Proceedings of the
47th IEEE Conference on Decision and Control
Cancun, Mexico, Dec. 9-11, 2008



# Reachability Analysis of Nonlinear Systems with Uncertain Parameters using Conservative Linearization

Matthias Althoff, Olaf Stursberg, and Martin Buss

*Abstract*— **Given an initial set of a nonlinear system with uncertain parameters and inputs, the set of states that can possibly be reached is computed. The approach is based on local linearizations of the nonlinear system, while linearization errors are considered by Lagrange remainders. These errors are added as uncertain inputs, such that the reachable set of the locally linearized system encloses the one of the original system. The linearization error is controlled by splitting of reachable sets. Reachable sets are represented by zonotopes, allowing an efficient computation in relatively high-dimensional space.**

## I. Introduction

In order to ensure reliability and safety of technical systems, one has to ensure that the system works as specified in all operating conditions. A possibility to find system failures is given by numeric simulation with changing initial conditions, inputs, and disturbances. The test by simulation can be improved by a guided search for simulation runs that violate the system, see e.g. [1], [2]. The sets of violating or dangerous states are also referred to as the sets of unsafe states. A disadvantage of the simulation based techniques is that they can only conclude that a system (with continuous or hybrid dynamics) is unsafe, but safety cannot be guaranteed. This is because the set of initial states, inputs and disturbances is continuous, hence infinitely many executions of the system exist, which cannot be completely checked.

In contrast to simulation techniques, reachability analysis allows to guarantee safety. A reachable set is the set of states that can be reached by a system for given sets of initial states, inputs, and disturbances. If the reachable set does not intersect with the set of unsafe states, safety can be guaranteed. In this work, reachable sets are computed for nonlinear continuous systems. The extension to nonlinear hybrid systems (i.e. systems with combined discrete and continuous dynamics, see e.g. [3]) can be accomplished by methods presented in [4], [5].

It has not yet been shown that the computation of exact reachable sets for nonlinear continuous systems is possible [6]. Approximations of reachable sets for nonlinear systems have been developed e.g. in [7], [8] - they only allow to conclude safety if an over-approximation of the reachable set can be guaranteed. This is because one can conclude, that the exact reachable set does not intersect any unsafe set, if the over-approximated reachable set does not. A method that does not explicitly compute reachable sets but leads to over-approximated bounds on reachable sets are barrier certificates [9]. The explicit computation of over-approximated reachable sets has been performed for polynomial nonlinear systems using Bézier control nets in [10] and for general nonlinear systems using global optimization techniques and face lifting in [11], [12] respectively. These approaches compute the reachable sets based on the dynamics of the original nonlinear system.

Another research direction is the computation of reachable sets based on abstracted models. The most common models used to abstract nonlinear dynamics, are systems with constant bounds on the derivative ($\dot{x} \in [\underline{a}, \overline{a}]$, $\underline{a} \leq \overline{a} \in \mathbb{R}^n$) and linear systems ($\dot{x} \in Ax + U$, $A \in \mathbb{R}^{n \times n}, x \in \mathbb{R}^n, U \subset \mathbb{R}^n$). In order to abstract the nonlinear dynamics, the state space of the system is usually partitioned into regions in which the nonlinear system is locally abstracted. The partition of the state space into regions can be performed on-the-fly depending on the geometry of the reachable set or in advance with elements of fixed structure (e.g. by hyperrectangles of fixed size and orientation). The disadvantage of the fixed partitioning is that it usually imposes stronger limits on the dimension $n$ of the state space which can be handled: e.g., a partition of $w$ segments for each dimension results into $w^n$ regions. Basic work for the reachability analysis using models of constant bounds on the derivatives has been performed e.g. in [13], [14] which has been advanced in [15] using on-the-fly partitioning. Abstraction to linear systems using a fixed partition has been investigated in [16]. For the abstraction to linear systems using on-the-fly partitioning, the first approach known by the authors, is described in [17].

In this work, reachable sets of nonlinear systems are also computed by on-the-fly abstraction to linear systems. However, this approach differs in the following points from [17]:

- Intervals of the linearization error are computed separately for each dimension by evaluating the Lagrange remainder of the linearized system. In [17], the infinity norm of the linearization error is computed which has to be applied to all dimensions equally, resulting in a more conservative reachable set. The difference is evident for systems where sensitive inputs[1] have small linearization errors compared to other insensitive inputs. Applying the infinity norm also to the sensitive inputs, results in significant over-approximations of the reachable sets.
- Reachable sets of the linearized system are represented by zonotopes instead of polytopes. Zonotopes have shown to be a more efficient representation for the

All authors are with Institute of Automatic Control Engineering (LSR) , Technische Universität München, 80290 München, Germany {althoff,stursberg,mb}@tum.de

[1]Small perturbations of the input result in large perturbations of the state derivatives.

reachability analysis of linear systems, see [18]. Zonotopes are not closed under intersection and convex hull computation, resulting in a more conservative computations of reachable sets, particularly for hybrid systems. However, it is believed that these disadvantages can be overcompensated by the efficient representation of zonotopes.

- Uncertain parameters in the system model are considered.
- The linearization error is limited by splitting reachable sets.

