Forward inner-approximated reachability of hybrid systems

E. Goubault
LIX, Ecole Polytechnique, CNRS,
Université Paris-Saclay, 91128 Palaiseau,
France
goubault@lix.polytechnique.fr

S. Putot
LIX, Ecole Polytechnique, CNRS,
Université Paris-Saclay, 91128 Palaiseau,
France
putot@lix.polytechnique.fr

ABSTRACT

- forward inner- and outer- approximations of the set of states reachable by an uncertain hybrid systems, that is with uncertain initial conditions and parameters.
- little studied and difficult problem, the small number of existing approaches mostly attack the dual problem aof backward inner-apporximated reachability
- based on a combination of Taylor based methids for teh solution of IVP and generalized mean value theorem for inner-approximation [8]
- experiments with matlab implementation

Categories and Subject Descriptors

F.1.1 [**Theory of Computation**]: Computation by Abstract Devices; G.1.7 [**Mathematics of Computing**]: Numerical Analysis; G.1.0 [**Numerical Analysis**]: General—*Interval arithmetic,Numerical algorithms*
; G.4 [**Mathematical Software**]: Reliability and robustness

Keywords

Inner-approximation, Taylor models, affine arithmetic, modal intervals

1. INTRODUCTION

The verification of software-enabled real-time control systems requires reasoning about non-linear hybrid systems, that exhibit both discrete and continuous behavior. Computing the reachable set of such systems is a central component of model-checking. While the exact reachability problem for hybrid systems is generally undecidable, in the recent years there has been much progress in the computation of outer-approximations of the reachable set, first for the verification of affine hybrid systems [], but also for the more general class of non-linear hybrid systems []. An outer-approximation makes possible the verification of safety properties of such systems. However, the verification of more general temporal properties, such as viability [] properties for instance, or the falsification of safety properties, also require inner-approximating the reachable set, that is computing states that are definitely reached.

Methods for inner-approximated reachability are far less developed, and especially in the non-linear case, since most methods in the non-linear case rely on conservative linearizations, which necessarily produce outer approximations.

HSCC'17, April 17–20, 2017, Pittsburgh, Pennsylvania

ISBN 978-1-4503-2138-9.

DOI: http://dx.doi.org/XXXX.XXXX

Contributions:.

In previous work [8,9], we proposed an approach for direct forward inner-approximated reachability of

— Attention au double-blind review

discrete dynamical systems, and gave a few hints as to how we would handle continuous and hybrid systems. We build here on this previous work.

- computing inner-approximations of the flow of uncertain IVP: for a continuous dynamical system, combining Taylor based outer-approximation, on time intervals, of the solution of the initial value problem, and its jacobian with respect to initial value, with a generalized mean value theorem as used in [8], but applied here to the solution of the IVP, yielding both inner and outer approximations of the set of states reachable from a set of values of initial conditions and uncertain parameters
- guards
- experiments with a matlab implementation and tentative comparisons to existing work (but dual approaches - mostly bacward inner reachability ? - combination to be studied ?)

2. PROBLEM STATEMENT

We will consider in this article, general systems of parametric ODEs, i.e. possibly non-linear, or even non-polynomial, of the form :

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

where the continuous variables x belong to a state-space domain $\mathcal{D} \subseteq \mathbb{R}^n$, the (constant) parameters p belong to the uncertainty domain $\mathcal{P} \subseteq \mathbb{R}^p$, and $f : \mathcal{D} \times \mathcal{P} \times \mathbb{R}^+ \to \mathcal{D}$ is assumed sufficiently smooth on $\mathcal{D} \subseteq \mathbb{R}^n$ (at least $\mathcal{C}^1$, and sometimes more when we will use higher Taylor models, see Section 3.5).

Introducing the new state variable $z = (x, p, t)$ with $\dot{z} = (\dot{x}, 0, 1)$, and defining $\mathcal{Z} = \mathcal{D} \times \mathcal{P} \times \mathbb{R}^+$, the equation (1) can

be rewritten with all uncertainties embedded in the initial state vector :

$$\dot{z}(t) = f_q(z), \tag{2}$$

$$\gamma_e\left(z(t)\right) = 0. \tag{3}$$

Sylvie : Def de forward inner approximation

Related work:.

Sylvie : Pour le moment ci-dessous = surtout du copie-coller de HSCC2014 + des trucs en vrac, je vais reprendre/enrichir bien sur, mais j'attends de savoir jusqu'ou on va et comment sur les gardes car ca risque d'orienter la biblio...

