we use $d_i f$ with $i \in [1; n]$ to denote the *partial derivative* (of order 1) of f with respect to the ith coordinate and extend this to *partial derivatives of order* $j \in \mathbb{Z}_{\geq 2}$ with $i_1, \ldots, i_j \in [1; n]$ recursively by $d_{i_1\ldots i_j} f = d_{i_1}(d_{i_2,\ldots,i_j} f)$. We use $D^j f(x)$ to denote the function from $(\mathbb{R}^n)^j$ to $\mathbb{R}$ given by

$$D^j f(x)(y_1, \dots, y_j) = \sum_{i_1=1}^{n} \dots \sum_{i_j=1}^{n} d_{i_1 \dots i_j} f(x) y_{1,i_1} \cdots y_{j,i_j}$$

where y_{k,i_k} denotes the i_kth entry of $y_k \in \mathbb{R}^n$. We use $D^j f(x)(y)^j$ as short-hand for $D^j f(x)(y_1, \dots, y_j)$ if $y = y_1 = \dots = y_j$. The notation extends naturally to vector-valued function $f : \mathbb{R}^n \to \mathbb{R}^m$, by applying the operation to each component. If the domain of a function f is explicitly partitioned in several subdomains, i.e., $f : \mathbb{R}^{n_1} \times \cdots \times \mathbb{R}^{n_k} \to \mathbb{R}^m$, we use $D_i^j f(x_1, \dots, x_k)$ to denote the function $D^j h(z)$ where $h(z) = f(x_1, \dots, x_{i-1}, z, x_{i+1}, \dots, x_k)$.

3 PROBLEM DESCRIPTION

We introduce the notions of reachable set and reachable tube in terms of a general differential inclusion of the form

$$\dot{\xi}(t) \in F(\xi(t)) \qquad (3)$$

with $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$. It allows us to describe uncertain nonlinear systems of the form (1) as well as other differential inclusions that we use as helper systems in the computation of the reachable set. Throughout the paper we work with differential inclusions, whose right-hand-side is continuous ([44, Def. 5.4, Ch. 5.B]) and $F(x)$ is compact and convex for all $x \in \mathbb{R}^n$.

Given an interval $I \subseteq \mathbb{R}$, we define a *solution* of (3) on I as absolutely continuous function $\xi : I \to \mathbb{R}^n$ that satisfies (3) for almost all $t \in I$. The *set of solutions* ξ on $[0, t]$ with $\xi(0) = x$ is denoted by $S_t(x)$, see e.g. [7].

The *reachable set* of (3) from $\Omega \subseteq \mathbb{R}^n$ at $t \in \mathbb{R}_{\geq 0}$ is given by

$$\psi(t, \Omega) = \{\xi(t) \in \mathbb{R}^n \mid \xi \in S_t(\Omega)\}. \qquad (4)$$

The *reachable tube* of (3) from $\Omega \subseteq \mathbb{R}^n$ at $t \in \mathbb{R}_{\geq 0}$ is given by $\psi([0, t], \Omega)$.

In this work, we propose an algorithm to over-approximate the reachable tube $\psi([0, T], \Omega)$ as well as the reachable set $\psi(T, \Omega)$ for $T \in \mathbb{R}_{\geq 0}$ and $\Omega \subseteq \mathbb{R}^n$, with Ω being compact, of the differential inclusion resulting from the nonlinear system with time-varying inputs given in (2), i.e., the right-hand-side is given by $F(x) = f(x, W)$. The algorithm follows the usual hybridization schemes [4–6, 9, 19, 20, 25]. It is based on the linearization of the right-hand-side and we use the following assumptions to ensure that the algorithm is applicable to compute an over-approximation of the reachable set/tube.

Assumption 1. *The function f is given by $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ and the set $W \subseteq \mathbb{R}^m$ is nonempty and compact. For all $x \in \mathbb{R}^n$ the set $f(x, W)$ is compact and convex. For all $w \in W$, the partial derivatives up to order two of $f(\cdot, w)$ exist and are continuous, i.e., for all $i, j, k, \in [1; n]$, the functions $d_i f_k : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ and $d_i d_j f_k : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ are continuous.*

Note that Assumption 1 guarantees for every $x \in \mathbb{R}^n$ the existence of at least one solution of (2) on some interval from x, see e.g. [7]. Nevertheless, it is not guaranteed that such a solution exist on a-priori given interval $[0, T]$, since a solution of (2) can blow up in finite time smaller than T. In this case the reachable tube of (2) from $\{x\}$ at T is unbounded and the algorithm that we propose in this paper does not terminate.

4 MOTIVATING EXAMPLES

We show that the methods in [1, 4], in general are unable to produce precise approximations of reachable sets for nonlinear systems with time-varying inputs.

A natural approach to increase the accuracy of hybridization schemes is to decrease the domains on which the complex dynamics are approximated. For autonomous systems this is actually effective, see e.g. [5, Thm. 1], [6, Thm. 2]. When applied to systems with inputs, this would require to partition the input set W into smaller sets W_i, $i \in [1; p]$ and compute reachable sets with respect to the partition elements W_i. Example 1 demonstrates that this is not a viable approach.

Example 1. *Consider a system of the form (2) with $f : \mathbb{R}^3 \to \mathbb{R}^2$ given by*

$$f(x, w) = (1, x_1 w) \qquad \textit{and} \qquad W = [-1, 1]. \qquad (5)$$

A quick analysis of the dynamics shows that trajectories ξ of (5) with initial state $(-1, 0)$ are given by

$$\xi_1(t) = -1 + t \qquad \textit{and} \qquad \xi_2(t) = \int_0^t (-1 + s)\omega(s)\mathrm{d}s. \qquad (6)$$

Consider the input signals ω_1 and ω_2 defined on $[0, 2]$ and given by

$$\omega_1(t) = -\omega_2(t) = \begin{cases} 1 & \textit{if } t \leq 1 \\ -1 & \textit{if } t > 1. \end{cases}$$

An evaluation of (6) shows that the states reached by (5) from $x = (-1, 0)$ at time $t = 2$ associated with ω_1 and ω_2 are given by $(1, -1)$ and $(1, 1)$, respectively. Moreover, those states enclose all other reachable states, so that the reachable set from $\Omega = \{(-1, 0)\}$ at time $t = 2$ is given by

$$\psi(2, \Omega) = \{1\} \times [-1, 1]. \qquad (7)$$

Let us use the smaller sets $W_1 = [-1, 0]$ and $W_2 = [0, 1]$ to cover W. Subsequently, we denote the reachable set of (5) with W_i, $i \in [1; 2]$ in place of W by ψ_i. We apply the same analysis as before and obtain

$$\psi_1(1, \Omega) = \psi_2(1, \Omega) = \{1\} \times [-1/2, 1/2].$$

It is straightforward to see that those sets are not useful in over-approximating $\psi(1, \Omega)$ since

$$\psi(1, \Omega) \nsubseteq \psi_1(1, \Omega) \cup \psi_2(1, \Omega).$$

We use the next example to illustrate the consequences of this observation.

Example 2. *Consider a system of the form (1) with*

$$f(x, w) = \frac{1}{1 + w^2} \qquad \textit{and} \qquad W = [-1, 1]. \qquad (8)$$

We determine the reachable set from $\Omega = \{0\}$ at time $t = 1$ by inspection to

$$\psi(1, \{0\}) = \left[\tfrac{1}{2}, 1\right]. \qquad (9)$$

Following the algorithm in [4], we use the differential inclusion

$$\dot{\xi}(t) \in a(\xi(t) - \bar{x}) + f(\bar{x}, \bar{w}) + b(\{-\bar{w}\} + W) + [-e, e] \qquad (10)$$

as an approximation of (8) around the linearization point $\bar{x}$ and $\bar{w}$. The scalars a and b are obtained by evaluating the partial derivatives of the dynamics at $\bar{x}$ and $\bar{w}$. Subsequently, we fix $\bar{x} = 0$, $\bar{w} = 0$ and obtain

$$a = 0 \qquad \textit{and} \qquad b = -\frac{2\bar{w}}{(1 + \bar{w}^2)^2} = 0.$$

The interval $[-e, e]$ *accounts for the linearization error and is determined by bounding the Lagrange remainder of the dynamics maximized over the Cartesian product of the convex hull of the reachable tube* $\operatorname{con}\psi([0,1],\{0\}) = [0,1]$ *and* $W = [-1,1]$*. This results to*

$$\begin{aligned} e &= \max_{x,z\in[0,1]} \max_{w,v\in W} \tfrac{1}{2}|D^2 f(z,v)((x-\bar{x}, w-\bar{w}))^2| \\ &= \max_{w,v\in[-1,1]} |\frac{3v^2-1}{(1+v^2)^3}|(w-\bar{w})^2 = 1. \end{aligned} \tag{11}$$

With $f(\bar{x},\bar{w}) = 1$*, we obtain the differential inclusion*

$$\dot{\xi}(t) \in 1 + [-1,1]$$

whose reachable set $\psi(1,\{0\}) = [0,2]$ *indeed over-approximates the reachable set* $[1/2, 1]$ *of* (8)*. However, the accuracy of the approximation is rather coarse, e.g. the Hausdorff distance of the two reachable sets is given by* $H(\psi(1,\{0\}),\psi(1,\{0\})) = 1$*, which is actually larger than the diameter of the reachable set itself. In order to increase the accuracy, we need to decrease the error e in* (11)*. The only possibility to decrease e is to make W smaller, which – as illustrated in Example 1 – is not allowed. Therefore, we cannot increase the accuracy of the approximation obtained on the basis of* (10).