## II. Objective

The objective is to compute the over-approximated reachable set of a nonlinear system with uncertain initial states, parameters, and inputs. The initial state $x(0)$ can take values from a set $X_0 \subset \mathbb{R}^n$. The dynamics depends on a set of model parameters $p_i(t)$, bounded by an interval $\mathcal{I} = [c, d]$ with $c < d$ and $c, d \in \mathbb{R}$. A parameter $p_i(t)$ can vary over time $t$ within the specified intervals, such that a vector $p$ of all parameters stays within an interval hull $P \in \mathcal{I}^o$ and $o$ is the number of parameters. Note that each parameter may vary independently. The input $u$ takes values from a set $U \subset \mathbb{R}^m$. The evolution of the state $x$ is defined by the following differential equation:

$$\dot{x} = f(x(t), u(t), p(t)), \tag{1}$$
$$x(0) \in X_0 \subset \mathbb{R}^n, \quad p(t) \in P \subset \mathcal{I}^o, \quad u(t) \in U \subset \mathbb{R}^m$$

where $u(t)$ and $p(t)$ are Lipschitz continuous. The set of reachable states of (1) at a time point $t = r$ is defined as:

*Definition 1:* The exact reachable set $R^e(r)$ that can be reached starting from $X_0$ (for $t = 0$) at time $t = r$ for $p \in P$ and $u \in U$ is:

$$R^e(r) = \{x | x(t) \text{ is a solution of (1), } t = r\}$$

An over-approximation of the reachable set at time $r$ is defined as $R(r) \supseteq R^e(r)$. The over-approximated set for the complete time interval $t \in [0, r]$ is defined as the union of all $R(t)$ for $t \in [0, r]$: $R([0, r]) := \bigcup_{t \in [0,r]} R(t)$.

## III. Overview of Reachable Set Computations

A brief description of the overall concept of computing $R([0, i \cdot r])$ is shown in Fig. 1 where $i \in \mathbb{N}^+$ is the time step and $r \in \mathbb{R}^+$ is the time increment. The reachable set is iteratively computed for smaller time intervals $t \in [(k-1) \cdot r, k \cdot r]$ where $k \in \mathbb{N}^+$, such that $R([0, i \cdot r])$ is obtained by their union: $R([0, i \cdot r]) = \bigcup_{k=1 \ldots i} R([(k-1) \cdot r, k \cdot r])$.
The reachable sets $R(r)$ and $R([0, r])$ for the first time step ($k = 1$) are computed based on the initial set $R(0)$. First, the nonlinear system $\dot{x} = f(x, u, p)$ is linearized on-the-fly to a system of the form $\dot{x} \in f_{lin}(x, u, p) = A(p)\Delta x + B(p)u + d(p) + L$. The matrices $A(p)$, $B(p)$ are matrices of proper dimension, depending on the parameter vector $p$, and $d(p)$ is a vector depending on $p$. The set $L$ is the set of possible linearization errors for $t \in [(k-1) \cdot r, k \cdot r]$, which has to ensure $f(x, u, p) \in f_{lin}(x, u, p)$, such that the reachable set is enclosed by the approximation of the linearized system.

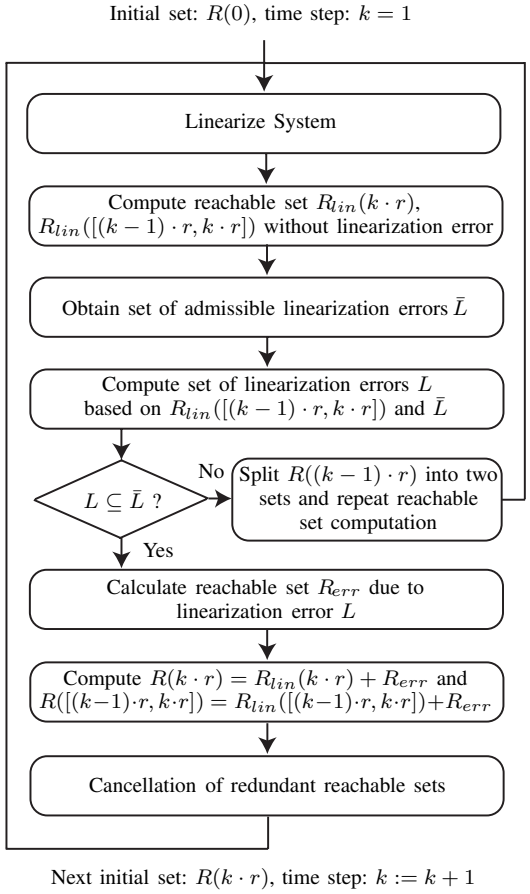



Fig. 1. Computation of reachable sets - overview.

In contrast to the reachable sets, the linearization error is modeled as a multi-dimensional interval $L \in \mathcal{I}^n$ in analogy to the set of parameters.
In order to compute $L$, the reachable set $R_{lin}(k \cdot r)$ and $R_{lin}([(k-1) \cdot r, k \cdot r])$ of $f_{lin}(x, u, p)$ without linearization error ($L = 0$) is computed first. Due to the superposition principle of linear systems, the reachable set $R_{err}$ due to the set of linearization errors $L$ can be computed separately and added to $R_{lin}$ later. In order to restrict the expansion of the reachable set due to the linearization error, a set $\bar{R}_{err}$ in which $R_{err}$ has to be enclosed is defined. This set allows to compute the set $\bar{L}$ of admissible linearization errors obtained from the linearized system dynamics $f_{lin}(x, u, p)$.
Based on the admissible reachable set $R_{adm}([(k-1) \cdot r, k \cdot r]) := R_{lin}([(k-1) \cdot r, k \cdot r]) + \bar{R}_{err}$, obtained by Minkowski addition[2] of $R_{lin}$ and $\bar{R}_{err}$, the set of linearization errors $L$ can be computed. In case that $L \nsubseteq \bar{L}$, the linearization error is not admissible, requiring to split the initial reachable set $R((k-1) \cdot r)$ of the current time interval into two reachable sets. This implies to perform the reachable set computation for both of the newly obtained sets once more. Hence, the number of reachable set segments for this time interval has increased by one. If $L \subseteq \bar{L}$, the linearization error is accepted and the reachable set is obtained by superposition of the