Under-approximate bounded vertex representation of polyhedra have been proposed for the analysis of Simulink/Stateflow models [11], **Sylvie : Idem c'est backward a priori?** but they are restricted to linear transformers. Hybrid systems falsification [16], relies on simulation-based local inner-approximations. **Sylvie : Enrichir en ref plus recentes. Parler de falsification comme exemple? Aussi l'exemple [3] non?**

Outer and inner-approximations for linear systems has been well studied, [4, 13].

There exist a few methods to compute global inner-approximations of the image of non-linear vector-valued functions, mostly based on bisections of the input domain, see for instance [6], later extended by the authors in [7], or inner approximating sets of (semi-algebraic) constraints [10]. But these bisections are very costly if an accurate approximation is needed, and they are not directly applicable to the problem of inner reachability of dynamical systems. For the case of discrete-time dynamical systems for instance, this would require to apply these methods separately to each iterate, with a very costly symbolic representation.

Under-approximate flowpipes [1]. Some recent work [17] propose a computation of backward inner-approximation. The problem is in some sense dual to the one we consider:

Definir qq part les differentes notions/definitions: set inversion, etc

Actually, most existing inner-approximating approaches solve this dual problem, which does not permit to prove such property as (reflechir/verifier et elaborer ou supprimer...).

EXAMPLE 1. *We will consider throughout the paper, the Brusselator equation [14] :*

$$f(x) = \begin{pmatrix} 1 - 2x_1 + \frac{3}{2}x_1^2 x_2 \\ x_1 - \frac{3}{2}x_1^2 x_2 \end{pmatrix}$$

over the time interval $[0, h]$ *(*$h = \frac{1}{20}$*), and with initial conditions* $x_1^0 \in [2, 2.15]$*,* $x_2^0 \in [0.1, 0.15]$*. (...)*

3. PRELIMINARIES

Let us first introduce the ingredients that will be instrumental in the computation of inner approximations of the range of a function over interval inputs, and in particular generalized intervals and mean-value theorem for inner-approximation . The results and notations quickly introduced in this section are mostly based on the work of Goldsztejn *et al.* on modal intervals [5].

3.1 Interval extensions, outer and inner approximations

Classical intervals are used in many situations to rigorously compute with interval domains instead of reals, usually leading to outer approximations of function ranges over boxes. The set of classical intervals is denoted by $\mathbb{IR} = \{[a, b],\ a \in \mathbb{R}, b \in \mathbb{R}, a \leqslant b\}$. In what follows, uncertain quantities defined in intervals are noted in bold, outer-approximating interval enclosures are noted in bold plus brackets, and inner-approximating intervals are noted in bold plus outward brackets. An outer approximating extension of a function $f : \mathbb{R}^n \to \mathbb{R}$ is a function $[\boldsymbol{f}] : \mathbb{IR}^n \to \mathbb{IR}$ such that $\forall \boldsymbol{x} \in \mathbb{IR}^n, \text{range}(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\} \subseteq [\boldsymbol{f}](\boldsymbol{x})$. The natural interval extension consists in replacing real operations by their interval counterparts in the expression of the function. A generally more accurate extension relies on the mean-value theorem, linearizing the function to compute.

Classical interval computations can be interpreted as quantified propositions. Consider for example $f(x) = x^2 - x$. Its natural interval extension, evaluated on $[2, 3]$, is $[\boldsymbol{f}]([2, 3]) = [2, 3]^2 - [2, 3] = [1, 7]$, which can be interpreted as the proposition

$$(\forall x \in [2, 3])\,(\exists z \in [1, 7])\,(f(x) = z).$$

The mean-value extension gives $f(2.5) + [\boldsymbol{f}'](([2, 3]) \times ([2, 3] - 2.5) = [1.25, 6.25]$, and can be interpreted similarly.

