Reachability Analysis of Generalized Input-Affine Systems with Bounded Measurable Time-varying Uncertainties

Francois Bidet, Eric Goubault, Sylvie Putot

Reachability Analysis of Generalized Input-Affine Systems with Bounded Measurable Time-varying Uncertainties

François Bidet, Éric Goubault, *Member, IEEE*, and Sylvie Putot

***Abstract*—This paper presents an approach to over-approximate the reachable set of states of a system whose uncertainties are arbitrarily time-varying. Most approaches generally assume piecewise continuity or sometimes Riemann-integrability of the uncertainties. In this paper we go one step further, only assuming Lebesgue measurability, which is the weakest meaningful hypothesis. We develop our new technique, based on a decomposition of components as a difference of positive functions, for separable systems, a generalization of control-affine systems. We compare the over-approximation produced by our method with the ones obtained using the tools Flow* and CORA on simple examples, and show that correct outer-approximations of the reachable sets are computable with a high degree of precision even for these general forms of uncertainties.**

***Index Terms*—Switched systems, Time-varying systems, Uncertain systems**

I. Introduction

MANY interesting systems, such as vehicles, have there dynamic modelled as non autonomous differential equations and depend on external time-varying uncertainties. It is often unrealistic to make strong assumptions about these uncertainties, in particular when they account for physical modeling uncertainties, sensor and actuator noise, external measurable events, or phenomena that are complicated to model such as friction in contact mechanics. Despite those uncertainties, we still want to prove some guarantees about the possible behaviors of the systems: for instance, we want to keep a minimal distance between vehicles, that ensures that vehicles will not collide after an emergency breaking, whatever the environment state.

Computing the reachable states of the system is a classical way to prove such properties: knowing the set of possible states at one instant, we compute all possible states in the future. Such computations are often impossible to do exactly, but approximations can be computed. An over-approximation of the reachable set is a set guaranteed to contain all reachable states. It can be used to prove safety properties: if all states of the over-approximation satisfy the property, the system is proved safe.

The presence of external time-varying uncertainties is generally modelled either as switched systems or hybrid automata or as differential inclusions. In all these cases, a specific difficulty when trying to compute the reachable set of such systems with arbitrary time-varying uncertainties arises when different dynamics tend to interact closely. This is in particular the case in sliding mode conditions in a hybrid system, when both dynamics across a switching surface tend to bring back the trajectory towards this surface. In these cases, existing reachability approaches and tools often tend to use ad-hoc solutions that often rely on linearization and on chattering, necessarily bounded by the maximal number of switches to consider.

In this paper, we present a set-based algorithm relying on a decomposition of the vector field as a difference of positive functions to compute an over-approximation of the reachable set of a generalization of control-affine systems, in which the set of arbitrary time-varying controls or uncertainties is only bounded and measurable[1]. The first result is to prove that we do not need (piecewise) continuity conditions. The second result is algorithmical: our approach avoids inelegant and inefficient chattering approaches to reachability, while being sound for a very general class of time-varying uncertainties. We then demonstrate on various examples that this approach can yield even better over-approximations than some state-of-the-art tools, while under more general hypotheses.

The paper is organized as follows. In Section IV, we introduce the problem of interest. Section V presents the main result at the basis of the computation of an over-approximation of the reachable set. In Section VI, we introduce Taylor models as set representations. In Section VII, we detail the algorithm and present in Section VIII an optimal solution to the decomposition of the vector field that appears in this algorithm. Finally, we demonstrate in Sections IX and X our algorithm on various examples and compare it to state-of-the-art tools.

II. Related work

Our work is linked, first, to the theory of switched systems, see e.g. [2], and in particular of arbitrary switched systems. An old result (see [3, Theorem 7]) states that given a compact set $\mathcal{U}$, an ordinary differential equation (ODE) $\dot{x} = f(x, u)$, with f a continuous mapping from

Work supported by DGA AID project “Essaims de drones”

[1] Which, in some sense, is the weakest condition one may hope for: exhibiting a non-mesurable set of switching events requires going past classical Zermelo-Fraenkel set theory without the axiom of choice [1].

$\mathbb{R}^n \times \mathbb{R}^k \to \mathbb{R}^n$ and $u : \mathbb{R} \to \mathbb{R}^k$ measurable, has the same solutions as the differential inclusion $\dot{x} \in f(x, \mathcal{U})$ if for all x, $f(x, \mathcal{U})$ is convex and for all time t, $u(t) \in \mathcal{U}$. However, it does not give any procedure to compute the set of solutions or an approximation and no proof was found stating the convexified differential inclusion produces the same set of solutions. Generalizing this result to this context, and making it practical, is one of the aims of this paper.