[2]Minkowski addition of two sets $A, B$: $A + B = \{a + b | a \in A, b \in B\}$

reachable set without linearization error and the one due to the linearization error: $R(k \cdot r) = R_{lin}(k \cdot r) + R_{err}$ and $R([(k-1) \cdot r, k \cdot r]) = R_{lin}([(k-1) \cdot r, k \cdot r]) + R_{err}$. It remains to increase the time step ($k := k + 1$) and cancel redundant reachable sets that are already covered by previously computed reachable sets, which decreases the number of reachable sets that have to be considered in the next time interval. The initial set for the next time step is $R(k \cdot r)$.

Besides the splitting of the reachable set in the state space, it is also possible to split the input and parameter sets in an analogous way. However, splitting of the reachable set is usually most effective as the linearization error is mostly dominated by the uncertainty of the state, and not by input or parameter uncertainties.

## IV. Reachable Set Computation of the Linearized System

This section describes the different steps of the linearization procedure in more detail, and explains the basics for the computation of reachable sets using zonotopes. The local linearization of the nonlinear system (1) is performed by a Taylor series. In order to introduce a concise notation, the state and input vector are combined to a new vector $z^T = \left[x^T, u^T\right]$. This allows to formulate a Taylor series of the nonlinear system dynamics (1) for a $p \in P$ as:

$$\dot{x}_i = f_i(z,p) = f_i(z^*,p) + \frac{\partial f_i(z,p)}{\partial z}\Big|_{z=z^*}(z-z^*) + \frac{1}{2}(z-z^*)^T \frac{\partial^2 f_i(z,p)}{\partial z^2})\Big|_{z=z^*}(z-z^*) + \dots$$

The infinite Taylor series can be over-approximated by a first order Taylor series and its Lagrange remainder:

$$\dot{x}_i \in \underbrace{f_i(z^*,p) + \frac{\partial f_i(z,p)}{\partial z}\Big|_{z=z^*}(z-z^*)}_{1^{st}\text{ order Taylor series}} + \underbrace{\frac{1}{2}(z-z^*)^T \frac{\partial^2 f_i(\xi,p)}{\partial z^2}(z-z^*)}_{\text{Lagrange remainder } L_i}. \quad (2)$$

Let $z$ be restricted to a convex set and let $z, z^*$ be fixed, then the Lagrange remainder $L$ can take any value that results from $\xi \in \{z^* + \alpha(z-z^*) | \alpha \in [0,1]\}$, see [19]. The computation of the set $L$ resulting from the set of possible values of $z$ and $\xi$ is presented in Sec. V. In order to obtain the standard notation of the linearized system, the $z$ vector is separated into the state vector $x$ and the input vector $u$.

$$\begin{aligned}\dot{x} &\in f(z^*,p) + \frac{\partial f(z,p)}{\partial z}\Big|_{z=z^*}(z-z^*) + L \\ &= A\Delta x + B\Delta u + f(x^*,u^*,p) + L\end{aligned} \quad (3)$$

with

$$\Delta x = x - x^*, \quad \Delta u = u - u^*$$
$$A = \frac{\partial f(x,u,p)}{\partial x}\Big|_{x=x^*}, \quad B = \frac{\partial f(x,u,p)}{\partial u}\Big|_{u=u^*}$$

In case there are no uncertain parameters $p$, one obtains matrices $A \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{n \times m}$ where the elements are real numbers. If the system contains uncertain parameters, the elements of the matrices are intervals such that $A \in \mathcal{I}^{n \times n}$ and $B \in \mathcal{I}^{n \times m}$.

### A. Reachable Set Computations for the Linear System

Reachable sets of linear systems with uncertain parameters and inputs have been computed in an earlier work of the authors [20]. The basic steps that are undertaken in order to compute the reachable set of the linearized system in (3), are recalled in the following. The reachable set of a time interval $t \in [(k-1) \cdot r, k \cdot r]$ is obtained by

1) computation of the reachable set $\hat{R}$ without input at the time points $t = (k-1) \cdot r$ and $t = k \cdot r$,
2) generation of the convex hull of the time point solutions,
3) enlarging of the convex hulls to ensure enclosure of all trajectories for the current time interval $t \in [(k-1) \cdot r, k \cdot r]$ under all possible inputs.

These basic steps are illustrated in Fig. 2. The same concept is applied for many algorithms (e.g. [18], [11], [21]) that compute over-approximated reachable sets.

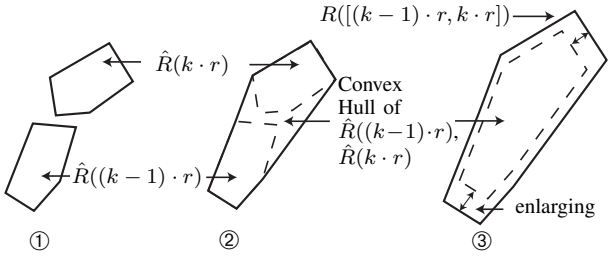



Fig. 2. Computation of reachable sets for a linear system.