Inner approximations determine a set of values proved to belong to the range of the function over some input box. The fact that some $]\boldsymbol{z}[\in \mathbb{IR}$ satisfies $]\boldsymbol{z}[\subseteq \text{range}(f, \boldsymbol{x})$, i.e., is an inner approximation of the range of f over $\boldsymbol{x}$, can again be written using quantifiers :

$$(\forall z \in]\boldsymbol{z}[)\,(\exists x \in \boldsymbol{x})\,(f(x) = z).$$

3.2 Generalized intervals

Let us first introduce generalized intervals, i.e., intervals whose bounds are not ordered, and the Kaucher arithmetic [12] on these intervals. The set of generalized intervals is denoted by $\mathbb{IK} = \{[a, b],\ a \in \mathbb{R}, b \in \mathbb{R}\}$. Related to a set of real numbers $\{x \in \mathbb{R},\ a \leqslant x \leqslant b\}$, one can consider two generalized intervals, $[a, b]$, which is called *proper*, and $[b, a]$, which is called *improper*. We define the operations dual $[a, b] = [b, a]$ and pro $[a, b] = [\min(a, b), \max(a, b)]$.

DEFINITION 1. *Let* $f : \mathbb{R}^n \to \mathbb{R}$ *be a continuous function and* $\boldsymbol{x} \in \mathbb{IK}^n$*, which we can decompose in* $\boldsymbol{x}_{\mathcal{A}} \in \mathbb{IR}^p$ *and* $\boldsymbol{x}_{\mathcal{E}} \in (\textit{dual}\ \mathbb{IR})^q$ *with* $p + q = n$*. A generalized interval* $\boldsymbol{z} \in \mathbb{IK}$ *is* $(f, \boldsymbol{x})$*-interpretable if*

$$(\forall x_{\mathcal{A}} \in \boldsymbol{x}_{\mathcal{A}})\,(Q_z z \in \textit{pro}\ \boldsymbol{z})\,(\exists x_{\mathcal{E}} \in \textit{pro}\ \boldsymbol{x}_{\mathcal{E}}), (f(x) = z) \tag{4}$$

where $Q_z = \exists$ *if* $(\boldsymbol{z})$ *is proper, and* $Q_z = \forall$ *otherwise.*

When all intervals in (4) are proper, we retrieve the interpretation of classical interval computation, which gives an outer approximation of $\text{range}(f, \boldsymbol{x})$

$$(\forall x \in \boldsymbol{x})\,(\exists z \in [\boldsymbol{z}])\,(f(x) = z).$$

When all intervals are improper, (4) becomes an inner approximation of $\text{range}(f, \boldsymbol{x})$

$$(\forall z \in]\text{pro}\ \boldsymbol{z}[)\,(\exists x \in \text{pro}\ \boldsymbol{x})\,(f(x) = z).$$

3.3 Kaucher arithmetic and the generalized interval natural extension

Kaucher arithmetic [12] returns intervals that are interpretable as inner approximations in some simple cases. Kaucher

$\boldsymbol{x} \times \boldsymbol{y}$	$\boldsymbol{y} \in \mathcal{P}$	$\mathcal{Z}$	$-\mathcal{P}$	dual$\mathcal{Z}$
$\boldsymbol{x} \in \mathcal{P}$	$[\underline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \underline{x}\overline{y}]$	$[\underline{x}\underline{y}, \underline{x}\overline{y}]$
$\mathcal{Z}$	$[\underline{x}\overline{y}, \overline{x}\overline{y}]$	$[\min(\underline{x}\overline{y}, \overline{x}\underline{y}), \max(\underline{x}\underline{y}, \overline{x}\overline{y})]$	$[\overline{x}\underline{y}, \underline{x}\underline{y}]$	0
$-\mathcal{P}$	$[\underline{x}\overline{y}, \overline{x}\underline{y}]$	$[\underline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \overline{x}\underline{y}]$
dual$\mathcal{Z}$	$[\underline{x}\underline{y}, \overline{x}\underline{y}]$	0	$[\overline{x}\overline{y}, \underline{x}\overline{y}]$	$[\max(\underline{x}\underline{y}, \overline{x}\overline{y}), \min(\underline{x}\overline{y}, \overline{x}\underline{y})]$

Table 1: Kaucher multiplication

addition extends addition on classical intervals by $\boldsymbol{x} + \boldsymbol{y} = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $\boldsymbol{x} - \boldsymbol{y} = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$. We now decompose $\overline{\mathbb{IK}}$ in $\mathcal{P} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \wedge \overline{x} \geqslant 0\}$, $-\mathcal{P} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \wedge \overline{x} \leqslant 0\}$, $\mathcal{Z} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$, and dual $\mathcal{Z} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$. Kaucher multiplication $\boldsymbol{x} \times \boldsymbol{y}$ is described in Table 1.