We would like to emphasize that the claims in Example 2 are actually independent of the particular choice of discretization points $\bar{x}$ and $\bar{u}$ and a high-order approximation of (8) as proposed in [1] which is also not addressing the problem, since for this example the Lagrange remainder $\max_{w,v\in W} \frac{1}{n!} D^n f(v)(w-\bar{w})^n$ diverges for $n \longrightarrow \infty$.

We address the problem illustrated in Example 2 by conservatively approximating the effect of the nonlinear inputs at the linearization point $f(\bar{x},\bar{w})$ by a *direct* approximation of the set $f(\bar{x}, W)$, which does not rely on the derivative of f with respect to the second argument.

5 REACHABLE SET & TUBE COMPUTATION

We introduce the algorithm to over-approximate the reachable set and the reachable tube of (2) for a given time horizon $T \in \mathbb{R}_{\geq 0}$ and a convex and compact set of initial states $\Omega \subseteq \mathbb{R}^n$. We follow closely the approach in [4, 25], which according to the classification in [9], is a time-triggered dynamic hybridization algorithm. However, our novel extension can easily be adapted to other types of hybridization methods such as state-triggered and static methods as well as variants thereof.

The algorithm invokes several high-level commands. Rather than providing a detailed explanation of those commands, we refer the interested reader to further literature. Nevertheless, for the analysis of the algorithm in Section 6, we impose several assumptions on the high-level commands, which we label with equation numbers. The assumptions with labels ending in "a" are used to ensure the correctness of the algorithm, while we use the assumptions ending in "a" as well as "b" to ensure the convergence of the algorithm. We compactly summarize the imposed assumptions in the respective theorems.

We assume that we can over-approximate (to any desired accuracy) the reachable set and the reachable tube of linear differential inclusions of the form

$$\dot{\xi}(t) \in A\xi(t) + V \tag{12}$$

where A is an $n \times n$ matrix with entries in $\mathbb{R}$ and V is a non-empty, compact and convex subset of $\mathbb{R}^n$. Such an algorithm is for example described in [32] and implemented in the tool SpaceEx [23] for the case that Ω and V are given in terms of their support functions. Subsequently, we use

$$\begin{aligned} \Omega_h &= \mathtt{ReachSetLin}_\gamma(A, V, \Omega, h) \\ \Omega_{[0,h]} &= \mathtt{ReachTubeLin}_\gamma(A, V, \Omega, h) \end{aligned} \tag{13}$$

to refer to the algorithms that compute an over-approximation of the reachable set $\chi(h,\Omega)$, respectively, the reachable tube $\chi([0,h],\Omega)$ of (12) from $\Omega \subseteq \mathbb{R}^n$ at time $h \in \mathbb{R}_{\geq 0}$. We assume that our implementation of (13) is an over-approximation with compact sets, i.e.,

$$\Omega_h, \Omega_{[0,h]} \in \mathbb{K}(\mathbb{R}^n), \quad \chi(h,\Omega) \subseteq \Omega_h \text{ and } \chi([0,h],\Omega) \subseteq \Omega_{[0,h]}, \tag{14a}$$

where $\mathbb{K}(\mathbb{R}^n)$ denotes the set of compact subsets of $\mathbb{R}^n$. Moreover, for any $\bar{K} \in \mathbb{K}(\mathbb{R}^n)$ and $\gamma \in \mathbb{R}_{>0}$, we can parameterize the implementation, such that for every $\Omega \in \mathbb{K}(\mathbb{R}^n)$ with $\Omega \subseteq \bar{K}$, we have

$$\Omega_h \subseteq \chi(h,\Omega) + \gamma\mathbb{B} \text{ and } \Omega_{[0,h]} \subseteq \chi([0,h],\Omega) + \gamma\mathbb{B}. \tag{14b}$$

Additionally, we assume the availability of an algorithm to over-approximate (to any desired accuracy) for every $x \in \mathbb{R}^n$ the convex and compact set $f(x, W)$. We use $\mathtt{Approx}_\gamma$ to denote this operation and assume

$$f(x,W) \subseteq \mathtt{Approx}_\gamma(f(x,W)) \tag{15a}$$

$$\mathtt{Approx}_\gamma(f(x,W)) \subseteq f(x,W) + \gamma\mathbb{B}. \tag{15b}$$

As before, we use the parameter γ to denote the accuracy of the approximation. If we know the support function of $f(x,W)$, we can use the approximation theory in [40] to establish such a property of an algorithm implementing $\mathtt{Approx}_\gamma$.

For the approximation of the reachable set and the reachable tube of (2), the time horizon T is divided in $N \in \mathbb{N}$ congruent subintervals and the computation is carried out iteratively for each interval $h[i-1;i]$ with $h = T/N$, $i \in [1;N]$ separately. As in the case of the numerical solution of initial value problems, the rational behind such an approach is the fact that the reachable set satisfies

$$\psi(2h,\Omega) = \psi(h,\psi(h,\Omega))$$

so that the reachable set over a longer horizon can be obtained by the iterative approximation of the reachable set for shorter horizons. For the presented approach, for each subinterval $h[i-1,i]$, a conservative substitute of (2) is determined by a linear differential inclusion (12) with

$$\begin{aligned} A &= D_1 f(\bar{x},\bar{w}) \\ V &= -A\bar{x} + \mathtt{Approx}_\gamma(f(\bar{x},W)) + [-e,e] \end{aligned} \tag{16}$$

where $\bar{x} \in \mathbb{R}^n$ and $\bar{w} \in W$ are the points of the linearization and the hyper-interval $[-e,e]$ with $e \in \mathbb{R}^n_{\geq 0}$ is used to account for the linearization error. For a correct implementation, we need to guarantee that our approximation is indeed an over-approximation, which we ensure by establishing the inclusion

$$\forall x \in \Omega_{[0,h]}: \quad f(x,W) \subseteq D_1 f(\bar{x},\bar{w})(x-\bar{x}) + f(\bar{x},W) + [-e,e]. \tag{17}$$

In the implementation, we verify this inclusion by computing an upper bound of the change in the first-order derivate of $f(\cdot, w)$

with respect to $w \in W$ and the second-order remainder of the Taylor expansion of $f(\cdot, \bar{w})$. To this end, we introduce the function $E : \mathbb{K}(\mathbb{R}^n) \times \mathbb{R}^n \times W \to \mathbb{R}^n_{\geq 0}$, which for $i \in [1; n]$, is given by

$$\begin{aligned} &E_i(K, \bar{x}, \bar{w}) = \\ &\max_{z,x \in \mathrm{con}(K \cup \{\bar{x}\}), w \in W} \big(|(D_1 f_i(\bar{x}, w) - D_1 f_i(\bar{x}, \bar{w}))(x - \bar{x})| \\ &\qquad + \tfrac{1}{2}|D_1^2 f_i(z, w)(x - \bar{x})^2|\big). \end{aligned} \tag{18}$$

We use Assumption 1 to ensure that E is well defined, in the sense that for each component E_i, the maximum in (18) exists and is in $\mathbb{R}_{\geq 0}$. Indeed, Assumption 1 ensures that the objective function is continuous and the optimization domain $\bar{K} \times \bar{K} \times W$ with $\bar{K} = \mathrm{con}(K \cup \{\bar{x}\})$ is compact.

We show in Lemma 6.2 that if the a-priori error estimate e is greater than or equal to $\hat{e} = E(\Omega_{[0,h]}, \bar{x}, \bar{w})$, i.e., $e \geq \hat{e}$ (by components), then the inclusion (17) holds. We use ComputeError to denote the algorithm that computes the error and assume

$$\mathtt{ComputeError}(\Omega_{[0,h]}, \bar{x}, \bar{w}) \geq E(\Omega_{[0,h]}, \bar{x}, \bar{w}) \tag{19a}$$

holds for every call of ComputeError in the reachable set computation. Similarly to the other subroutines we assume that the error is computable to any desired precision. In particular, for every $K \in \mathbb{K}(\mathbb{R}^n)$ there exists a constant $c \in \mathbb{R}_{>0}$ so that the implementation satisfies for every $\bar{K} \in \mathbb{K}(\mathbb{R}^n)$ with $\bar{K} \subseteq K$, $\bar{x}$ and $\bar{w}$ the inequality

$$\mathtt{ComputeError}(\bar{K}, \bar{x}, \bar{w}) \leq E(\bar{K}, \bar{x}, \bar{w}) + c \operatorname{diam} \mathrm{con}(\bar{K} \cup \{\bar{x}\}). \tag{19b}$$

In our implementation, we evaluate the term in (18) with interval arithmetic over a hyper-interval that contains $\Omega_{[0,h]}$ and W. In order to satisfy (19b) it might be necessary to subdivide the set W to regulate the error due to the interval representation of W. For the sake of a simpler presentation we do not incorporate this effect in our convergence analysis.