In a first step, this procedure is applied to the linearized system (3) without considering the linearization error ($L = 0$) as described in Sec. III. After obtaining the linearization error $L$, the reachable set $R_{err}(t)$ of the linearized system (3) resulting from the additional input $L$ is computed. Due to the applicability of the superposition principle, the overall reachable set can be obtained by the Minkowski addition of $R_{lin}(t)$ and $R_{err}(t)$:

$$R(t) = R_{lin}(t) + R_{err}(t)$$

Note that $R(t)$ is the over-approximated reachable set of the original nonlinear system since the Lagrange remainder contains all possible linearization errors.

### B. Representation of Reachable Sets

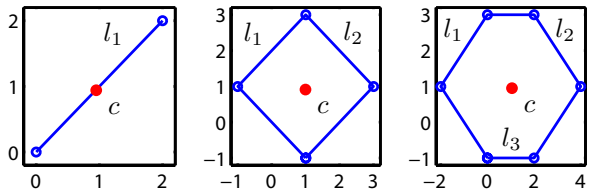
In this work, reachable sets are represented by zonotopes. They are chosen because linear transformations and Minkowski sums can be computed efficiently, allowing to compute reachable sets for large scale linear systems in continuous space [18], [20]. In addition, the axis-aligned bounding box, or so-called interval hull of zonotopes, can be computed in an efficient way what is advantageous for the computation of the Lagrange remainder. A zonotope is defined as follows:

*Definition 2 (Zonotope):* A zonotope is a set

$$Z = \left\{ x \in \mathbb{R}^n : x = c + \sum_{i=1}^{p} \beta^{(i)} \cdot g^{(i)}, \quad -1 \leq \beta^{(i)} \leq 1 \right\}$$

with $c, g^{(1)}, \ldots, g^{(p)} \in \mathbb{R}^n$. The vectors $g^{(1)}, \ldots, g^{(p)}$ are referred to as the *generators* and $c$ as the *center* of the zonotope. The order of a zonotope is $q = \frac{p}{n}$ and the notation is $(c, g^{(1 \ldots p)})$, where the first element in the parentheses always refers to the center of the zonotope.

In other words, a zonotope is defined by a center $c$ to which line segments $l_i = \beta^{(i)} \cdot g^{(i)}$, $-1 \leq \beta^{(i)} \leq 1$ are added via Minkowski sum. This is illustrated in Fig. 3, where the final zonotope is generated step by step from left to right by adding three two-dimensional line segments $l_1 \ldots l_3$ via Minkowski addition to the center of the zonotope. Zonotopes are always centrally symmetric to its center.




(a) $c + l_1$ (b) $c + l_1 + l_2$ (c) $c + l_1 + l_2 + l_3$

Fig. 3. Step-by-step construction of a zonotope from left to right via Minkowski addition of line segments.

The interval hull $\eta$ that encloses a zonotope can be computed as follows (see e.g. [18]):

$$\begin{aligned} \eta &= \mathcal{IH}(Z) = [\underline{\eta}, \overline{\eta}] \in \mathcal{I}^n \\ \underline{\eta} &= c - \sum_{i=1}^{p} |g^{(i)}|, \quad \overline{\eta} = c + \sum_{i=1}^{p} |g^{(i)}| \end{aligned} \tag{4}$$

where $\mathcal{IH}(Z)$ is the interval hull operator.

## V. Computation of the Linearization Error

As described in the previous section, the linearization error is obtained by evaluation of the Lagrange remainder. After defining $J_i(\xi, p) := \frac{\partial^2 f_i(\xi, p)}{\partial z^2}$, where $i$ is the system dimension of $f$, one can write the Lagrange remainder in (2) as

$$\begin{aligned} L_i &= \frac{1}{2}(z - z^*)^T J_i(\xi, p)(z - z^*), \\ \xi(z) &\in \{z^* + \alpha(z - z^*) | \alpha \in [0, 1]\} \end{aligned} \tag{5}$$

In order to determine the set $L_i$ for the time interval $t \in [0, r]$, one has to consider the possible values of $z$ within this time interval. The values of $z$ are within $\mathcal{Z}([0, r])$ which is the Cartesian product $\mathcal{Z}([0, r]) := R([0, r]) \times U$ as the state vector is restricted to $x([0, r]) \in R([0, r])$ and the input $u$ is restricted to $u \in U$. In order to determine the maximum absolute values of the $L_i$ for $z \in \mathcal{Z}([0, r])$ in an efficient way, the following over-approximation is computed:

*Proposition 1:* The absolute values of the Lagrange remainder can be over-approximated for $z \in \mathcal{Z}$ by the following computations:

$$|L_i| \subseteq [0, \hat{L}_i]$$

$$\text{with } \hat{L}_i = \frac{1}{2}\gamma^T \max(|J_i(\xi(z), p)|)\gamma, \; z \in \mathcal{Z}, \, p \in P$$

$$\text{and } \gamma = |c - z^*| + \sum_{i=1}^{p} |g^{(i)}|$$

where $c$ is the center and $g^{(i)}$ are the generators of the zonotope $\mathcal{Z}$. The max-operator and the absolute values are applied elementwise.