Let us interpret the result of the multiplication $\boldsymbol{z} = \boldsymbol{x} \times \boldsymbol{y}$ in one of the cases encountered when $\boldsymbol{y} \in$ dual $\mathcal{Z}$, for instance for $\boldsymbol{x} \in \mathcal{Z}$. Proposition 1 will express the fact that the result can be interpreted as in Definition 1. Interval $\boldsymbol{z}$ can a priori either be proper or improper, let us consider the improper case. We obtain an inner approximation of the range of the multiplication: according to the quantifiers in Definition 1, computing $\boldsymbol{z} = \boldsymbol{x} \times \boldsymbol{y}$ consists in finding $\boldsymbol{z}$ such that for all $x \in \boldsymbol{x}$, for all $z \in$ pro $\boldsymbol{z}$, there exists $y \in$ pro $\boldsymbol{y}$ such that $z = x \times y$. If $\boldsymbol{x}$ contains zero, which is the case when $\boldsymbol{x} \in \mathcal{Z}$, then $\boldsymbol{z}$ is necessarily 0, the result given in Table 1. Indeed, a property that holds for all $x \in \boldsymbol{x}$, holds in particular for $x = 0$, from which we deduce that for all $z \in$ pro $\boldsymbol{z}$, (there exists $y \in$ pro $\boldsymbol{y}$) $z = 0$.

When restricted to proper intervals, these operations coincide with the classical interval operations. Kaucher arithmetic defines a generalized interval natural extension (see [5]) :

PROPOSITION 1. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function, given by an arithmetic expression where each variable appears syntactically only once. Then for $\boldsymbol{x} \in \mathbb{IK}^n$, $f(\boldsymbol{x})$, computed using Kaucher arithmetic, is $(f, \boldsymbol{x})$-interpretable.*

Kaucher arithmetic can thus be used in some cases to compute an inner approximation of range$(f, \boldsymbol{x})$. But the restriction to functions f with single occurrences of variables, that is with no dependency, prevents its direct use. A mean-value extension allows us to by-pass this limitation.

3.4 Generalized interval mean value extension

In the general case of a differentiable function f, the mean-value theorem can be extended to define a generalized interval mean value extension (see [5]) :

THEOREM 1. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $\boldsymbol{x} \in \mathbb{IK}^n$ and suppose that for each $i \in \{1, \ldots, n\}$, we can compute $[\boldsymbol{\Delta}_i] \in \mathbb{IR}$ such that*

$$\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \textit{pro}\ \boldsymbol{x} \right\} \sqsubseteq [\boldsymbol{\Delta}_i]. \tag{5}$$

Then, for any $\tilde{x} \in$ pro $\boldsymbol{x}$, the following interval is $(f, \boldsymbol{x})$-interpretable :

$$\tilde{f}(\boldsymbol{x}) = f(\tilde{x}) + \sum_{i=1}^{n} [\boldsymbol{\Delta}_i](\boldsymbol{x}_i - \tilde{x}_i). \tag{6}$$

EXAMPLE 2. *Let f be defined by $f(x) = x^2 - x$, for which we want to compute an inner approximation of the range over $\boldsymbol{x} = [2, 3]$. Due to the two occurrences of x, $f(\boldsymbol{x})$, computed with Kaucher arithmetic, is not $(f, \boldsymbol{x})$-interpretable. The interval $\tilde{f}(\boldsymbol{x}) = f(2.5) + \boldsymbol{f}'([2, 3])(\boldsymbol{x} - 2.5) = 3.75 + [3, 5](\boldsymbol{x} - 2.5)$ given by its mean-value extension, computed with Kaucher arithmetic, is $(f, \boldsymbol{x})$-interpretable. For $\boldsymbol{x} = [3, 2]$, using the multiplication rule for $\mathcal{P} \times$ dual $\mathcal{Z}$, we get $\tilde{f}(\boldsymbol{x}) = 3.75 + [3, 5]([3, 2] - 2.5) = 3.75 + [3, 5][0.5, -0.5] = 3.75 + [1.5, -1.5] = [5.25, 2.25]$, that can be interpreted as: $\forall z \in [2.25, 5.25]$, $\exists x \in [2, 3]$, $z = f(x)$. Thus, $[2.25, 5.25]$ is an inner approximation of* range$(f, [2, 3])$.

In Section 4, we will be using Theorem 1 with f being the solution of the uncertain dynamical system (2): for this, we need to be able to outer-approximate, at any time t, $f(\tilde{x}), \tilde{x} \in$ pro $\boldsymbol{x}$, and its jacobian with respect to the (uncertain) initial value of the system, $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \text{pro}\ \boldsymbol{x} \right\}$. Computing an enclosure of the solution of an initial value problem is the object of Section 3.5.