The center of our work is reachability analysis of hybrid systems. Many papers focus on the reachability problem for linear vector fields: [4] and [5] propose over-approximations of the reachable states over time of linear dynamics with additive uncertainties using support functions, [6] handles uncertain linear dynamics $\dot{x}(t) = A(t)x(t) + u(t)$ with A and u piecewise continuous, i.e. Riemann-integrable on intervals. We consider more general (measurable) uncertainties and non-linear dynamics.

Some authors consider the more general ordinary differential equations $\dot{x}(t) = f(x(t), u(t))$ but use various hypotheses to enclose the original dynamic by a differential inclusion with a specific simpler form. For instance, the approach of [7] is based on linearizations of the dynamic. The more recent [8], assuming f to be differentiable, uses polynomial approximants, implemented in the MATLAB toolbox CORA, to which we will be comparing our results. Similarly, [9] assumes for all u, $x \mapsto f(x, u)$ is $\mathcal{C}^2(\mathbb{R}^n)$, without assumptions on $u \mapsto f(x, u)$, which is still much more than we assume.

Finally, some authors as [10], exploit different hypotheses on f, such as minimal Lipschitz condition or differentiability. This allows them to compute errors of different orders between the solutions of initial dynamics and the ones of similar dynamic in which the uncertainties are replaced by specific time varying functions.

The closest approach to ours is the approach taken by [11] in the Flow* tool. It handles time-varying uncertainties by replacing their occurrences by intervals and by using Taylor models to compute over-approximations of the solutions of the resulting differential inclusions, only assuming Lipschitz condition on f. Although we believe their approach would most probably be correct under our weaker assumptions as well, this does not seem to be explicitly stated anywhere, to the best of our knowledge.

III. Notations

Sets are denoted by rounded capital letters (e.g. $\mathcal{X}$). The powerset is denoted by the rounded capital letter $\mathscr{P}$: given a set $\mathcal{X}$, $\mathscr{P}(\mathcal{X})$ is the set of all subsets of $\mathcal{X}$.

Sets of consecutive integers are denoted as real intervals but with double squared brackets. E.g.:

$$[\![a, b]\!] = \{n \mid n \in \mathbb{N},\ a \leq n \leq b\} = \mathbb{N} \cap [a, b]$$

All integrals are Lebesgue integrals.

IV. Problem formulation

We consider particular differential systems with arbitrary time-varying bounded uncertain inputs:

$$\dot{x}(t) = f(t, x(t), u(t)) \tag{1}$$

with $\dot{x}$ denoting the vector of L^1 weak derivatives of the components of the state x that takes values in $\mathcal{X} \subset \mathbb{R}^n$, u denoting some uncertainties which takes values in the bounded set $\mathcal{U} \subset \mathbb{R}^k$. Solutions of (1) are considered in the sense of Carathéodory, i.e. for almost all time $t \in [0, T]$.

The particular systems we will be studying are those that can be written:

$$f(t, x(t), u(t)) = g(u(t)) \cdot h(t, x(t)) \tag{2}$$

with h a vector-valued continuous function from $[0, T] \times \mathcal{X} \to \mathbb{R}^m$ and g a matrix-valued continuous function from $\mathcal{U} \to \mathbb{R}^n \times \mathbb{R}^m$. We assume $x(0) = x_0 \in \mathcal{X}_0$, with $\mathcal{X}_0 \subset \mathcal{X}$ the set of possible initial states, and the input u to be measurable and taking values in a bounded set $\mathcal{U} \subset \mathbb{R}^k$.

We call such systems separable with respect to the arbitrary time-varying bounded uncertain inputs u. They are a generalization of control-affine systems (see [12]).

Carathéodory's existence theorem guarantees the existence of solutions $y_{x_0,u}$ to the system (see [13, Theorem 1]) when we assume that for all possible functions u taking values in $\mathcal{U}$, there exists a Lebesgue-integrable function $m : [0, T] \to \mathbb{R}_+$ such that $\forall (x, t) \in \mathcal{X} \times [0, T],\ \|f(t, x, u(t))\| \leq m(t)$. To guarantee the uniqueness of the solution (see [13, Theorem 2]), we also assume for all inputs u, there exists a Lebesgue-integrable function $k : [0, T] \to \mathbb{R}_+$ such that $\forall (x_1, x_2, t) \in \mathcal{X} \times \mathcal{X} \times [0, T],\ \|f(t, x_1, u(t) - f(t, x_2, u(t))\| \leq k(t) \|x_1 - x_2\|$.

Our goal is to determine an over-approximation of the reachable set of the system on a time interval $[0, T]$, given the set $\mathcal{X}_0$ of all possible initial states and a bounded set $\mathcal{U}$ of inputs value: we want to define a set-valued function φ such that for all $t \in [0, T]$, $\{y_{x_0,u}(t) \mid x_0 \in \mathcal{X}_0, u : [0, T] \to \mathcal{U}\} \subset \varphi(t)$.