*Proof:* The following over-approximations apply for the absolute value of $L_i$:

$$\begin{aligned} |L_i| &= \left\{ \frac{1}{2} |(z - z^*)^T J_i(\xi(z), p)(z - z^*)| \, \middle| \, z \in \mathcal{Z}, p \in P \right\} \\ &\subseteq \frac{1}{2}[0, \max\left(|(z - z^*)^T J_i(\xi(z), p)(z - z^*)|\right)] \\ &\subseteq \frac{1}{2}[0, \max\left(|z - z^*|^T |J_i(\xi(z), p)||z - z^*|\right)] \\ &\subseteq \frac{1}{2}[0, \max(|z - z^*|)^T \max(|J_i(\xi(z), p)|) \max(|z - z^*|)] \end{aligned}$$

The expression $\max(|z - z^*|)$ can be further rewritten since $z \in \mathcal{Z}$ is within a zonotope with center $c$ and generators $g^{(i)}$:

$$\begin{aligned} &z \in \mathcal{Z}, x^{(i)} \in [-1, 1] : \max(|z - z^*|) = \\ &\max(|c - z^* + \sum_{i=1}^{p} x^{(i)} g^{(i)}|) \leq |c - z^*| + \sum_{i=1}^{p} |g^{(i)}| = \gamma \end{aligned}$$

such that the expression of proposition 1 is obtained. ■

The expression $\max(|J_i(\xi(z), p|)$ in proposition 1 is computed via interval arithmetics [22]. To do so, the values of $z$ have to be over-approximated by an interval vector as shown in (4): $z \in \mathcal{IH}(\mathcal{Z})$. From this follows that $\xi(z) \in \{z^* + \alpha(z - z^*) | \alpha \in [0, 1]\}$ also becomes an interval vector and the values of $p$ are intervals by definition.
The result of proposition 1 also allows to find a linearization point $z^*$ that minimizes the values $\hat{L}_i$ and thus the set of Lagrange remainders.

*Proposition 2:* The bound of the Lagrange remainder $\hat{L}$ is minimized by choosing $z^* = c$ as the linearization point.

*Proof:* The value of $\gamma$ is minimized by $z^* = c$ which can be directly checked from its computation in proposition 1. By choosing $z^* = c$, it follows that $\{\xi(z) | z \in \mathcal{Z}\} = \mathcal{Z}$ (which is independent of $z^*$) , such that $\max(|J_i(\xi(z), p)|)$ is not affected by the linearization point $z^*$. From this follows that $z^* = c$ minimizes $\hat{L}_i$. ■

After choosing $z^* = c$, it remains to solve the problem that the center $c$ of $\mathcal{Z}([0, r])$ is not known, since $\mathcal{Z}([0, r])$ is computed after linearization. As a solution, $c$ is approximated based on the center $\hat{c}$ of $\mathcal{Z}(0)$:

$$z^* = \hat{c} + \frac{r}{2} f(\hat{c}, mid(p)) \approx c$$

The operator $mid()$ returns the center of an interval vector.

## VI. Restriction of the Linearization Error

It is clear, that the Lagrange remainder strongly depends on the size and the center of a reachable set of a partial time interval. In order to deal with the increase of the linearization error with the size of the reachable set, the linearization error $R_{err}$ is restricted to a multidimensional interval $\bar{R}_{err}$. The rate of growth of the admissible expansion of $\bar{R}_{err}$ is restricted by the expansion vector $\theta \in \mathbb{R}^n$ which has to be set as a parameter of the reachability computations:

$$\bar{R}_{err}(r) \overset{!}{\subseteq} [-\theta \cdot r, \theta \cdot r] \tag{6}$$

The reachable set of the linearized system due to the linearization error $L = [-\hat{L}, \hat{L}]$ is as shown in [20]:

$$\bar{R}_{err}(r) = A^{-1}(e^{Ar} - I)[-\hat{L}, \hat{L}].$$

After the left multiplication of $(e^{Ar}-I)^{-1}A$ and the insertion of (6), one obtains

$$(e^{Ar} - I)^{-1}A[-\theta \cdot r, \theta \cdot r] \supseteq [-\hat{L}, \hat{L}],$$

which is fulfilled if

$$|(e^{Ar} - I)^{-1}A|\, \theta \cdot r =: \bar{L} \geq \hat{L}. \tag{7}$$

The absolute value in the above inequality is obtained elementwise. In case the constraint $\bar{L} \geq \hat{L}$ is not fulfilled for the time interval $t \in [k \cdot r, (k+1) \cdot r]$, the reachable set $R(k \cdot r)$ is split up, as explained below.

### A. Splitting of Reachable Sets

One can split a zonotope $Z$ into two zonotopes $Z_1$ and $Z_2$ by splitting the $j^{th}$ generator of $Z$:

*Proposition 3:* A zonotope $Z = (c, g^{(1\dots p)})$ is split into two zonotopes $Z_1$ and $Z_2$ such that $Z_1 \cup Z_2 = Z$ and $Z_1 \cap Z_2 = Z^*$ where

$$Z_1 = (c - \frac{1}{2}g^{(j)}, g^{(1\dots j-1)}, \frac{1}{2}g^{(j)}, g^{(j+1\dots p)})$$
$$Z_2 = (c + \frac{1}{2}g^{(j)}, g^{(1\dots j-1)}, \frac{1}{2}g^{(j)}, g^{(j+1\dots p)})$$
$$Z^* = (c, g^{(1\dots j-1)}, g^{(j+1\dots p)})$$

*Proof:* First, a zonotope $(0, g^{(j)})$ that consists of the $j^{th}$ generator only, is generated. This generator can be split up into two generators:

$$(0, g^{(j)}) = (-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)}) \cup (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})$$