3.5 Enclosing the flow of an uncertain ODE with interval Taylor methods

Consider the uncertain dynamical system (2), where $z = (x, p, t)$ and with initial condition $z(t_0) \in \mathcal{Z}_\prime$ at time $t_0 \geq 0$. Let us denote $\mathcal{Z}(t; t_0, \mathcal{Z}_\prime)$ the set of solutions of (2) at time t for initial conditions in $\mathcal{Z}_\prime$ at t_0. We define time grid $t_0 < t_1 < \ldots < t_N$, and assume $\mathcal{Z}_\prime = \boldsymbol{z}_0 = [\underline{z}_0, \overline{z}_0]$ at time $t_0 \geq 0$.

Interval Taylor methods for guaranteed set integration, see [15] for a review, compute flowpipes that are guaranteed to contain the reachable set of solutions $\mathcal{Z}(t; t_0, \mathcal{Z}_\prime)$ of (2) for all time t in $[t_j, t_{j+1}]$. They first verify the existence and uniqueness of the solution using the Banach fixed point theorem and the Picard-Lindelöf operator, and compute an a priori rough enclosure $[\boldsymbol{r}_{j+1}]$ of $\mathcal{Z}(t)$ for all t in $[t_j, t_{j+1}]$. A tighter enclosure for the set of reachable values for t in $[t_j, t_{j+1}]$ is then computed using a Taylor series expansion of order k of the solution at t_j, where $[\boldsymbol{r}_{j+1}]$ is used to enclose the remaining term :

$$[\boldsymbol{z}](t, t_j, [\boldsymbol{z}_j]) = [\boldsymbol{z}_j] + \sum_{i=1}^{k-1} (t - t_j)^i f_q^{[i]}([\boldsymbol{z}_j]) + (t - t_j)^k f_q^{[k]}([\boldsymbol{r}_{j+1}]), \tag{7}$$

where the Taylor coefficients $f_q^{[i]}$ can be computed by automatic differentiation.
Finally, we use enclosure $[\boldsymbol{z}_{j+1}] = [\boldsymbol{z}](t_{j+1}, t_j, [\boldsymbol{z}_j])$ as initial solution set at time t_{j+1} to derive the interval Taylor model on the next time step.

If evaluated plainly in interval arithmetic, scheme (7) yields enclosures of increasing width. A classical way to improve this evaluation is the method introduced by Lohner, that uses QR-factorization. In the experiments presented in Section 5, we chose to control wrapping using affine arithmetic [2] instead of interval arithmetic to evaluate the solution enclosures given by (7).

4. FORWARD INNER REACHABILITY OF CONTINOUS SYSTEMS

As in Section 3.5, we consider the uncertain dynamical system (2), where $z = (x, p, t)$ and with initial condition

$z(t_0) \in \mathcal{Z}_\prime = \boldsymbol{z}_0 = [\underline{z}_0, \overline{z}_0]$ at time $t_0 \geq 0$, and we denote $\mathcal{Z}(t; t_0, \boldsymbol{z}_0)$ the set of solutions $\{z(t, z_0),\ z_0(t_0) \in \boldsymbol{z}_0\}$ of (2) at time t. We have seen in Section 3.5, that for a time grid $t_0 < t_1 < \ldots < t_N$, we can compute on each time interval $[t_j, t_{j+1}]$, a flowpipe (7) that is guaranteed to contain the reachable set of solutions of (2) for all time t in $[t_j, t_{j+1}]$.

We now want to compute also an inner-approximating flowpipe of this reachable set, that is for all t in $[t_j, t_{j+1}]$, a range $]\boldsymbol{z}[(t, t_j, [\boldsymbol{z}_j])$ such that all values inside that range are sure to be reached at time t by an execution of system (2). For that, we will apply Theorem 1, at all time t, to the function z from $\mathbb{R}^n$ to R^n, defined by $z_0 \mapsto z(t, z_0)$, solution to the IVP (2).

We thus need an (outer-approximating) enclosure of $z(t, \tilde{z_0})$ for some $\tilde{z_0} \in \boldsymbol{z}_0$, and of its Jacobian with respect to z_0, evaluated over range $\boldsymbol{z}_0$, defined by the coefficients $J_{ij}(t, \boldsymbol{z}_0) = \frac{\partial z_i}{\partial z_{0,j}}(t, \boldsymbol{z}_0)$, for i and j between 1 and n, and where z_i is the i-th component of the vector flow function z, and $z_{0,j}$ the j-th component of the vector of initial conditions z_0.