V. Reachability theorem

Lemma 1: Let $\mathcal{U}$ be a bounded subset of $\mathbb{R}$ and $g_{i,j}$ be a Lebesgue-integrable function from $\mathcal{U} \to \mathbb{R}$. Let h_j be a Lebesgue-integrable function from $[0, T] \to \mathbb{R}$ and consider any decomposition of h_j as a difference of positive functions, i.e. $h_j = h_j^+ - h_j^-$. Consider any interval over-approximation $\mathcal{C}$ of the closure of the convex hull of $\{g_{i,j}(v) \mid v \in \mathcal{U}\}$. Then for all Lebesgue-integrable functions $u : [0, T] \to \mathcal{U}$, we have:

$$\int_0^T g_{i,j}(u(s)) h_j(s)\, ds \in \left\{ u_1 \int_0^T h_j^+(s)\, ds \right.$$
$$\left. - u_2 \int_0^T h_j^-(s)\, ds \;\middle|\; u_1 \in \mathcal{C},\ u_2 \in \mathcal{C} \right\}$$

Proof: Let $[a, b] = \mathcal{C}$. For all $s \in [0, T]$, we have

$$a h_j^+(s) - b h_j^-(s) \leq g_{i,j}(u(s)) h_j(s) \leq b h_j^+(s) - a h_j^-(s)$$

Then, integrating each part, we obtain

$$a \int_0^T h_j^+(s)\, ds - b \int_0^T h_j^-(s)\, ds \leq \int_0^T g_{i,j}(u(s)) h_j(s)\, ds$$

$$\int_0^T g_{i,j}(u(s)) h_j(s)\, ds \leq b \int_0^T h_j^+(s)\, ds - a \int_0^T h_j^-(s)\, ds$$

Let I_- denote the lower bound and I_+ denote the upper bound. Then there exists $\alpha \in [0,1]$ such that $\int_0^T g_{i,j}(u(s))h_j(s)\,ds = \alpha I_- + (1-\alpha)I_+$. Let $u_1 = \alpha a + (1-\alpha)b$ and $u_2 = \alpha b + (1-\alpha)a$, we have $u_1 \in [a,b]$ and $u_2 \in [a,b]$. ■

Remark 1: We cannot directly replace the function u by an element of $\mathcal{C}$ without decomposition. This is illustrated by the following example. Let $h(t) = g(u(t)) = -1$ if $t < 1$ and $h(t) = g(u(t)) = 1$ if $t \geq 1$. We have $\mathcal{C} = [-1,1]$ but

$$\int_0^2 g(u(s))h(s)\,ds = 2 \qquad \forall \alpha \in \mathcal{C},\ \int_0^2 h(s)\,ds = 0$$

So we have $\int_0^2 g(u(s))h(s)\,ds \notin \left\{\alpha \int_0^2 h(s)\,ds \middle| \alpha \in \mathcal{C}\right\}$.

Remark 2: This lemma is only valid for one-dimensional systems. To illustrate this, let us consider:

$$\forall t \in [0,2],\ h(t) = \begin{pmatrix} t \\ t^2 \end{pmatrix} \quad g(u(t)) = \begin{pmatrix} u(t) & 0 \\ 0 & u(t) \end{pmatrix}$$

with for $t \leq 1$, $u(t) = -1$ and for $t > 1$, $u(t) = 1$. We have:

$$\int_0^2 g(u(s))h(s)\,ds = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.75 \end{pmatrix} \int_0^2 h(s)\,ds$$

and $\begin{pmatrix} 0.5 & 0 \\ 0 & 0.75 \end{pmatrix}$ is not in the convex hull of the image of $g(u(t))$, which is $\left\{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \middle| \alpha \in [-1,1]\right\}$.

Consider now the higher-dimensional case $h : [0,T] \times \mathcal{X} \to \mathbb{R}^m$. Let us suppose $h = h^+ - h^-$, i.e. each component of h is decomposed as a difference of positive functions h^+ and h^-. Given two matrices $A = (a_{i,j})$ and $B = (b_{i,j})$ such that for all $(i,j) \in [\![1,n]\!] \times [\![1,m]\!]$, $a_{i,j}$ and $b_{i,j}$ belong to the interval $C_{i,j} \supset \{g_{i,j}(v) | v \in \mathcal{U}\}$ and x_0 the initial state, we define the following operator on the set of functions $p : [0,T] \to \mathcal{X}$:

$$\mathbb{P}_{x_0,A,B}(p) := t \mapsto x_0 + A \int_0^t h^+(s, p(s))\,ds - B \int_0^t h^-(s, p(s))\,ds \qquad (3)$$

This operator is the counterpart of Picard's operator used in the proof of the Picard-Lindelöf theorem when the right-hand side of the ODE is continuous in time. In the sequel, we call this operator the modified Picard operator. This operator can be naturally lifted on set-valued functions $\varphi : [0,T] \to \mathscr{P}(\mathcal{X})$.