Adding $Z^*$ to both sides of the above statement yields

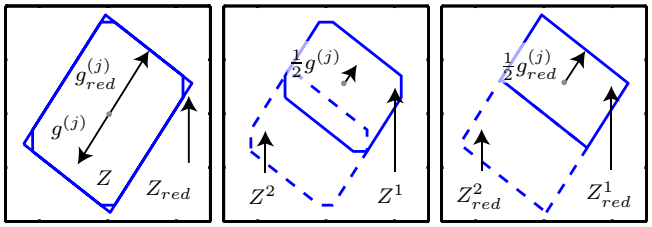
$$Z^* + (0, g^{(j)}) = Z^* + \left((-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)}) \cup (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})\right)$$
$$= \left(Z^* + (-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})\right) \cup \left(Z^* + (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})\right)$$

as $A + (B \cup C) = (A + B) \cup (A + C)$. The addition of zonotopes is performed by adding the centers and concatenating the generators (see, e.g. [18]), such that $Z = Z^* + (0, g^{(j)})$, $Z_1 = Z^* + (-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})$ and $Z_2 = Z^* + (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})$, resulting in $Z = Z_1 \cup Z_2$.
Furthermore, it can be clearly seen that

$$Z_1 \cap Z_2 = \left(Z^* + (-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})\right) \cap \left(Z^* + (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)})\right) = Z^*$$

as $(-\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)}) \cap (\frac{1}{2}g^{(j)}, \frac{1}{2}g^{(j)}) = \{0\}$. ■

The higher the order of a zonotope $Z$ is, the bigger is the overlapping zonotope $Z^*$ and consequently, the less effective is a split. For this reason, zonotopes should be reduced to a certain order with, e.g., the methods presented in [5]. The order reduction of zonotopes is performed in an over-approximated way, such that for the reduced zonotope $Z_{red}$ holds: $Z_{red} \supset Z$. The advantages and disadvantages of the order reduction are illustrated for a zonotope $Z$ in a two-dimensional space with 4 generators according to Fig. 4(a). The splitted zonotopes of the original zonotope $Z$ are denoted $Z^1$, $Z^2$ and the ones of the reduced zonotope $Z_{red}$ are denoted $Z^1_{red}$, $Z^2_{red}$ and can be found in Fig 4(b) and Fig. 4(c). The advantage of the split of the unreduced zonotope is that the splitted zonotopes cover a smaller region: $Z^1 \cup Z^2 = Z \subset Z_{red} = Z^1_{red} \cup Z^2_{red}$. However, $Z^1$ and $Z^2$ overlap more than $Z^1_{red}$ and $Z^2_{red}$: $Z^1 \cap Z^2 = Z^* \supset Z^*_{red} = Z^1_{red} \cap Z^2_{red}$ and $Z^*$, $Z^*_{red}$ are the zonotopes where the splitted generator is removed as shown in proposition 3. In order to obtain an optimal result, one has to find a compromise between the overlapping and the over-approximation of reachable sets.




(a) $Z$, $Z_{red}$ (b) $Z^1$, $Z^2$ (c) $Z^1_{red}$, $Z^2_{red}$

Fig. 4. Split of a zonotope and the corresponding reduced zonotope.

It remains to find the $j^{th}$ generator that splits the reachable set $R(k \cdot r)$ into $R^{1,j}(k \cdot r)$ and $R^{2,j}(k \cdot r)$ in an optimal way. The indices $1, 2$ distinguish the two reachable sets that result after splitting the $j^{th}$ generator. This requires a performance index for each split which is based on the Lagrange remainder. Therefore, the reachable sets $R^{1,j}([k \cdot r, (k+1) \cdot r])$ and $R^{2,j}([k \cdot r, (k+1) \cdot r]))$ for the time interval are computed based on the corresponding initial sets $R^{1,j}(k \cdot r)$ and $R^{2,j}(k \cdot r)$. The reachable sets for the time interval allow to obtain the corresponding linearization error bounds $\hat{L}^{1,j}$ and $\hat{L}^{2,j}$. The performance index $\rho^j$ for the split of the $j^{th}$ generator is computed as:

$$\rho^j = \max(\hat{L}^{1,j}/\bar{L}^j) \cdot \max(\hat{L}^{2,j}/\bar{L}^j)$$

where $\hat{L}^{1,j}/\bar{L}^j$ and $\hat{L}^{2,j}/\bar{L}^j$ are divided elementwise and $\max()$ returns the maximum value of the resulting vectors. The component $j$ with the lowest value in the performance

vector $\rho$ returns the generator that has to be split. In case the lowest performance value is greater than one, the obtained split sets have to be split again recursively. If the performance index is less than one, the linearization error limit (7) is fulfilled, such that the reachable sets for the next time step can be calculated.

### *B. Cancellation of Redundant Reachable Sets*

After a total number of $i$ splits in the time interval $[0, k\cdot r]$, $i$ reachable sets have to be computed for the next time interval $[k\cdot r, (k+1)\cdot r]$. Hence, the computational complexity of reachable sets grows linearly with the number of splits. This effect can be reduced by cancelling reachable sets that already have been reached. In order to check if a computed reachable set has been reached before, the set difference operation is used. As the set difference of two zonotopes is no zonotope anymore, the zonotopes are over-approximated by polytopes as presented in [5]. The over-approximation is performed for the reachable set segments of the past $\zeta$ time steps, where $\zeta$ can be freely chosen. If a polytope of the current time interval is empty after the set difference computation with the polytopes of the past $\zeta$ time steps, this reachable set segment is cancelled. After the cancellation, the remaining polytopes are transformed back to zonotope representation. As the cancellation of reachable sets leads to an over-approximation of the reachable set, and in addition is computationally expensive, the described procedure is only applied every $\delta \in \mathbb{N}^+$ time steps, which is set by the user.