Note that the over-approximation $\Omega_{[0,h]}$ of the reachable tube of (12) with the parameters given by (16) is available only *after* we fixed the error estimate $e \in \mathbb{R}^n_{\geq 0}$. Hence, we need to devise a strategy for the case that $e \ngeq \hat{e}$. Given that the linearization error converges to zero for $\operatorname{diam} \Omega_{[0,h]} \to 0$ (see Lemma 6.5), a natural procedure to address this issue, which is also implemented in [4], is to recompute the over-approximation of the reachable tube of (12) for a smaller set of initial states. Alternatively, or additionally, one could also decrease the time horizon h. An option that is subject to future analysis. We use

$$\{\Omega_1, \Omega_2, \ldots, \Omega_p\} = \mathtt{SubDiv}(\Omega) \tag{20}$$

to denote the operation that subdivides the set Ω in $p \in \mathbb{N}$ subsets and assume that

$$\Omega \subseteq \cup_{i \in [1;p]} \Omega_i \tag{21a}$$

to ensure the correctness of our approach. Moreover, in the convergence analysis we impose the stronger assumption of

$$\max_{i \in [1;p]} \operatorname{diam} \Omega_i \leq \rho \operatorname{diam} \Omega \quad \text{and} \quad \Omega = \cup_{i \in [1;p]} \Omega_i \tag{21b}$$

where ρ is a scalar in $[0, 1[$.

Given the operations (13), (15), (19) and (20) we are ready to state the main procedure to over-approximate the reachable set and reachable tube of (2) in Algorithm 1. It takes the time horizon $T \in \mathbb{R}_{>0}$ and a compact and convex set $\Omega \subseteq \mathbb{R}^n$ as input. The parameters of the algorithm are the number of subintervals $N \in \mathbb{N}$, the error parameter e and an input $\bar{w} \in W$, which is used in the linearization of right-hand-side of (2). After initializing the data in lines 1-2, the computation proceeds by successively iterating over the time-intervals $h[i-1, i]$ for $i \in [1; N]$ in line 3. The queue Q contains a list of sets that over-approximate the reachable set at time $t = h(i-1)$, i.e.,

$$\psi(h(i-1), \Omega_0) \subseteq \cup_{\bar{\Omega} \in Q} \bar{\Omega}.$$

Those sets are computed for each time-interval $h[i-1, i]$ by the help of a linear differential inclusion that is used as a conservative substitute of (2) in lines 9-11. The point of linearization is heuristically chosen as in [4] to

$$\bar{x} = \mathtt{center}(\bar{\Omega}) + \frac{1}{2} h f(\mathtt{center}(\Omega), \bar{w})$$

where $\mathtt{center}(\Omega) \in \Omega$ simply returns an element of Ω. Afterwards, in lines 12 and 13, the algorithms (13) are invoked to compute an over-approximation of the reachable set and the reachable tube of the linear substitute. Subsequently, the linearization error (19) is computed in line 14. If the a-priori error is sufficiently large, the sets Ω_h and $\Omega_{[0,h]}$ are indeed an over-approximation of $\psi(h, \Omega)$ and $\psi([0, h], \Omega)$, respectively. Consequently, Ω_h is added to the queue Q' and Ω_i in line 16 and 17, respectively. Simultaneously, the over-approximation of the reachable tube is updated in line 18 with $\Omega_{[0,h]}$. If the error check in line 14 fails, the currently processed

Algorithm 1 Over-approx. of $\psi(T, \Omega)$ and $\psi([0, T], \Omega)$ of (2)

```
Parameter: $N \in \mathbb{N}$, $e \in \mathbb{R}^n_{>0}$, $\bar{w} \in W$
Input: $\Omega \subseteq \mathbb{R}^n$, $T \in \mathbb{R}_{>0}$
Output: $\Omega_N$, $\Omega_{[0;N]}$
 1: $h := T/N$                                         // time-step
 2: $Q' := \{\Omega\}$                     // queue of sets to be processed
 3: for $i = 1 \ldots N$ do
 4:     $Q := Q'$                                      // update queue
 5:     $Q' := \varnothing$
 6:     $\Omega_i := \varnothing$, $\Omega_{[i-1;i]} := \varnothing$              // sets to be computed
 7:     while $Q \neq \varnothing$ do
 8:         $\bar{\Omega} := \mathtt{pop}(Q)$                  // remove set from queue
 9:         $\bar{x} := \mathtt{center}(\bar{\Omega}) + \frac{1}{2} f(\mathtt{center}(\bar{\Omega}), \bar{w})$
10:         $A := D_1 f(\bar{x}, \bar{w})$
11:         $V := -A\bar{x} + \mathtt{Approx}_\gamma(f(\bar{x}, W)) + [-e, e]$
12:         $\Omega_h := \mathtt{ReachSetLin}_\gamma(A, V, \bar{\Omega}, h)$
13:         $\Omega_{[0,h]} := \mathtt{ReachTubeLin}_\gamma(A, V, \bar{\Omega}, h)$
14:         $\hat{e} = \mathtt{ComputeError}(\Omega_{[0,h]}, \bar{x}, \bar{w})$     // determine $\hat{e}$ in (19)
15:         if $e \geq \hat{e}$ then
16:             $Q' := Q' \cup \{\Omega_h\}$           // queue for next time-interval
17:             $\Omega_i := \Omega_i \cup \Omega_h$                        // reachable set
18:             $\Omega_{[i-1;i]} := \Omega_{[i-1;i]} \cup \Omega_{[0,h]}$          // reachable tube
19:         else
20:             $Q := Q \cup \mathtt{SubDiv}(\bar{\Omega})$              // subdivide initial set
21:         end if
22:     end while
23: end for
24: return $\Omega_N$, $\Omega_{[0;N]} := \cup_{i \in [1;N]} \Omega_{[i-1;i]}$
```

set Ω is subdivided in line 20 and the computation is repeated with the smaller sets. The algorithm proceeds in this way until all sets in Q are processed and all time-intervals $h[i-1;i]$ are processed at which point it returns the sets Ω_N and $\Omega_{[0;N]}$.

6 ANALYSIS

We analyze Algorithm 1. In general, it is not ensured that Algorithm 1 terminates. Nevertheless, as we are going to show in Theorem 6.1, if it terminates then output sets Ω_N and $\Omega_{[0;N]}$ are guaranteed to over-approximate the reachable set $\psi(T,\Omega)$ and the reachable tube $\psi([0,T],\Omega)$ of (2), respectively. Moreover, under suitable assumptions, we show in Theorem 6.3 that for any desired approximation accuracy there exist parameters so that Algorithm 1 is guaranteed to terminate and the output sets Ω_N and $\Omega_{[0;N]}$ approximate the sets $\psi(T,\Omega)$, respectively, $\psi([0,T],\Omega)$ with the prescribed precision.

In the analysis, we use the map $G_e : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ which is parameterized by $e \in \mathbb{R}^n_{\geq 0}$, $\bar{x} \in \mathbb{R}^n$ and $\bar{w} \in W$ and defined as

$$G_e(x) = D_1 f(\bar{x},\bar{w})(x-\bar{x}) + f(\bar{x},W) + [-e,e]. \tag{22}$$

6.1 Correct over-approximation

We show the correctness of Algorithm 1.

Theorem 6.1. *Consider* (2) *under Assumption 1. Let $\psi(T,\Omega)$ and $\psi([0,T],\Omega)$ denote the reachable set, respectively, reachable tube of* (2) *from $\Omega \subseteq \mathbb{R}^n$ at $T \in \mathbb{R}_{\geq 0}$. Fix the parameters $N \in \mathbb{N}$, $e \in \mathbb{R}^n_{>0}$ and $\bar{w} \in W$. Suppose that the subroutines of Algorithm 1 satisfy the following:* $\texttt{ReachSetLin}_\gamma$, $\texttt{ReachTubeLin}_\gamma$ *satisfy* (13) *and* (14a)*;* $\texttt{Approx}_\gamma$ *satisfies* (15a)*;* `ComputeError` *satisfies* (19a) *and* `SubDiv` *satisfies* (20) *and* (21a)*. If Algorithm 1 terminates for the inputs Ω and T, then we have*

$$\psi(T,\Omega) \subseteq \Omega_N \quad \text{and} \quad \psi([0,T],\Omega) \subseteq \Omega_{[0;N]}. \tag{23}$$

In the proof of Theorem 6.1 we need the following lemma.