We compute these outer-approximations by applying the Taylor method of Section 3.5 to $z(t, \tilde{z_0})$ and $J(t, z_0)$ where $z_0 \in \boldsymbol{z}_0$ and with initial condition $J(t_0) = Id$ the identity matrix : $z(t, \tilde{z_0})$ satisfies system (2) with $z(t_0) = \tilde{z_0} \in \boldsymbol{z}_0$, so that we can directly use the Taylor expansion (7) on each time interval $[t_j, t_{j+1}]$ to compute $\mathcal{Z}(t; t_0, \tilde{z_0})$. The coefficients of the Jacobian matrix of the flow satisfy the following differential equations :

$$\dot{J}_{ij}(t, z_0) = \sum_{k=1}^{n} \frac{\partial f_i}{\partial z_k}(z).J_{kj}(t, z_0) \tag{8}$$

that can be rewritten

$$\dot{J}(t, z_0) = \mathrm{Jac}_z f(z(t, z_0)).J(t, z_0). \tag{9}$$

with $J(t_0) = Id$. A Taylor expansion can thus be used to outer-approximate the solution of (9) noted $\mathcal{J}(t; t_0, \boldsymbol{z}_0)$ on each time interval $[t_j, t_{j+1}]$, using the outer-approximation for $z(t, z_0)$ given by Taylor expansion (7).

EXAMPLE 3. *We consider the continous system of Example 1 :*

$$f(x) = \begin{pmatrix} 1 - 2x_1 + \frac{3}{2}x_1^2 x_2 \\ x_1 - \frac{3}{2}x_1^2 x_2 \end{pmatrix}$$

The corresponding variational equations, for the Jacobian of the solutions x_i with respect to the initial conditions (at time 0) x_j^0 are $J_{i,j} = \frac{\partial x_i}{\partial x_j^0}$:

$$\dot{J}_{1,1} = (-2 + 3x_1x_2)J_{1,1} + \frac{3}{2}x_1^2 J_{2,1} \tag{10}$$

$$\dot{J}_{1,2} = (-2 + 3x_1x_2)J_{1,2} + \frac{3}{2}x_1^2 J_{2,2} \tag{11}$$

$$\dot{J}_{2,1} = (1 - 3x_1x_2)J_{1,1} - \frac{3}{2}x_1^2 J_{2,1} \tag{12}$$

$$\dot{J}_{2,2} = (1 - 3x_1x_2)J_{1,2} - \frac{3}{2}x_1^2 J_{2,2} \tag{13}$$

with initial conditions (at time 0) $J_{i,j} = \delta_{i,j}$.

Altogether, the algorithm, given a time grid $t_0 < t_1 < \ldots < t_N$, an initial range $\boldsymbol{z}_0$, and some $\tilde{z_0} \in \boldsymbol{z}_0$, is as follows :
Initialize: $j = 0$, $t_j = t_0$, $[\boldsymbol{z}_j] = \boldsymbol{z}_0$, $[\tilde{z}_j] = \tilde{z}_0$, $[\boldsymbol{J}_j] = Id$
On each time interval $[t_j, t_{j+1}]$ do:
- compute a priori enclosures $[\boldsymbol{r}_{j+1}]$ of $\mathcal{Z}(t; t_j, \boldsymbol{z}_j)$ for all t in $[t_j, t_{j+1}]$, $[\tilde{\boldsymbol{r}}_{j+1}]$ of $\mathcal{Z}(t; t_j, \tilde{z}_j)$ for all t in $[t_j, t_{j+1}]$, and $[\boldsymbol{R}_{j+1}]$ of $\mathcal{J}(t; t_j, \boldsymbol{z}_j)$
- compute the Taylor Models valid on $[t_j, t_{j+1}]$:

$$[\boldsymbol{z}](t, t_j, [\boldsymbol{z}_j]) = [\boldsymbol{z}_j] + \sum_{i=1}^{k-1} (t - t_j)^i f_q^{[i]}([\boldsymbol{z}_j]) + (t - t_j)^k f_q^{[k]}([\boldsymbol{r}_{j+1}]). \tag{14}$$