## VII. Numerical Examples

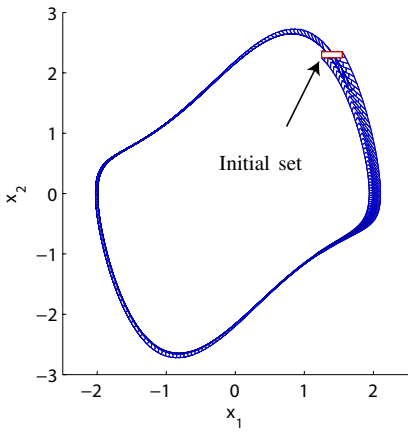
The approach is demonstrated for two examples. The Van-der-Pol oscillator is a standard example for nonlinear systems that have a limit cycle:

$$\dot{x}_1 = x_2$$
$$\dot{x}_2 = (1 - x_1^2)x_2 - x_1$$

The reachable sets are computed with a time step of $r = 0.02$ and are visualized in Fig. 5(a). The expansion vector is set to $\theta = [0.05, 0.05]^T$ and the cancellation of reachable sets is performed every $\delta = 100$ time steps. The number of reachable sets that have to be computed for a single time step is shown in Fig. 5(b). It can be seen that reachable sets are rejected after 4 and 6 time units. Further, one observes that the limit cycle is stable as the reachable set after one cycle is enclosed by the initial reachable set. This example is implemented in Matlab and the computation time is 76 seconds on a desktop computer with 3.7 GHz.

As a second example, a water tank system with uncertain inputs and parameters as illustrated in Fig. 5 is considered. The states $x_i$ are the water levels of each tank and $u$ is the water flow into the system that is controlled by measuring the water level of the last tank. This example is chosen as it can be easily formulated for different numbers of states by adding additional water tanks. The differential equation for the water level of the first tank is given by Toricelli's law:

$$\dot{x}_1 = \frac{1}{A_1}(u + v - k_1\sqrt{2gx_1})$$




(a) Van-der-Pol oscillator: reachable set.

(b) Number of computed sets per time step.

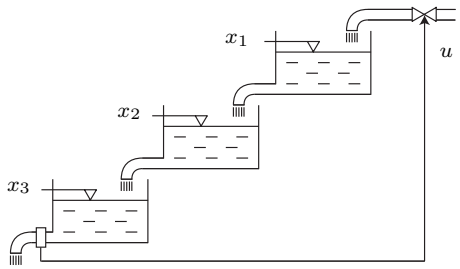


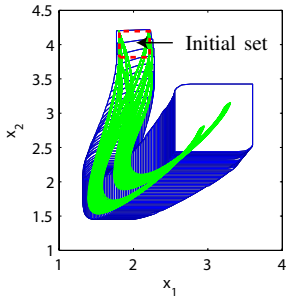

Fig. 5. Water tank system.

where $A_1$ and $k_1$ are tank specific parameters, $g$ is the gravity constant, $u$ is the inflow and $v$ is a disturbance. The inflow $u$ is chosen as $u = 0.1 + \kappa(4 - x_n)$ and $x_n$ is the water level of the last tank. The differential equation for the i$^{th}$ tank is

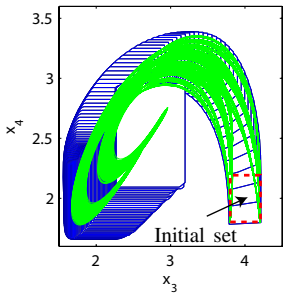
$$\dot{x}_i = \frac{1}{A_i}(k_{i-1}\sqrt{2gx_{i-1}} - k_i\sqrt{2gx_i})$$

and for simplicity, all $A_i$ are set to $A_i = 1$. The reachable set for $t \in [0, 400]$ with $v \in [-0.005, 0.005]$ and the uncertain parameters $k_i \in [0.0149, 0.015]$ for 6 tanks is shown in Fig. 6 together with exemplary trajectories starting from the vertices of the initial set [3]. The time step is chosen to $r = 4$ and the expansion vector is set to $\theta_i = 0.001$ for all $i$. Computational times for different system dimensions using the same parameters and settings than for the 6-tank system are presented in Tab. I for the case of uncertain and certain parameters $k_i$. The values are chosen as $k_i = 0.015$ in the case of certain parameters and $k_i \in [0.0149, 0.015]$ in the uncertain case. All computations have been performed using Matlab on a desktop computer with 3.7 GHz. It can be observed from Tab. I that the computation time moderately increases with the system dimension due to the efficient computation of reachable sets using zonotopes.

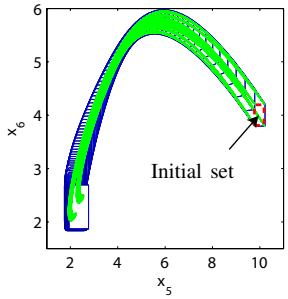
[3]The exemplary trajectories are only computed for constant $v$ and $k_i$ values although the values may be time varying.




(a) Projection onto $x_1$, $x_2$.




(b) Projection onto $x_3$, $x_4$.




(c) Projection onto $x_5$, $x_6$.

Fig. 6. Reachable sets of the tank system.