Lemma 6.2. *Consider* (2) *under Assumption 1. Let $x, \bar{x} \in \mathbb{R}^n$, $\bar{w} \in W$ and $S = \operatorname{con}\{x,\bar{x}\}$. Consider the map G_e in* (22) *for parameters e, $\bar{x}$ and $\bar{w}$. Let E be given in* (18)*. Then the following implication holds*

$$e \geq E(S,\bar{x},\bar{w}) \implies f(x,W) \subseteq G_e(x) \tag{24}$$

Proof. Let $w \in W$. By an application of Taylor's Theorem [10, Thm. 40.9], for every $i \in [1;n]$ there exists $z_i \in S$ so that

$$f_i(x,w) = f_i(\bar{x},w) + D_1 f_i(\bar{x},w)(x-\bar{x}) + \tfrac{1}{2}D_1^2 f_i(z_i,w)(x-\bar{x})^2.$$

By adding and subtracting $D_1 f_i(\bar{x},\bar{w})(x-\bar{x})$ on the right, we have

$$\begin{aligned} f_i(x,w) = f_i(\bar{x},w) &+ D_1 f_i(\bar{x},\bar{w})(x-\bar{x}) + D_1 f_i(\bar{x},w)(x-\bar{x}) \\ &- D_1 f_i(\bar{x},\bar{w})(x-\bar{x}) + \tfrac{1}{2}D_1^2 f_i(z_i,w)(x-\bar{x})^2. \end{aligned}$$

The absolute value of the last three terms on the right are bounded by $E_i(S,\bar{x},\bar{w})$ and we obtain

$$f_i(x,w) \in D_1 f_i(\bar{x},\bar{w})(x-\bar{x}) + f_i(\bar{x},w) + [-e_i,e_i].$$

Since this holds for every $i \in [1;n]$ and $w \in W$ we obtain the assertion. □

Proof of Theorem 6.1. For $i \in [1;N]$, consider the sets Ω_i, and $\Omega_{[i-1;i]}$ initialized in line 6 and updated in lines 17 and 18. For $i \in [1;N]$, let Q_{i-1} denote the set of sets $\bar{\Omega}$ that are removed from Q in line 8 throughout the while-loop and that lead to the error $\hat{e}$ (computed in line 14) that satisfies $e \geq \hat{e}$. Let us show that $\Omega_i \subseteq \cup_{\bar{\Omega}\in Q_i}\bar{\Omega}$ holds for all $i \in [0;N[$. For the sake of contradiction, assume that $x \in \Omega_i$ but there does not exist any $\bar{\Omega}$ in Q_i so that $x \in \bar{\Omega}$. In the first iteration of the while-loop, we have $\Omega_i = \cup_{\bar{\Omega}\in Q}\bar{\Omega}$ (see the lines 16 and 17), and we see that $\Omega_i \not\subseteq \cup_{\bar{\Omega}\in Q_i}\bar{\Omega}$ can only happen if an element $\bar{\Omega}$ is removed from Q so that the associated error computation in line 14 leads to $e \not\geq \hat{e}$ and the newly added sets in line 20 do not cover $\bar{\Omega}$. But his cannot happen, since $\bar{\Omega} \subseteq \cup_{\Omega' \in \texttt{SubDiv}(\bar{\Omega})}\Omega'$ holds.

For $i \in [1;N]$, let $\bar{\Omega} \in Q_{i-1}$ and consider the associated quantities $\bar{x}$, Ω_h and $\Omega_{[0,h]}$ computed in lines 9, 12 and 13, respectively. Let $x \in \Omega_{[0,h]}$ and define $S = \{\lambda x + (1-\lambda)\bar{x} \in \mathbb{R}^n \mid \lambda \in [0,1]\}$. Clearly, we have $S \subseteq \operatorname{con}(\Omega_{[0,h]} \cup \{\bar{x}\})$. From the definition of Q_{i-1} follows that $e \geq \hat{e}$ and we get $e \geq E(\Omega_{[0,h]},\bar{x},\bar{w}) \geq E(S,\bar{x},\bar{w})$, where we used $S \subseteq \operatorname{con}(\Omega_{[0,h]} \cup \{\bar{x}\})$ and (19a). We apply Lemma 6.2 and see that $f(x,W) \subseteq G_e(x)$. Since this holds for every $x \in \Omega_{[0,h]}$ we obtain (17). Since $f(x,W)$ is included in the linear inclusion (12) with A and V computed in lines 10, respectively, 11 and the primitives $\texttt{ReachSetLin}_\gamma$ and $\texttt{ReachTubeLin}_\gamma$ satisfy (14) we obtain

$$\psi(h,\bar{\Omega}) \subseteq \Omega_h \text{ and } \psi([0,h],\bar{\Omega}) \subseteq \Omega_{[0,h]}.$$

Given the computation of Ω_i and $\Omega_{[i-1;i]}$ in lines (17), respectively, (18), it is straightforward to derive

$$\begin{aligned} \psi(h,\Omega_{i-1}) &\subseteq \cup_{\bar{\Omega}\in Q_{i-1}}\psi(h,\bar{\Omega}) &&\subseteq \Omega_i \\ \psi([0,h],\Omega_{i-1}) &\subseteq \cup_{\bar{\Omega}\in Q_{i-1}}\psi([0,h],\bar{\Omega}) &&\subseteq \Omega_{[i-1;i]}. \end{aligned}$$

A repeated application of the inclusion

$$\psi(ih,\Omega) \subseteq \psi((i-1)h,\psi(h,\Omega)) \subseteq \psi((i-1)h,\Omega_1)$$

shows that $\psi(ih,\Omega) \subseteq \Omega_i$ for all $i \in [0;N]$. In particular it shows $\psi(T,\Omega) \subseteq \Omega_N$. Moreover, we derive

$$\begin{aligned} \psi([0,T],\Omega) &= \cup_{i\in[1;N]}\psi([0,h],\psi((i-1)h,\Omega)) \\ &\subseteq \cup_{i\in[1;N]}\psi([0,h],\Omega_{i-1}) \subseteq \cup_{i\in[1;N]}\Omega_{[i-1;i]} = \Omega_N \end{aligned}$$

which completes the proof. □

6.2 Convergence Analysis

For an appropriate choice of parameters, Algorithm 1 supports the approximation of reachable sets and reachable tubes of (2) to any desired precision.

Theorem 6.3. *Consider* (2) *under Assumption 1. Let $\psi(T,\Omega)$ and $\psi([0,T],\Omega)$ denote the reachable set, respectively, reachable tube of* (2) *from $\Omega \subseteq \mathbb{R}^n$ at time $T \in \mathbb{R}_{\geq 0}$. Assume the existence of a compact set K so that the following inclusion holds*

$$\psi([0,T],\Omega) \subseteq K. \tag{25}$$

Let $\delta \in \mathbb{R}_{>0}$ be desired accuracy.

Suppose that for any $\gamma \in \mathbb{R}_{>0}$ the subroutines $\texttt{ReachSetLin}_\gamma$, $\texttt{ReachTubeLin}_\gamma$ *and* $\texttt{Approx}_\gamma$ *satisfy* (13), (14) *and* (15) *for all $\Omega \in \mathbb{K}(\mathbb{R}^n)$ with $\Omega \subseteq K + 3\delta\mathbb{B}$. Suppose there exists $c \in \mathbb{R}_{>0}$ so that* `ComputeError` *satisfy* (19)*, for all $\bar{K} \in \mathbb{K}(\mathbb{R}^n)$ with $\bar{K} \subseteq K + 3\delta\mathbb{B}$, $\bar{x} \in K + 3\delta\mathbb{B}$ and $\bar{w} \in W$. Let* `SubDiv` *satisfy* (20)-(21) *with $\rho \in [0,1[$.*

Then there exists $d \in \mathbb{R}_{>0}$ so that if Algorithm 1 and its subroutines are called with parameters $N \in \mathbb{N}$, $e \in \mathbb{R}^n_{>0}$, $\bar{w} \in W$ and $\gamma \in \mathbb{R}_{>0}$ that satisfy

$$\|e\| \leq d, \quad 1/N \leq de_{i^*}, \quad \gamma \leq de_{i^*} \quad \textit{and} \quad \gamma N \leq d \tag{26}$$

for $e_{i^*} = \min_{i \in [1;n]} e_i$, then Algorithm 1 terminates and the output satisfies

$$\Omega_N \subseteq \psi(T, \Omega) + \delta\mathbb{B} \quad \textit{and} \quad \Omega_{[0;N]} \subseteq \psi([0,T], \Omega) + \delta\mathbb{B}. \tag{27}$$

In the proof of the theorem we use the following lemmas.

Lemma 6.4. *Consider* (2) *under Assumption 1. Fix a compact set $K \subseteq \mathbb{R}^n$, $\bar{x} \in \mathbb{R}^n$ and $\bar{w} \in W$. Let G_e be given in* (22) *with parameters $e \geq E(K, \bar{x}, \bar{w})$, $\bar{x}$ and $\bar{w}$, with E defined in* (18)*. Then, for all $x \in K$ we have*

$$G_e(x) \subseteq f(x, W) + 2[-e, e]. \tag{28}$$

Proof. Let G_0 be given in (22) with parameters 0, $\bar{x}$ and $\bar{w}$. We show that for all $x \in K$ we have $G_0(x) \subseteq f(x, W) + [-e, e]$.