Let $\varphi_{x_0,A,B}$ be a bounded set-valued function from $[0,T]$ to $\mathscr{P}(\mathbb{R}^n)$ such that $\forall t \in [0,T]$, $\mathbb{P}_{x_0,A,B}(\varphi_{x_0,A,B})(t) \subset \varphi_{x_0,A,B}(t)$. Such functions always exist for small enough $T \geq 0$, because h^+ and h^- are continuous thus bounded on every compact set. We will furthermore suppose for all $t \in [0,T]$, the set $\varphi_{x_0,A,B}(t)$ is closed and convex, which will be the case using Taylor models (cf. Section VI). Let φ be the union of all fixed-point set-valued functions $\varphi_{x_0,A,B}$:

$$\varphi = t \mapsto \bigcup_{x_0 \in \mathcal{X}_0,\ a_{i,j} \in \mathcal{C}_{i,j},\ b_{i,j} \in \mathcal{C}_{i,j}} \varphi_{x_0,A,B}(t)$$

Theorem 1: For all $t \in [0,T]$, $\varphi(t)$ is an over-approximation of the reachable set at time t of (1).

Proof: Let y be a solution of the dynamics with uncertainties u and initial state x_0. Then y has to satisfy the integral equation for all $t \in [0,T]$

$$y(t) = x_0 + \int_0^t g(u(s)) \cdot h(s, x(s))\,ds$$

Using Lemma 1 on each component of y, there exist matrices A and B such that $y = \mathbb{P}_{x_0,A,B}(y)$. Because for all $t \in [0,T]$, $\varphi_{x_0,A,B}(t)$ is closed and convex, using Schauder's fixed-point theorem as in [14, section 3], we have $y(t) \in \varphi_{x_0,A,B}(t) \subset \varphi(t)$. ■

We thus obtain a way to check that a set-valued function parametrized by the initial vector and the uncertainties values is an over-approximation of the solutions set. A direct application of this result will be presented in Section VII.

VI. Set representation

We represent the uncertainties on time dependent variables with Taylor models (see [15] and [11]). A Taylor model is defined on a domain $\mathcal{D}$ as a pair $\mathrm{TM}(p, \mathcal{R})$ consisting of a polynomial to encode an approximation of the dependence in the initial conditions x_0 and time t (or even more parameters) and a set $\mathcal{R}$ (called remainder) to encode the error between this polynomial and the actual function: $\mathrm{TM}(p, \mathcal{R})(x_0, t) = \{p(x_0,t) + r \mid r \in \mathcal{R}\}$. It is convenient to use intervals as representation of the remainder. A Taylor model $\mathrm{TM}(p, \mathcal{R})$ is an over-approximation of a function φ if all possible values of φ are in the corresponding evaluation of the Taylor model:

$$\forall x \in \mathcal{D},\ \exists r \in \mathcal{R},\ \varphi(x) = p(x) + r \qquad (4)$$

We can soundly interpret operations on Taylor models (see [16] and [14]):

$$\mathrm{TM}(p_1, \mathcal{R}_1) + \mathrm{TM}(p_2, \mathcal{R}_2) = \mathrm{TM}(p_1 + p_2, \mathcal{R}_1 + \mathcal{R}_2)$$

Subtraction is handled similarly as addition.

$$\mathrm{TM}(p_1, \mathcal{R}_1) \cdot \mathrm{TM}(p_2, \mathcal{R}_2) = \mathrm{TM}(p_1 \cdot p_2,\ [p_1] \cdot \mathcal{R}_2 + \mathcal{R}_1 \cdot [p_2] + \mathcal{R}_1 \cdot \mathcal{R}_2)$$

with $[p]$ the interval enclosure of the polynomial p over its domain of definition. And, for all $t \in [0,T]$

$$\int_0^t \mathrm{TM}(p, \mathcal{R})(s)\,ds = \mathrm{TM}\left(\int_0^t p(s)\,ds,\ \mathcal{R} \cdot [0,T]\right)$$

Taylor models provide bounded, closed and convex set-valued functions (see [14]). Therefore, Taylor models will be used in Section VII to compute set-valued functions $\varphi_{x_0,A,B}$ to apply Theorem 1.

On the practical side, Taylor models are convenient for implementation purposes since we can also handle floating point arithmetic errors by replacing coefficients of the polynomial part by guaranteed intervals (see [17]).