TABLE I
COMPUTATIONAL TIMES.

| Dimension $n$ | 6 | 12 | 18 | 24 | 30 |
|---|---|---|---|---|---|
| CPU-time [sec] (no uncertain parameters) | 18.1 | 64.9 | 170 | 367 | 704 |
| CPU-time [sec] (with uncertain parameters) | 26.3 | 82.6 | 201 | 417 | 796 |

## VIII. CONCLUSIONS

An approach for the efficient computation of reachable sets of high dimensional nonlinear systems has been presented. The method performs well, especially for systems with lower nonlinearity measure. In case of highly nonlinear systems, such as chaotic systems, the implementation may get stuck due to numerical problems, which is a challenge for other algorithms, too. Special characteristics are the consideration of uncertain parameters, the linearization error evaluation using the Lagrange remainder, and the possibility of splitting reachable sets represented by zonotopes. The presented approach can be included in algorithms for the reachability analysis of hybrid systems with nonlinear dynamics.

## ACKNOWLEDGEMENTS

The authors gratefully acknowledge the comments of the reviewers and the partial financial support of this work by the Deutsche Forschungsgemeinschaft (German Research Foundation) within the Transregional Collaborative Research Centre 28 ”Cognitive Automobiles”.

## REFERENCES

[1] J. Esposito, “Randomized test case generation for hybrid systems: metric selection,” in *Proc. of the 36th Southeastern Symposium of System Theory*, 2004, pp. 236–240.
[2] A. A. Julius, G. Fainekos, M. Anand, I. Lee, and G. Pappas, “Robust test generation and coverage for hybrid systems.” in *Hybrid Systems: Computation and Control*, 2007, pp. 329–342.
[3] T. Henzinger, *The theory of hybrid automata*, ser. NATO ASI Series F: Computer and Systems Sciences. Springer, 2000, vol. 170, pp. 265–292.
[4] A. Girard and C. L. Guernic, “Zonotope/hyperplane intersection for hybrid systems reachability analysis,” in *Proc. of Hybrid Systems: Computation and Control*, 2008, pp. 215–228.
[5] M. Althoff, O. Stursberg, and M. Buss, “Verification of uncertain embedded systems by computing reachable sets based on zonotopes,” in *Proc. of the 17th IFAC World Congress*, 2008, pp. 5125–5130.
[6] G. Lafferriere, G. Pappas, and S. Yovine, “A new class of decidable hybrid systems,” in *Hybrid Systems: Computation and Control*, ser. LNCS 1569. Springer, 1999, pp. 137–151.
[7] I. Mitchell, A. M. Bayen, and C. J. Tomlin, “Validating a hamilton–jacobi approximation to hybrid system reachable sets,” in *Hybrid Systems: Computation and Control*, 2001, pp. 418–432.
[8] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi, “Computational techniques for the verification and control of hybrid systems,” in *Proceedings of the IEEE*, vol. 91, 2003, pp. 986–1001.
[9] S. Prajna, “Barrier certificates for nonlinear model validation,” *Automatica*, vol. 42, pp. 117–126, 2006.
[10] T. Dang, “Approximate reachability computation for polynomial systems,” in *Hybrid Systems: Computation and Control*, 2006, pp. 138–152.
[11] A. Chutinan and B. H. Krogh, “Computational techniques for hybrid system verification,” in *IEEE Transactions on Automatic Control*, vol. 48, no. 1, 2003, pp. 64–75.
[12] T. Dang and O. Maler, “Reachability analysis via face lifting,” in *Hybrid Systems: Computation and Control*, 1998, pp. 96–109.
[13] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, “Algorithmic analysis of nonlinear hybrid systems,” *IEEE Transactions on Automatic Control*, vol. 43, pp. 540–554, 1998.
[14] O. Stursberg and S. Kowalewski, “Analysis of Controlled Hybrid Processing Systems based on Approximation by Timed Automata using Interval Arithmetics,” in *IEEE Mediterranean Conf. on Control and Automation*, 2000, pp. TA–1–3.
[15] G. Frehse, “Phaver: Algorithmic verification of hybrid systems past HyTech.” in *Hybrid Systems: Computation and Control*, 2005, pp. 258–273.
[16] E. Asarin, T. Dang, and A. Girard, “Reachability analysis of nonlinear systems using conservative approximation,” in *Hybrid Systems: Control and Computation*, 2003, pp. 20–35.
[17] Z. Han and B. H. Krogh, “Reachability analysis of nonlinear systems using trajectory piecewise linearized models,” in *Proc. of the American Control Conference*, 2006, pp. 1505–1510.
[18] A. Girard, “Reachability of uncertain linear systems using zonotopes,” in *Hybrid Systems: Computation and Control*, vol. 3414, 2005, pp. 291–305.
[19] M. Berz and G. Hoffstätter, “Computation and application of taylor polynomials with interval remainder bounds,” *Reliable Computing*, vol. 4, pp. 83–97, 1998.
[20] M. Althoff, O. Stursberg, and M. Buss, “Reachability analysis of linear systems with uncertain parameters and inputs,” in *Proc. of the 46th IEEE Conference on Decision and Control*, 2007, pp. 726–732.
[21] O. Stursberg and B. H. Krogh, “Efficient representation and computation of reachable sets for hybrid systems,” in *Hybrid Systems: Computation and Control*, ser. LNCS 2623. Springer, 2003, pp. 482–497.
[22] L. Jaulin, M. Kieffer, and O. Didrit, *Applied Interval Analysis*. Springer, 2006.