Let $x \in K$ and pick $y \in G_0(x)$. Then there exists $w \in W$ so that

$$y = D_1 f(\bar{x}, \bar{w})(x - \bar{x}) + f(\bar{x}, w). \tag{29}$$

We continue the analysis for each component y_i with $i \in [1;n]$ in isolation. We add and subtract $D_1 f_i(\bar{x}, w)(x - \bar{x})$ to the ith component in (29) to get

$$\begin{aligned} y_i = &f_i(\bar{x}, w) + D_1 f_i(\bar{x}, w)(x - \bar{x}) + D_1 f_i(\bar{x}, \bar{w})(x - \bar{x}) \\ &- D_1 f_i(\bar{x}, w)(x - \bar{x}). \end{aligned} \tag{30}$$

Taylor’s Theorem [10, Thm. 40.9] allows us to pick $z \in \operatorname{con}(K \cup \{\bar{x}\})$ so that

$$f_i(x, w) = f_i(\bar{x}, w) + D_1 f_i(\bar{x}, w)(x - \bar{x}) + \tfrac{1}{2} D_1^2 f_i(z, w)(x - \bar{x})^2. \tag{31}$$

We add and subtract $\frac{1}{2} D_1^2 f_i(z, w)(x - \bar{x})^2$ in (30) and use (31) to get

$$y_i = f_i(x, w) + D_1(f_i(\bar{x}, \bar{w}) - f_i(\bar{x}, w))(x - \bar{x}) - \tfrac{1}{2} D_1^2 f_i(z, w)(x - \bar{x})^2.$$

The last two terms are bounded by $E_i(K, \bar{x}, \bar{w})$ so that

$$y_i \in f_i(x, w) + [-e_i, e_i].$$

Since this inclusion holds for all $i \in [1;n]$ we obtain $G_0(x) \subseteq f(x, W) + [-e, e]$ and (28) follows. □

Lemma 6.5. *Consider* (2) *under Assumption 1. Let $K \in \mathbb{K}(\mathbb{R}^n)$ and $\bar{h} \in \mathbb{R}_{>0}$, then there exists $C \in \mathbb{R}_{>0}$ so that for every $\bar{\Omega} \in \mathbb{K}(\mathbb{R}^n)$ with $\bar{\Omega} \subseteq K$, $\gamma \in \mathbb{R}_{>0}$, $\bar{w} \in W$ and $\hat{x} \in \bar{\Omega}$, the function E in* (18) *and the reachable tube $\chi([0,h], \bar{\Omega})$ of* (12) *from $\bar{\Omega}$ at $h \in [0, \bar{h}]$ with*

$$\begin{aligned} \bar{x} &= \hat{x} + \tfrac{h}{2} f(\hat{x}, \bar{w}) \\ A &= D_1 f(\bar{x}, \bar{w}) \\ V &= -A\bar{x} + f(\bar{x}, W) + \gamma\mathbb{B} \end{aligned}$$

satisfy $\|E(\chi([0,h], \bar{\Omega}) + \gamma\mathbb{B}, \bar{x}, \bar{w})\| \leq C(\operatorname{diam} \bar{\Omega} + h + \gamma)$.

In the proof of the lemma, we use the following estimate on the solution of linear differential equations. Let $\xi : [0,h] \to \mathbb{R}^n$ and $v : [0,h] \to V$ satisfy $\dot{\xi}(t) = A\xi(t) + v(t)$ for almost all $t \in [0,h]$. Then for all $t \in [0,h]$ the following inequality holds

$$\|\xi(t)\| \leq v e^{ah}(\|\xi(0)\| + h) \tag{32}$$

where $a = \|A\|$ and $v \in \mathbb{R}_{\geq 1}$ satisfies: $w \in V$ implies $\|w\| \leq v$.

Proof of Lemma 6.5. As f is continuous and K is compact, there exists $M \in \mathbb{R}_{>0}$ so that for all $x \in K$ we have $\|f(x, \bar{w})\| \leq M$. Similarly, because of the continuity of the first-order partial derivatives of $f(\cdot, \bar{w})$ there exists $a \in \mathbb{R}_{>0}$ so that for all $x \in K + \bar{h}/2M\mathbb{B}$ we have $\|D_1 f(x, \bar{w})\| \leq a$. We pick $v \in \mathbb{R}_{\geq 1}$ so that $x \in K + \bar{h}/2M\mathbb{B}$ and $w \in f(x, W) + \gamma\mathbb{B}$ implies $\|w\| \leq v$.

Let $y \in \chi([0,h], \bar{\Omega})$. From the definition of $\chi([0,h], \bar{\Omega})$ we see that there exists an absolutely continuous function $\xi : [0,t] \to \mathbb{R}^n$ that satisfies $\xi(0) \in \bar{\Omega}$, $\xi(t) = y$ and $\dot{\xi}(s) \in A\xi(s) + V$ for almost all $s \in [0,t]$. We apply [33, Thm. 6.1] and pick a bounded, measurable function $\nu : [0,t] \to f(\bar{x}, W) + \gamma\mathbb{B}$ that satisfies $\dot{\xi}(s) = A\xi(s) - A\bar{x} + \nu(s)$. Let $\eta : [0,t] \to \mathbb{R}^n$ be given by $\eta(s) = \xi(s) - \bar{x}$ which satisfies for almost all $s \in [0,t]$ the differential equation $\dot{\eta}(s) = A\eta(s) + \nu(s)$ and we use (32) to obtain the inequality $\|\eta(s)\| \leq v e^{at}(\|\eta(0)\| + h)$. In particular, we get $\|y - \bar{x}\| \leq v e^{ah}(\|\eta(0)\| + h)$. The same estimates holds for all $y \in \chi([0,h], \bar{\Omega})$. Then using $\|\eta(0)\| = \|\xi(0) - \bar{x}\| \leq \operatorname{diam} \bar{\Omega} + h/2M$ we obtain

$$\operatorname{diam} \chi([0,h], \bar{\Omega}) \leq D(\operatorname{diam} \bar{\Omega} + h)$$

for $D = 2(v e^{a\bar{h}} + M/2 + 1)$.

Let $\bar{K} = K + D(\operatorname{diam} K + \bar{h})\mathbb{B} + \gamma\mathbb{B}$ so that $\chi([0,h], \bar{\Omega}) + \gamma\mathbb{B} \subseteq \bar{K}$. Since $\bar{K} \times W$ is compact and the partial derivatives of $f(\cdot, \bar{w})$ are continuous, we can pick $B_1, B_2 \in \mathbb{R}_{\geq 0}$ so that for all $i \in [1;n]$ we have $\|D_1(f_i(\bar{x}, w) - f_i(\bar{x}, \bar{w}))\| \leq B_1$ and $\frac{1}{2}\|D_1^2 f_i(z, w)(x - \bar{x})\| \leq B_2$ for all $x, z \in \operatorname{con}(\bar{K} \cup \{\bar{x}\})$ and $w \in W$. For $B = B_1 + B_2$ together with

$$\begin{aligned} \operatorname{diam} \operatorname{con}(\chi([0,h], \bar{\Omega}) + \gamma\mathbb{B} \cup \{\bar{x}\}) &\leq \operatorname{diam} \chi([0,h], \bar{\Omega}) + 2\gamma + Mh \\ &\leq D(\operatorname{diam} \bar{\Omega} + h) + 2\gamma + Mh \end{aligned}$$

we get

$$\begin{aligned} \|E(\chi([0,h], \bar{\Omega}) + \gamma\mathbb{B}, \bar{x}, \bar{w})\| &\leq B \max_{x \in \operatorname{con}(\chi([0,h], \bar{\Omega}) + \gamma\mathbb{B} \cup \{\bar{x}\})} \|x - \bar{x}\| \\ &\leq B(D(\operatorname{diam} \bar{\Omega} + h) + 2\gamma + Mh) \\ &\leq C(\operatorname{diam} \bar{\Omega} + h + \gamma) \end{aligned}$$

for $C \geq B(D + M + 2)$. Since this constant is independent of the particular choices of $\bar{\Omega} \subseteq K$, $\hat{x} \in \bar{\Omega}$ and $\bar{w} \in W$, the assertion follows. □

We use the following version of Grownwall’s Lemma, whose proof can be found in [7, Ch. 2, Sec. 4, Thm. 1].

Lemma 6.6. *Consider* (2) *with $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$, $\emptyset \neq W \subseteq \mathbb{R}^m$ and let $f(x, W)$ be closed for all $x \in \mathbb{R}^n$. Consider a compact and convex set $K \subseteq \mathbb{R}^n$. Suppose that f is continuous and there exists $k \in \mathbb{R}_{>0}$ so that all $x, \bar{x} \in K$ we have*

$$H(f(x, W), f(\bar{x}, W)) \leq k\|x - \bar{x}\|. \tag{33}$$

Let $\zeta : [0,t] \to \mathbb{R}^n$ with $t \in \mathbb{R}_{\geq 0}$ be an absolutely continuous function that satisfies $\dot{\zeta}(s) \in f(\zeta(s), W) + \varepsilon\mathbb{B}$ for almost all $s \in [0,t]$, where $\varepsilon \in \mathbb{R}_{\geq 0}$. Consider the function $\alpha : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ given by

$$\alpha(s, \delta) := e^{ks}\delta + \frac{\varepsilon}{k}(e^{sk} - 1)$$

and assume that $\zeta(s) + \alpha(s, \delta) \in K$ for all $s \in [0,t]$ and let $p \in \mathbb{R}^n$ with $\|p - \zeta(0)\| \leq \delta$. Then there exists a solution ξ of (2) *on $[0,t]$ that satisfies $\xi(0) = p$ and*

$$\forall s \in [0,t] : \quad \|\zeta(s) - \xi(s)\| \leq \alpha(s, \delta).$$

We have all the ingredients to provide the proof of Theorem 6.3.