VII. Algorithm

In this section, we assume all variables are unidimensional variables: $\mathcal{X}_0 \subset \mathbb{R}$ and $\mathcal{U} \subset \mathbb{R}$. We can generalize the algorithm to the general multidimensional case by applying each step to each dimension.

To compute an over-approximation of the reachable set of system (1), we will use Taylor models as a representation for sets, with a given maximal order. We need a function to convert an uncertainty or a state variable to a Taylor model. We call *Lift* such a function which simply consists in defining a Taylor model with a symbolic variable as polynomial and a null set as remainder.

The algorithm consists in four steps:

Step 1, a priori global enclosure:
Given the initial set of states, we compute a rough enclosure of the solution on the entire time step, e.g. using contraction of intervals.

Step 2, functions' decomposition:
Using the a priori enclosure, we decompose each function h_i (for $i \in [\![1, m]\!]$) as a difference of positive functions h_i^+ and h_i^- (see Section VIII).

Step 3, polynomial expansion:
We start by computing the (multivariate) polynomial part of the expected Taylor model of the solution. We start with a simple Taylor model $\varphi_0(x_0, t) = \mathrm{TM}\left(x_0,\, [0]\right)$ and we iterate the operator defined in (3), with matrices A and B encoded as Taylor models returned by the *Lift* function, until the polynomial part of the Taylor model, depending on x_0, t, A, and B, reaches a fixed-point due to truncation.

Step 4, valid remainder computation:
Given $\mathrm{TM}\left(p,\, I\right)$ the result of the polynomial expansion, we have to guess a remainder $\mathcal{R}$ such that $\mathbb{P}\left(\mathrm{TM}\left(p,\, \mathcal{R}\right)\right) \subset \mathrm{TM}\left(p,\, \mathcal{R}\right)$. We can for example enlarge I until we get such a contraction by $\mathbb{P}\left(\right)$ and then iterate $\mathrm{TM}\left(p,\, I_{n+1}\right) = \mathbb{P}\left(\mathrm{TM}\left(p,\, I_n\right)\right)$ until reaching a fixed-point to get a tighter over-approximation.

VIII. Function decomposition

The second step of the algorithm consists in decomposing the functions h_i of the dynamics as differences of positive functions.

Consider a function $h : \mathcal{X} \to [a, b]$ from a convex compact domain $\mathcal{X} \subset \mathbb{R}^d$ to an interval $[a, b]$. If $a \geq 0$ or $b \leq 0$, the decomposition we are looking for is trivial. We assume now $a < 0 < b$. A simple possibility is to shift the function in the positive or the negative side:

$$h(x) = (h(x) - a) - (-a) \quad \text{(shifted in the positive side)}$$
$$h(x) = (b) - (b - h(x)) \quad \text{(shifted in the negative side)}$$

We can also use an affine transformation:

$$h(x) = \left(\frac{b}{b-a}h(x) - \frac{ab}{b-a}\right) - \left(\frac{a}{b-a}h(x) - \frac{ab}{b-a}\right) \tag{5}$$

Of course we can imagine many other valid decompositions, e.g. $h(x) = (h(x) + 0.5)^2 - \left(h(x)^2 + 0.25\right)$.

The best decompositions are those that minimize the over-approximation of the Taylor Model returned by the algorithm. Because we are using Taylor Models with intervals as remainders, we want to minimize $\|h^+\|_1 + \|h^-\|_1$. It can be proven that the affine decomposition (5) minimizes this quantity.[2]

TABLE I
Decompositions and Resulting Over-Approximations

Decomposition	Over-Approximation
$(h_1 + 0.1) - 0.1$	$[-0.04, 0.04]$
$(0.5h_1 + 0.05) - (0.05 - 0.5h_1)$	$[-0.02, 0.02]$
$(h_1 + 0.5)^2 - (h_1^2 + 0.25)$	$[-0.102, 0.102]$
$(h_1 + 0.25)^2 - (h_1 - 0.25)^2$	$[-0.027, 0.027]$

For example, let $\dot{x}(t) = (0.1 - t)u(t)$ with $x(0) = 0$ and for all $t \in [0, 0.2]$, $u(t) \in [-1, 1]$. We have $h_1(x, t) = (0.1 - t)$ and for all $t \in [0, 0.2]$, $h_1(x, t) \in [-0.1, 0.1]$. We compare over-approximations produced by our algorithm using different decompositions in the Table I. We note that the affine decomposition given in (5) produces the tightest over-approximation on this example, even with respect to some polynomial decompositions.