$$[\tilde{\boldsymbol{z}}](t, t_j, [\tilde{\boldsymbol{z}}_j]) = [\tilde{\boldsymbol{z}}_j] + \sum_{i=1}^{k-1} (t - t_j)^i f_q^{[i]}([\tilde{\boldsymbol{z}}_j]) + (t - t_j)^k f_q^{[k]}([\tilde{\boldsymbol{r}}_{j+1}]). \tag{15}$$

$$[\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j]) = [\boldsymbol{J}_j] + \sum_{i=1}^{k-1} (t - t_j)^i \mathrm{Jac}_x(f_q^{[i]})([\boldsymbol{r}_{j+1}])[\boldsymbol{J}_j] \tag{16}$$

$$+ (t - t_j)^k \mathrm{Jac}_x(f_q^{[k]})([\boldsymbol{r}_{j+1}])[\boldsymbol{R}_{j+1}] \tag{17}$$

- deduce an inner-approximation valid for t in $[t_j, t_{j+1}]$: if $]\boldsymbol{z}[(t, t_j)$ defined by Equation (18) is an improper interval

$$]\boldsymbol{z}[(t, t_j) = [\tilde{\boldsymbol{z}}](t, t_j, [\tilde{\boldsymbol{z}}_j]) + [\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j]) * ([\overline{z_0}, \underline{z_0}] - \tilde{z_0}) \tag{18}$$

then interval pro $]\boldsymbol{z}[(t, t_j)$ is an inner-approximation of the set of solutions $\{z(t, z_0),\ z_0(t_0) \in \boldsymbol{z}_0\}$ of (2) at time t, otherwise the inner-approximation is empty.
- compute $[\boldsymbol{z}_{j+1}] = [\boldsymbol{z}](t_{j+1}, t_j, [\boldsymbol{z}_j])$, $[\tilde{\boldsymbol{z}}_{j+1}] = [\tilde{\boldsymbol{z}}](t_{j+1}, t_j, [\tilde{\boldsymbol{z}}_j])$, $[\boldsymbol{J}_{j+1}] = [\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j])$

EXAMPLE 4. *We carry on with the computation of outer-approximations for solutions and Jacobians for the Brusselator, on the first time step, using affine arithmetic for estimating the images of functions on initial intervals.*

— OK?

(...)

REMARK 1. *We use the same Taylor expansion, but with different initial conditions, to compute in (14) an outer-approximation of the solution of system(2) with $z(t_0) = \tilde{z_0}$, used as the center in inner-approximation (18), and in (15) an outer-approximation of the solution of the same system but with uncertain $z(t_0) \in \boldsymbol{z}_0$, used to compute the Taylor coefficients in Equation (17) which outer-approximates the Jacobian of the flow with respect to the initial condition z_0.*

REMARK 2. *Note that the wider the outer-approximation in Taylor models (14-17), the tighter thus the less accurate the inner-approximation (18): it can even potentially even leading to an empty inner-approximation if the result of Equation (18) in Kaucher arithmetic is not an improper interval.*

This can occur in two ways. First, note that $[\overline{z_0}, \underline{z_0}] - \tilde{z_0}$ is an improper interval that belongs to dual $\mathcal{Z}$ as defined in Section 3. The outer-approximation of the Jacobian matrix, $[\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j])$ is a proper interval. The Kaucher multiplication as defined in Table tabmult will yield a non-zero improper interval only if $[\boldsymbol{J}](t, t_j, [\boldsymbol{z}_j])$ does not contain 0. And, in this case, the result of this multiplication will depend on the lower bound of the absolute value of the Jacobian (while the same mean-value theorem used for outer-approximation would imply a multiplication of proper intervals that would,

in the same case, depend on the upper bound of the absolute value of the Jacobian). The larger this lower bound, the wider the inner-approximation.

Suppose now that the Kaucher multiplication indeed yields an improper interval. It will then be added to (proper) outer-approximation $[\tilde{\boldsymbol{z}}](t, t_j, [\tilde{\boldsymbol{z}}_j])$ of the solution at time t of the solution of the system starting from point $\tilde{\boldsymbol{z}}_0$. Ideally, this should be tight, but if this interval is wider than the improper interval resulting from the Kaucher multiplication, then the sum of the two intervals - computed using the extension of interval addition - will be proper, and the inner-approximation empty.

— Fait-on une section ou sous-section avec calcul par arithmetique affine? Ou on dit ca juste dans exemples quand on fait un calcul pratique, pour le running example typiquement?

Example 5.