Proof of Theorem 6.3. Let $M \in \mathbb{R}_{>0}$ be such that

$$1 + \max_{x,\bar{x} \in K+3\delta\mathbb{B},\, w \in W} \|D_1 f(x,\bar{w})(x-\bar{x}) + f(x,w)\| = M. \tag{34}$$

Since f and the partial derivatives of $f(\cdot,w)$ are continuous and $(K+3\delta\mathbb{B}) \times W$ is compact, the maximum is guaranteed to exist. Moreover, since $f(\cdot,W)$ is continuous and K is compact, we can pick $k \in \mathbb{R}_{>0}$ so that (33) holds for all $x, \bar{x} \in K + 3\delta\mathbb{B}$. We pick e so that

$$\|e\| \le 1/2 \quad \text{and} \quad 2\|e\|(\mathrm{e}^{kT}-1)/k \le \delta/2. \tag{35}$$

Let C be the constant in Lemma 6.5 for the compact set $K + 3\delta\mathbb{B}$ and $\bar{h} = 1$. Then we fix γ and N so that for $h = T/N$ we have

$$\begin{aligned} &C\gamma \le e_{i^*}/4, \quad \gamma\|(\mathrm{e}^{kT}-1)/k\| \le \delta/4, \quad \gamma \le 1, \quad h \le 1, \\ &hM \le \delta, \quad (C+cM)h \le e_{i^*}/4, \text{ and } \gamma N \mathrm{e}^{kT} \le \delta/4. \end{aligned} \tag{36}$$

Let us introduce $\kappa_0 = 0$ and for $i \in [1;N]$ the constant

$$\kappa_i = \frac{2\|e\| + \gamma}{k}(\mathrm{e}^{ikh}-1) + \gamma\sum_{j=1}^{i} \mathrm{e}^{(j-1)kh}.$$

From our choice of e and γ follows $\kappa_i \le \delta$ for all $i \in [0;N]$.

In Algorithm 1 for $i \in [1;N]$, consider the sets Ω_i, and $\Omega_{[i-1;i]}$ initialized in line 6 and updated in lines 17 and 18 and let $\Omega_0 = \Omega$. We show that

$$\Omega_{i-1} \subseteq \psi((i-1)h, \Omega) + \kappa_{i-1}\mathbb{B}$$

implies

a) the while-loop terminates;
b) $\Omega_i \subseteq \psi(ih,\Omega) + \kappa_i\mathbb{B}$;
c) $\Omega_{[i-1;i]} \subseteq \psi([0,h], \psi((i-1)h,\Omega)) + \kappa_i\mathbb{B}$.

We begin with a). For the sake of contradiction, let us assume that the while-loop does not terminate, i.e., the list of sets Q never becomes empty – new sets are added repeatedly in line 20. This can only happen if the error check in line 15 fails repeatedly. For two subsets P and $\bar{P}$ of $\mathbb{R}^n$ with $P \subseteq \bar{P}$ we have $\texttt{ComputeError}(P,\bar{x},\bar{w}) \le \texttt{ComputeError}(\bar{P},\bar{x},\bar{w})$ and we can bound the error $\hat{e}$ computed in line 14 by $\texttt{ComputeError}(\chi([0,h],\bar{\Omega}) + \gamma\mathbb{B}, \bar{x}, \bar{w})$ where we used (14b). Then we apply (19b) with $c \operatorname{diam} \operatorname{con}(\bar{\Omega} \cup \{\bar{x}\}) \le c \operatorname{diam} \bar{\Omega} + cMh$ and Lemma 6.5 to see that in each iteration we have

$$\|\hat{e}\| \le c \operatorname{diam} \bar{\Omega} + cMh + C(\operatorname{diam} \bar{\Omega} + h + \gamma) \le (C+c) \operatorname{diam} \bar{\Omega} + e_{i^*}/2$$

where we used the inequalities $(cM + C)h \le e_{i^*}/4$ and $C\gamma \le e_{i^*}/4$ which follow from the choice of the parameters. Due to (21b), we see that any time new sets are added to the queue Q, the diameter is strictly smaller, and the error check in line 15 can fail only finitely many times.

We continue with b) and c). Consider the for-loop in line 3, with $i \in [1;N]$ and let Q_{i-1} denote the set of sets $\bar{\Omega}$ that are removed from Q in line 8 throughout the while-loop and that lead to the error $\hat{e}$ (computed in line 14) that satisfies $e \ge \hat{e}$. We pick $\bar{\Omega} \in Q_{i-1}$ and consider the sets Ω_h and $\Omega_{[0,h]}$ computed in lines 12, respectively, 13 using the linear differential inclusion (12) with A and V computed in lines 10, respectively, 11. As $\texttt{SubDiv}$ satisfies (20) we have $\cup_{\bar{\Omega}\in Q_{i-1}} \subseteq \Omega_{i-1}$. Note that $Ax + V \subseteq G_e(x) + \gamma\mathbb{B}$ where G_e is given in (22) and parameterized with e, $\bar{x}$ and $\bar{w}$, with $\bar{x}$ computed in line 9. We apply Lemma 6.4 with $\Omega_{[0,h]}$ in place of K and use (15) to see that

$$Ax + V \subseteq G_e(x) + \gamma\mathbb{B} \subseteq f(x,W) + 2[-e,e] + \gamma\mathbb{B}$$

holds for all $x \in \Omega_{[0,h]}$.

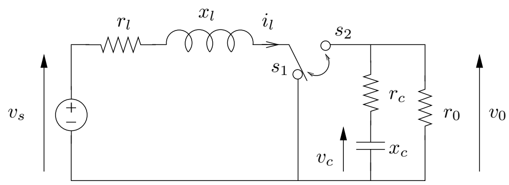

Figure 1: The DC-DC boost converter [24].

Let $\chi(h,\Omega)$ and $\chi([0,h],\Omega)$ denote the reachable set, respectively, the reachable tube of (12) from $\bar{\Omega}$ at time h. Let ζ be a solution of (12) on $[0,h]$ with $\zeta(0) \in \bar{\Omega}$. It follows from Theorem 6.1 that for $s \in [0,t]$ we have $\zeta(s) \in \Omega_{[0,h]}$. Hence, $\dot{\zeta}(s) \in f(\zeta(s),W) + \varepsilon\mathbb{B}$ with $\varepsilon = 2\|e\| + \gamma$ holds for almost all $s \in [0,t]$. Consider the context of Lemma 6.6 with $K + 3\delta\mathbb{B}$ and κ_{i-1} in place of K and δ, respectively. A straightforward computation shows that the function α satisfies for all $s \in [0,h]$

$$\alpha(s,\kappa_{i-1}) \le \alpha(h,\kappa_{i-1}) + \gamma = \kappa_i \le \delta.$$

We use (35) and (36) to see that $\varepsilon \le 1$ so that from (34) follows $\|\dot{\zeta}(s)\| \le M$ for all $s \in [0,t]$. Moreover, $\zeta(0) \in \bar{\Omega} \subseteq \Omega_{i-1} \subseteq \psi((i-1)h,\Omega) + \kappa_{i-1}\mathbb{B} \subseteq K + \delta\mathbb{B}$. Since, $Mh \le \delta$ (see (36)) we have $\zeta(s) \in K + 2\delta\mathbb{B}$ for all $s \in [0,t]$. Hence, $\zeta(s) + \alpha(s,\kappa_{i-1}) \in K + 3\delta\mathbb{B}$. As $\bar{\Omega} \subseteq \Omega_{i-1} \subseteq \psi(h(i-1),\Omega) + \kappa_{i-1}\mathbb{B}$ we can pick $p \in \psi((i-1)h,\Omega)$ with $\|\zeta(0) - p\| \le \kappa_{i-1}$. It follows from Lemma 6.6 that there exists a solution ξ of (2) on $[0,t]$ with $\xi(0) = p$ so that $\|\zeta(s) - \xi(s)\| \le \alpha(s,\kappa_{i-1})$. Therefore, we get

$$\begin{aligned} \Omega_h \subseteq \chi(h,\bar{\Omega}) + \gamma\mathbb{B} &\subseteq \psi(h,\psi((i-1)h,\Omega)) + (\alpha(h,\kappa_{i-1}) + \gamma)\mathbb{B} \\ &\subseteq \psi(ih,\Omega) + \kappa_i\mathbb{B}, \end{aligned}$$

where we used (14b) to obtain the first inclusion. Similarly, we have

$$\Omega_{[0,h]} \subseteq \chi([0,h],\bar{\Omega}) + \gamma\mathbb{B} \subseteq \psi([0,h],\psi((i-1)h,\Omega)) + \kappa_i\mathbb{B}.$$

Since this inclusions hold for all $\bar{\Omega} \in Q_{i-1}$, the statements b) and c) follow and one can derive (27). □

7 DEMONSTRATION

We illustrate the performance of Algorithm 1 by computing reachable sets and reachable tubes of a DC-DC boost converter, taken from [11] and illustrated in Figure 1. The DC-DC boost converter is modelled as a switched linear system, whose state vector $x = (i_L, 5v_C) \in \mathbb{R}^2$ is given by the inductor current and the capacitor voltage (scaled as in [24]). The system dynamics is of the form

$$f(x,w) = A_u(w)x + B(w) \tag{37}$$

where $u \in \{1,2\}$ is the control input to indicate the switch position. The time-varying input $w = (r_0, v_S)$ represents the load r_0 and the source voltage v_S. Subsequently, we restrict our analysis to the switch position s_2 in which case the system description is given by

$$A_2(w) = \frac{1}{200r_0 + 1}\begin{pmatrix} \frac{-(220r_0+1)}{60} & -40r_0/3 \\ 100r_0/7 & -20/7 \end{pmatrix}, \quad B(w) = \begin{pmatrix} v_S/3 \\ 0 \end{pmatrix}.$$

We set the bound on the input signals to $W = [1, 5] \times [0.8, 1.2]$, which accounts for load as well as voltage source fluctuations. Note that $f(x, W)$ might not be convex for all $x \in \mathbb{R}^2$. Subsequently, we approximate the reachable set and reachable tube of the convexified differential inclusion con $f(x, W)$. Clearly, this does not affect the correctness of our approach. Moreover, due to the relaxation theorem, the convergence result is also still valid, see [7] and [46].