IX. A detailed example

In this section, we detail the steps of the algorithm of Section VII on a simple one-dimensional system in which the derivative is independent of its state, similar to Example 1 in [9]:

$$\left\{\begin{array}{l}\dot{x}(t) = (0.1 - t)u(t)\\ x(0) = 0\end{array}\right. \text{with} \left\{\begin{array}{l}u(t) \in [-1, 1]\\ t \in [0, 0.2]\end{array}\right. \tag{6}$$

(we refer to this example as "Simple" in Section X).

We use this example to illustrate the importance of handling time-varying uncertainties during the integration's step: if u is constant over $[0, 0.2]$, $x(0.2) = 0$ whereas if u can arbitrarily vary over $[0, 0.2]$, $x(0.2)$ can have non zero values. We can deduce the exact reachable set using the fact the minimal (*resp.* maximal) value is reached for always minimal (*resp.* maximal) derivative: $x(t) \in \left[-0.1t + 0.5t^2, 0.1t - 0.5t^2\right]$ for $t \in [0, 0.1]$ and $x(t) \in \left[-0.01 + 0.1t - 0.5t^2, 0.01 - 0.1t + 0.5t^2\right]$ for $t \in [0.1, 0.2]$. So we have $x(0.2) \in [-0.01, 0.01]$.

We compute the over-approximation with one integration step over $[0, 0.2]$. The first step of the algorithm is the computation of an *a priori* global enclosure of the solution on the entire integration step in order to be able to decompose the dynamics. Here, the dynamics does not depend on the state so the *a priori* enclosure is useless.

Using interval arithmetic, we can over-approximate the image of $t \mapsto 0.1 - t$ by $[-0.1, 0.1]$ and deduce the decomposed dynamics (*cf.* Section VIII):

$$\dot{x}(t) = (0.1 - 0.5t)u(t) - (0.5t)u(t)$$

Now, we compute with Taylor models arithmetic and replace all occurrences of u by fresh variables to obtain the following iterator:

$$\mathbb{P}_{x_0,u_1,u_2}\left(\varphi\right)(t) = x_0 + u_1 \int_0^t (0.1 - 0.5s)\, ds - u_2 \int_0^t (0.5s)\, ds$$

[2] Such a proof is presented in `http://www.lix.polytechnique.fr/Labo/Francois.Bidet/Ressources/Appendices_LCSS2021.zip`

Starting with $\varphi_0 = \mathrm{TM}(x_0, [0])$, $x_0 = 0$, $t \in [0, 0.2]$, $u_1 \in [-1, 1]$ and $u_2 \in [-1, 1]$, we detect a fixed point of the polynomial after two iterations: $\varphi_{n \geq 1}(t) = \mathrm{TM}\left(0.1u_1 t - 0.25(u_1 + u_2)t^2, [0]\right)$.

We notice we also reach a fixed-point with Taylor models. We have therefore the over-approximation:

$$x(t) \in \left\{0.1u_1 t - 0.25(u_1 + u_2)t^2 \;\middle|\; (u_1, u_2) \in [-1, 1]^2\right\}$$

which can be rewritten $x(t) \in [-0.1t, 0.1t]$. We deduce $x(0.2) \in [-0.02, 0.02]$, which is twice as large as the exact reachable set $[-0.01, 0.01]$.

X. Comparison with other tools

We compare here our algorithm with results of the reachability tools Flow* [11] and CORA [8]. Our implementation has not been optimized and the comparison is merely intended to illustrate the correctness and accuracy of the method and not to demonstrate its efficiency.

We implemented the algorithm of Section VII. We then iterate over multiple integration steps: the over-approximation of a Taylor model obtained at the end of the current time step becomes the initial domain for the next integration step after being truncated so as to bound the number of monomial terms (in these examples the bound is 4). This is done by keeping the terms with larger absolute coefficients and over-approximating the truncated ones in the remainder. We consider fixed time-step for easier comparison with other tools.

We compare below the three tools on simple examples for which we are able to compute the exact reachable set.

The first example is the one presented in Section IX with a unique time-step of integration, equation (6).

The second example is a variation of the classical decreasing exponential where we added a non-linearity using a second state variable:

$$\left\{\begin{array}{l} \dot{x}(t) = -x(t) - x(t)y(t)u(t) \\ \dot{y}(t) = -y(t) \\ x(0) = 1;\ y(0) = 2 \end{array}\right. \quad \text{with} \left\{\begin{array}{l} u(t) \in [-1, 1] \\ t \in [0, 5] \end{array}\right.$$

(we refer to this example as "NonLinear" in Table II).

There are no uncertainties on the dynamic of y, we can thus compute its exact value: $y(t) = 2\mathrm{e}^{-t}$. Replacing y by its expression in the dynamic of x, we obtain a one-dimensional dynamic and we can compute the exact reachable set: $x(t) \in \left[\mathrm{e}^{2\left(\mathrm{e}^{-t}-1\right)-t}, \mathrm{e}^{2\left(1-\mathrm{e}^{-t}\right)-t}\right]$.