We implemented Algorithm 1 by adapting the `nonlinearSys` class in `CORA`. The tool uses zonotopes as underlying set representation. The algorithms $\texttt{ReachSetLin}_\gamma$, $\texttt{ReachSetTube}_\gamma$ and `SubDiv` are already provided by the tool and we only need to implement $\texttt{Approx}_\gamma$ and `ComputeError`. The subroutine `ComputeError` is a simple adaptation of similar error computations and subsequently, we explain the implementation of $\texttt{Approx}_\gamma(f(x, W))$. To this end, we used the support function $\sigma_{f(x,W)}$ of con $f(x, W)$ given by

$$\sigma_{f(x,W)}(y) = \max_{w \in W} y_1 f_1(x, w) + y_2 f_2(x, w). \tag{38}$$

Since each entry in $A(w)$ and $B(w)$ is either monotonically increasing or decreasing over $w \in W$, the maximization domain W in (38) can be reduced to the set of vertices $\{(1, 0.8), (5, 0.8), (1, 1.2), (1, 0.8)\}$ so that an evaluation of (38) for $y \in \mathbb{R}^2$ is straightforward. In the reachable set computations, we used the directions $l_1 = -l_2 = (1, 0)$ and $l_3 = -l_4 = (0, 1)$ to approximate $f(x, W)$, i.e.,

$$\texttt{Approx}_\gamma(f(x, W)) = \cap_{i \in [1;4]} \left\{ x \in \mathbb{R}^2 \mid l_i^\top x \leq \sigma_{f(x,W)}(l_i) \right\}. \tag{39}$$

In order to increase the accuracy of the linear differential inclusion in Algorithm 1 we also adapted the iterative error computation from ① in [3, Alg. 1].

We conducted a number of experiments to compute the reachable set $\psi(T, \Omega)$ of the DC-DC boost converter with switch position s_2 from $\Omega = \{(1, 5)\}$ at $T = 2$ sec. We compare the over-approximations obtained by Algorithm 1 with the algorithms implemented in `CORA` as well as `VNODELP`. We called Algorithm 1 with parameters $N = 20$, $e = (0.2, 0.2)$ and $\bar{w} = (3, 1)$. We fixed the zonotope order to 10. For `VNODELP` we used the default parameters, as increasing the relative and absolute tolerance did not influence the result. `CORA` provides many different options. We set the options, so that a linear differential inclusion as in Example 2 serves as conservative approximation, i.e., `tensorOrder = 2`, and activated the advanced error computation `advancedLinErrorComp = 1`, see [3]. Most of the other parameters, such as the step size $h = T/N = 0.1$, the zonotope order 10, the maximal error $e = 2$ and the number of Taylor terms 4 did not substantially influence the accuracy of the computation. However, when we decreased the maximal error to less than 1, the computation did not terminate, even with a step size of $h = 10^{-5}$ and zonotope order 100, which indicates that the algorithm does not converge. The results are illustrated in Figure 2, which shows that actually only Algorithm 1 is able to produce accurate approximations.

In Figure 3, we show three approximations of the reachable tube $\psi([0, 5], \{(1, 5)\})$ computed with Algorithm 1 for a step size $h = 0.1$, $\bar{w} = (3, 1)$ and error parameters $e_1 = (0.1, 0.1)$, $e_2 = (0.01, 0.01)$ and $e_3 = (0.001, 0.001)$. We improved the accuracy of `ComputeError` by evaluating the maximization argument in (18) with an increasing number of smaller intervals that cover W. We used 4, 16 and 512 intervals for the three computations, respectively. No subdivisions occurred for e_1 and e_2, while fifteen subdivisions occurred for e_3. The computation took 2.3, 3 and 149 sec, respectively. Adding directions $l \in \{(-1, 1), (-1, -1), (1, -1), (1, 1)\}$ in (39) to increased the accuracy of $\texttt{Approx}_\gamma$ did not influence the result. The black lines are random simulations of the DC-DC dynamics. The plot illustrate nicely, how the accuracy of the approximation increases with a decreasing error parameter.

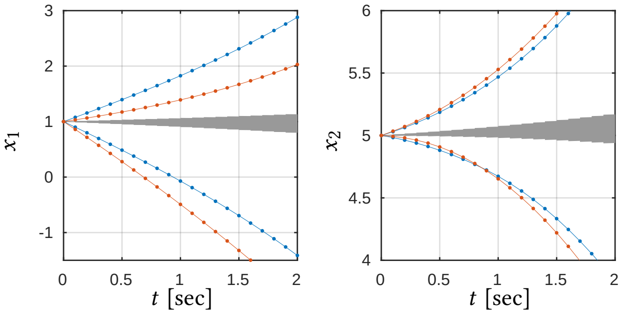

Figure 2: Approximation of $\psi([0, 2], \{(1, 5)\})$ projected onto x_1 (left) and x_2 (right) computed with Alg. 1 (gray shaded area), and approximation of $\psi(0.1i, \{(1, 5)\})$, $i \in [0; 20]$ projected onto x_1 and x_2 computed with `CORA` (red) and `VNODELP` (blue).

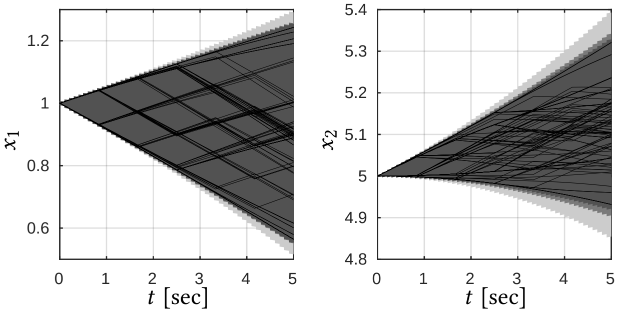

Figure 3: Approximations of $\psi([0, 5], \{(1, 5)\})$ projected onto x_1 (left) and x_2 (right) computed with Alg. 1 with $h = 0.1$, $e_1 = (0.1, 0.1)$ (light gray), $e_2 = (0.01, 0.01)$ (medium gray) and $e_3 = (0.001, 0.001)$ (dark gray). The black lines are random simulations of the DC-DC boost converter.

All the computations were performed on an Intel i7 3.5GHz CPU with 32GB memory.

8 SUMMARY

We have introduced a novel extension of hybridization methods that are known for autonomous systems to nonlinear systems with time-varying input parameters. The algorithm computes over-approximations of reachable sets and reachable tubes of nonlinear system of the form (2). The algorithm is correct (Theorem 6.1).

Moreover, it is possible to compute approximations of any desired accuracy (Theorem 6.3). We have demonstrate the effectiveness of the algorithm with the help of a small example.

9 ACKNOWLEDGEMENT

The authors wish to thank G. Reissig (Munich) for fruitful discussions related to the research reported in this paper. This work is supported in part by the DFG grant ZA 873/1-1 and TUM IGSSE.

REFERENCES

[1] M. Althoff. 2013. Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets. In *Proc. of the 16th Int. Conf. on Hybrid Systems: Computation and Control*. ACM, 173–182.

[2] M. Althoff. 2015. An Introduction to CORA 2015. In *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*. EasyChair, 120–151.

[3] M. Althoff and B. H. Krogh. 2014. Reachability analysis of nonlinear differential-algebraic systems. *IEEE Trans. Automat. Control* 59, 2 (2014), 371–383.

[4] M. Althoff, O. Stursberg, and M. Buss. 2008. Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization. In *Proc. of the 47th IEEE Conf. on Decision and Control*. IEEE, 4042–4048.

[5] E. Asarin, T. Dang, and A. Girard. 2003. Reachability analysis of nonlinear systems using conservative approximation. In *Proc. of the 6th Int. Conf. on Hybrid Systems: Computation and Control*. Springer, 20–35.

[6] E. Asarin, T. Dang, and A. Girard. 2007. Hybridization methods for the analysis of nonlinear systems. *Acta Informatica* 43, 7 (2007), 451–476.

[7] J.-P. Aubin and A. Cellina. 1984. *Differential inclusions: set-valued maps and viability theory*. Grundlehren der mathematischen Wisschenschaften, Vol. 264. Springer.

[8] R. Baier, M. Gerdts, and I. Xausa. 2013. Approximation of reachable sets using optimal control algorithms. *Numerical Algebra, Control and Optimization* 3, 3 (2013), 519–548.

[9] S. Bak, S. Bogomolov, T. A. Henzinger, T. Johnson, and P. Prakash. 2016. Scalable static hybridization methods for analysis of nonlinear systems. In *Proc. of the 19th Int. Conf. on Hybrid Systems: Computation and Control*. ACM, 155–164.

[10] R. G. Bartle. 1976. *The elements of real analysis*. Vol. 2. Wiley New York.

[11] A. G. Beccuti, G. Papafotiou, and M. Morari. 2005. Optimal control of the boost dc-dc converter. In *Proc. of the 44th IEEE Conf. on Decision and Control and European Control Conference*. IEEE, 4457–4462.

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

[13] W-J Beyn and J. Rieger. 2007. Numerical fixed grid methods for differential inclusions. *Computing* 81, 1 (2007), 91–106.

[14] O. Bokanowski, N. Forcadel, and H. Zidani. 2010. Reachability and minimal times for state constrained nonlinear problems without any controllability assumption. *SIAM Journal on Control and Optimization* 48, 7 (2010), 4292–4316.

[15] CAPD. 2017. Computer Assisted Proofs in Dynamics group, a C++ package for rigorous numerics. (2017). Retrieved Sep, 2017 from http://capd.ii.uj.edu.pl.

[16] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre. 1999. Set-valued numerical analysis for optimal control and differential games. In *Stochastic and differential games*. Springer, 177–247.

[17] X. Chen, E. Ábrahám, and S. Sankaranarayanan. 2013. Flow*: An analyzer for non-linear hybrid systems. In *Proc. of the Int. Conf. on Computer Aided Verification*. Springer, 258–263.

[18] P. Collins and L. Geretti. 2017. Ariadne: A C++ library for formal verification of cyber-physical systems, using reachability analysis for nonlinear hybrid automata. (2017). Retrieved Sep, 2017 from http://www.ariadne-cps.org/

[19] T. Dang, C. Le Guernic, and O. Maler. 2011. Computing reachable states for nonlinear biological models. *Theoretical Computer Science* 412, 21 (2011), 2095–2107.

[20] T. Dang, O. Maler, and R. Testylier. 2010. Accurate hybridization of nonlinear systems. In *Proc. of the 13th Int. Conf. on Hybrid Systems: Computation and Control*. ACM, 11–20.

[21] A. L. Dontchev and E. M. Farkhi. 1989. Error estimates for discretized differential inclusions. *Computing* 41, 4 (1989), 349–358.

[22] R. Freeman and P. V. Kokotovic. 1996. *Robust nonlinear control design: state-space and Lyapunov techniques*. Birkhäuser.

[23] G. Frehse and et al. 2011. SpaceEx: Scalable verification of hybrid systems. In *Proc. of the Int. Conf. on Computer Aided Verification*. Springer, 379–395.

[24] A. Girard, G. Pola, and P. Tabuada. 2010. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Trans. Automat. Control* 55 (2010), 116–126.

[25] Z. Han and B. H. Krogh. 2006. Reachability analysis of nonlinear systems using trajectory piecewise linearized models. In *American Control Conference*. IEEE, 1505–1510.

[26] S. M. Harwood and P. I. Barton. 2016. Efficient polyhedral enclosures for the reachable set of nonlinear control systems. *Mathematics of Control, Signals, and Systems* 28, 1 (2016), 1–33.

[27] T. A. Henzinger, B. Horowitz, R. Majumdar, and H. Wong-Toi. 2000. Beyond HYTECH: Hybrid systems analysis using interval numerical methods. In *Proc. of the 3rd Int. Conf. on Hybrid Systems: Computation and Control*, Vol. 1790. Springer, 130–144.

[28] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. 1995. What's decidable about hybrid automata?. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*. ACM, 373–382.

[29] B. Houska, F. Logist, J. Van Impe, and M. Diehl. 2012. Robust optimization of nonlinear dynamic systems with application to a jacketed tubular reactor. *Journal of Process Control* 22, 6 (2012), 1152–1160.

[30] T. Kapela and P. Zgliczyński. 2009. A Lohner-type algorithm for control systems and ordinary differential inclusions. *Discrete and Continuous Dynamical Systems. Series B. A Journal Bridging Mathematics and Sciences* 11, 2 (2009), 365–385.

[31] V. A. Komarov and K. E. Pevchikh. 1991. A method of approximating attainability sets for differential inclusions with a specified accuracy. *U. S. S. R. Comput. Math. and Math. Phys.* 31, 1 (1991), 153–157.

[32] C. Le Guernic and A. Girard. 2010. Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems* 4, 2 (2010), 250–262.

[33] D. Li. 2007. Morse decompositions for general dynamical systems and differential inclusions with applications to control systems. *SIAM Journal on Control and Optimization* 46, 1 (2007), 35–60.

[34] D. Limon, J. M. Bravo, T. Alamo, and E. F. Camacho. 2005. Robust MPC of constrained nonlinear systems based on interval arithmetic. *IEE Proceedings-Control Theory and Applications* 152, 3 (2005), 325–332.

[35] Y. Lin and M. A. Stadtherr. 2007. Deterministic global optimization of nonlinear dynamic systems. *AIChE Journal* 53, 4 (2007), 866–875.

[36] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin. 2005. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic control* 50, 7 (2005), 947–957.

[37] N. S. Nedialkov. 2011. Implementing a rigorous ODE solver through literate programming. In *Modeling, Design, and Simulation of Systems with Uncertainties*. Springer, 3–19.

[38] N. S. Nedialkov, K. R. Jackson, and G. F. Corliss. 1999. Validated solutions of initial value problems for ordinary differential equations. *Appl. Math. Comput.* 105, 1 (1999), 21–68.

[39] M. S. Nikol'skii. 1988. A method of approximating an attainable set for a differential inclusion. *U. S. S. R. Comput. Math. and Math. Phys.* 28, 4 (1988), 192–194.

[40] D. Nira, F. Elza, and M. Alona. 2014. *Approximation of Set-Valued Functions: Adaptation of Classical Approximation Operators*. World Scientific Publishing Company.

[41] A. Puri, V. Borkar, and P. Varaiya. 1996. ε-approximation of differential inclusions. In *Hybrid Systems III: Verification and Control*. Springer, 362–376.

[42] G. Reissig. 2011. Computing abstractions of nonlinear systems. *IEEE Trans. Automat. Control* 56, 11 (2011), 2583–2598.

[43] J. Rieger. 2009. Shadowing and the viability kernel algorithm. *Applied Mathematics & Optimization* 60, 3 (2009), 429–441.

[44] R. T. Rockafellar and R. J-B Wets. 2009. *Variational analysis*. Vol. 317. Springer.

[45] M. Rungger and G. Reißig. 2017. Arbitrarily Precise Abstractions for Optimal Controller Synthesis. In *Proc. of the 56th IEEE Conf. on Decision and Control*. IEEE, 1761 – 1768.

[46] M. Sandberg. 2008. Convergence of the forward Euler method for nonconvex differential inclusions. *SIAM J. Numer. Anal.* 47, 1 (2008), 308–320.

[47] J. K. Scott and P. I. Barton. 2013. Bounds on the reachable sets of nonlinear control systems. *Automatica* 49, 1 (2013), 93–100.

[48] J. K. Scott, D. M. Raimondo, G. R. Marseglia, and R. D. Braatz. 2016. Constrained zonotopes: A new tool for set-based estimation and fault detection. *Automatica* 69 (2016), 126–136.

[49] A. B. Singer and P. I. Barton. 2006. Global optimization with nonlinear ordinary differential equations. *Journal of Global Optimization* 34, 2 (2006), 159–190.

[50] E. D. Sontag. 1998. *Mathematical control theory: deterministic finite dimensional systems* (2 ed.). Textbooks in Applied Mathematics, Vol. 6. Springer.

[51] K. Taubert. 1981. Converging multistep methods for initial value problems involving multivalued maps. *Computing* 27, 2 (1981), 123–136.

[52] M. E. Villanueva, B. Houska, and B. Chachuat. 2015. Unified framework for the propagation of continuous-time enclosures for parametric nonlinear ODEs. *Journal of Global Optimization* 62, 3 (2015), 575–613.

[53] W. Walter. 1964. *Differential and integral inequalities*. Vol. 55. Springer. Translated from German in 1970 by L. Rosenblatt and L. Shampine.

[54] M. Zamani, G. Pola, M. Mazo, and P. Tabuada. 2012. Symbolic models for nonlinear control systems without stability assumptions. *IEEE Trans. Automat. Control* 57, 7 (2012), 1804–1809.

[55] S. G. Živanović and P. Collins. 2010. Numerical solutions to noisy systems. In *Proc. of the 49th IEEE Conf. on Decision and Control*. IEEE, 798–803.