The third example is such that multiple equilibrium points exist depending on the uncertain value:

$$\left\{\begin{array}{l} \dot{x}(t) = u(t) - x(t) \\ x(0) = 3 \end{array}\right. \quad \text{with} \left\{\begin{array}{l} u(t) \in [0, 1] \\ t \in [0, 20] \end{array}\right.$$

(we refer to this example as "Switching" in Table II).

This is a one-dimensional dynamics, thus using the fact the minimal (*resp.* maximal) value is reached for always minimal (*resp.* maximal) derivative, we obtain the exact reachable set: $x(t) \in [4\mathrm{e}^{-t} - 1, 2\mathrm{e}^{-t} + 1]$.

TABLE II
Areas of the over-approximations of $\boldsymbol{x(t)}$

	CORA	Flow*	prototype	exact
Simple	0.024	0.024	0.008	0.004
NonLinear	5.956	7.735	4.866	3.576
Switching	23.325	26.814	19.483	19.000
Dubins	0.114	0.114	0.099	0.086

TABLE III
Parameters for the different examples

	time-step	Taylor models' order
Simple	0.02	3
NonLinear	0.05	5
Switching	0.1	3
Dubins	0.01	5

The fourth and last example is a variation of the Dubins car model with controls as uncertainties:

$$\left\{\begin{array}{l} \dot{x}(t) = u_1(t)\cos(z(t)) \\ \dot{y}(t) = u_1(t)\sin(z(t)) \\ \dot{z}(t) = u_2(t) \\ x(0) = y(0) = z(0) = 0 \end{array}\right. \quad \text{with} \left\{\begin{array}{l} u_1(t) \in [0.9, 1] \\ u_2(t) \in [0, 1] \\ t \in [0, 1] \end{array}\right.$$

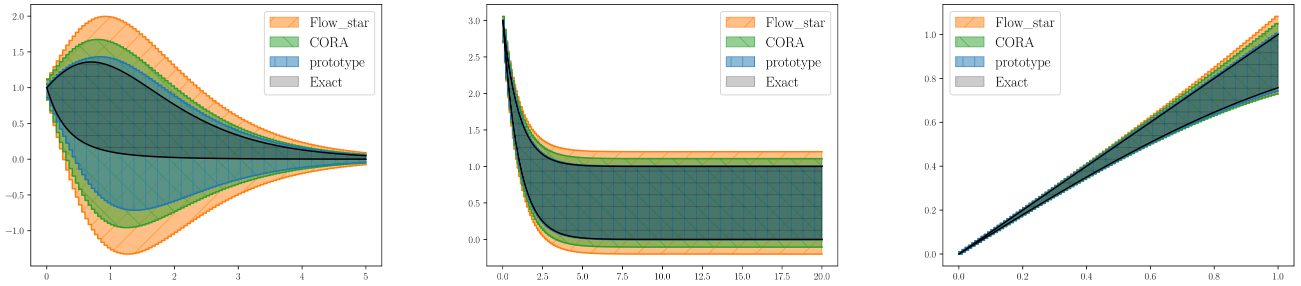
(we refer to this example as "Dubins" in Table II).

We can trivially compute the exact reachable set of $z(t) \in [0, t]$ and we deduce the exact reachable set of x: $x(t) \in [0.9\sin(t), t]$.

For each example, we fix the same reasonable small time-step for all the tools. The parameters for each example are gathered in Table III. We tried in Flow* to raise further the Taylor models' orders to improve the precision but without obtaining significantly different results. In the same way, we set the zonotopes' order's limit in CORA to quite high values in the hope of improving the precision, without obtaining significantly different results.

We use the area of the over-approximation of the first state variable over time to compare the precision of each tool. These areas are computed from the outputs of the tools, the over-approximation of the first state variable with respect to the time. We also give the area of the exact reachable set. Notice we consider for example "Simple", the bounded box of the reachable set, because it is what we use as over-approximation for CORA and our prototype. We gather the different areas in Table II. Our prototype produces tighter over-approximation on all these examples.

We also represent graphically the results of the different tools. Figure 1a shows the over-approximations produced by the three tools and the exact reachable set of the first component with respect to the time for the example "Nonlinear". Similar graphs are drawn in Figure 1b for example "Switching" and in Figure 1c for example "Dubins". They confirm our prototype exhibits a more precise over-approximation compared to CORA and Flow*, even very close to the exact solution on the "Switching" example. This is achieved even though ensuring the result is guaranteed for a larger class of uncertainties, i.e. measurable uncertainties.



(a) Nonlinear

(b) Switching

(c) Dubins car

Fig. 1. Reachable set of x with respect to time for each example and each tool

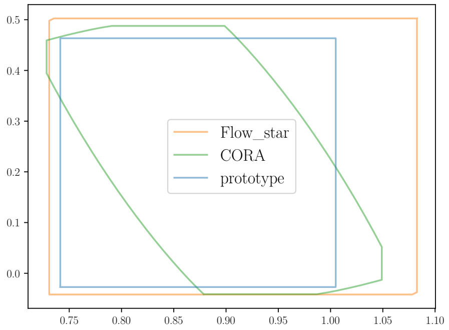


Fig. 2. Reachable set on time interval $[0.99, 1]$ for example "Dubins": y with respect to x

However, while the over-approximations of the projection on each dimension with respect to the time are tighter with our prototype, we lose dependencies between components, as shown on Figure 2.

XI. Conclusion

We presented an approach based on a simple and systematic decomposition of the vector field as a difference of positive functions to compute over-approximations of the reachable set of non-linear initial value problems that we call separable with respect to the uncertainties. We demonstrated the good precision of an implementation of our algorithm with Taylor models compared to the state-of-the-art tools Flow* and CORA. This leads us to think that the decomposition we propose, which guarantees correctness of results when handling uncertain inputs that are not Riemann-integrable, is not too conservative despite its simplicity. Measurable uncertainties such as considered in this work are a good abstraction of uncertainties generated by guards on states obtained for general switched or hybrid systems. The practical application of our methods for analysing precisely and efficiently the complete class of hybrid systems is left for future work.

References

[1] R. Solovay, “A model of set-theory in which every set of reals is lebesgue measurable*,” *Annals of Mathematics*, vol. 92, p. 1, 1970.

[2] D. Liberzon, *Switching in Systems and Control*, ser. Systems & control. Birkhauser, 2003.

[3] J. Nieuwenhuis, “Some remarks on set-valued dynamical systems,” *The ANZIAM Journal*, vol. 22, no. 3, pp. 308–313, 1981.

[4] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, “SpaceEx: Scalable Verification of Hybrid Systems,” in *Computer Aided Verification*, ser. Lecture Notes in Computer Science, G. Gopalakrishnan and S. Qadeer, Eds. Berlin, Heidelberg: Springer, 2011, pp. 379–395.

[5] C. Le Guernic and A. Girard, “Reachability analysis of linear systems using support functions,” *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 250–262, May 2010.

[6] M. Althoff, C. Le Guernic, and B. H. Krogh, “Reachable set computation for uncertain time-varying linear systems,” in *Proceedings of the 14th international conference on Hybrid systems: computation and control - HSCC ’11*. Chicago, IL, USA: ACM Press, 2011, p. 93.

[7] M. Althoff, O. Stursberg, and M. Buss, “Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization,” in *2008 47th IEEE Conference on Decision and Control*. IEEE, 2008, pp. 4042–4048.

[8] M. Althoff, “Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets,” in *Proceedings of the 16th international conference on Hybrid systems: computation and control*, 2013, pp. 173–182.

[9] M. Rungger and M. Zamani, “Accurate reachability analysis of uncertain nonlinear systems,” in *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*. Porto Portugal: ACM, Apr. 2018, pp. 61–70.

[10] S. Z. Gonzalez, P. Collins, L. Geretti, D. Bresolin, and T. Villa, “Higher order method for differential inclusions,” *arXiv preprint arXiv:2001.11330*, 2020.

[11] X. Chen, “Reachability analysis of non-linear hybrid systems using taylor models,” Ph.D. dissertation, Fachgruppe Informatik, RWTH Aachen University, 2015.

[12] Y. Chitour, F. Jean, and E. Trélat, “Singular trajectories of control-affine systems,” *SIAM Journal on Control and Optimization*, vol. 47, no. 2, pp. 1078–1095, 2008.

[13] A. F. Filippov, *Differential Equations with Discontinuous Righthand Sides*, ser. Mathematics and Its Applications. Dordrecht: Springer Netherlands, 1988, vol. 18.

[14] M. Berz and K. Makino, “Verified integration of odes and flows using differential algebraic methods on high-order taylor models,” *Reliable computing*, vol. 4, no. 4, pp. 361–369, 1998.

[15] K. Makino and M. Berz, “Remainder differential algebras and their applications,” *Computational differentiation: techniques, applications and tools*, pp. 63–74, 1996.

[16] M. Berz and G. Hoffstätter, “Computation and application of taylor polynomials with interval remainder bounds,” *Reliable Computing*, vol. 4, no. 1, pp. 83–97, 1998.

[17] N. Revol, K. Makino, and M. Berz, “Taylor models and floating-point arithmetic: proof that arithmetic operations are validated in cosy,” *The Journal of Logic and Algebraic Programming*, vol. 64, no. 1, pp. 135–154, 2005.