— Calculs pratiques de sous- et sur- approx des variables pour le Brusselator au first time step, detailles

5. EXPERIMENTS AND BENCHMARKS

———-

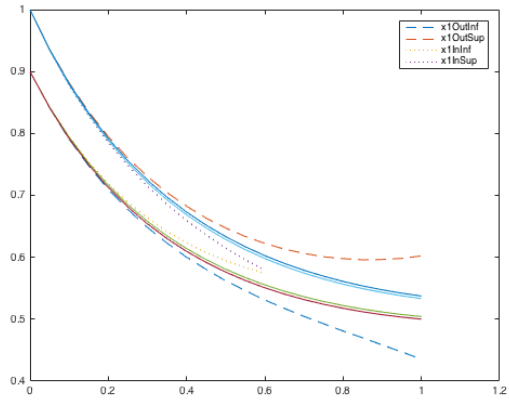
— Rajouter des exemples de la litterature

5.1 Brusselator

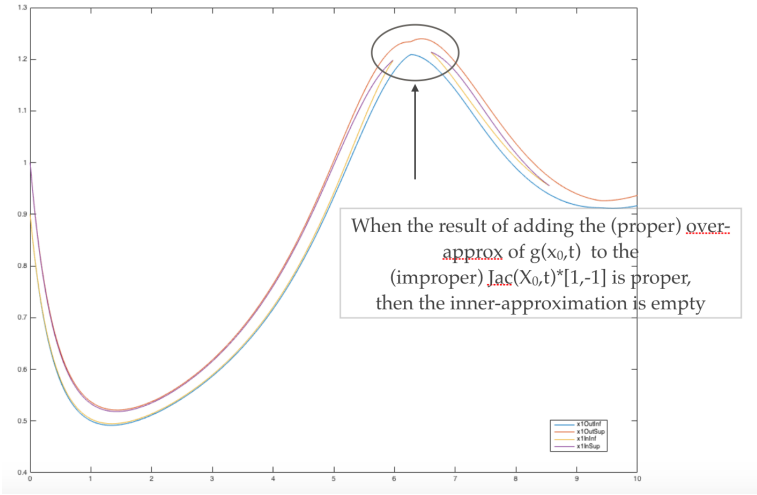
$$\begin{cases} \dot{x}_1 &= 1 + x_1^2 x_2 - 2.5 x_1 \\ \dot{x}_2 &= 1.5 x_1 - x_1^2 x_2 \end{cases}$$

with $x_1(0) \in [0.9, 1]$ and $x_2(0) \in [0, 0.1]$.

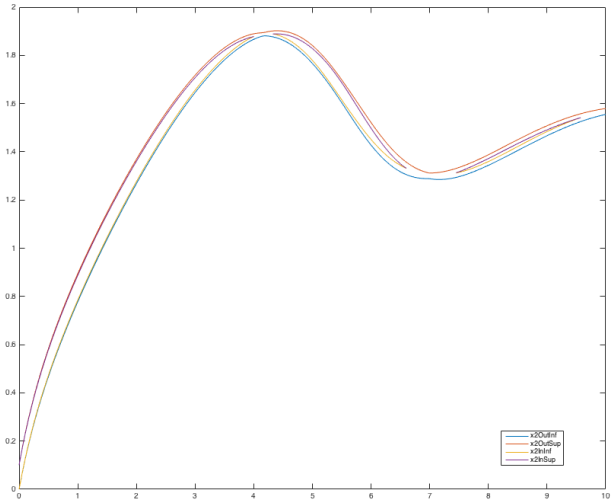
Taylor model of order 3 in t, interval vs affine arithmetic evaluation



The Brusselator (x1): Taylor model of order 4 in t, up to t=10



The Brusselator (x2): Taylor model of order 4 in t, up to t=10



Sylvie : Deja c'est joli - meme si il faudra sans doute que je refasse les figures - commenter que la sous-approx devient vide puis re-apparait, mais aussi reflechir a ce qu'on peut en deduire sur le systeme (cycle?), et si on veut que je fasse d'autres experiences

5.2 Car on the hill

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -9.81 \sin(\frac{dg}{dx}(x_1)) - 0.7 x_2 + u \end{cases}$$

where

$$g(x) = \frac{1}{2}(-\frac{1.1}{1.2}\cos(x) + \frac{1.2}{1.1} cos(1.1x)),$$

the command u is bounded in $[-2, 2]$, the initial condition is $x_1(0) \in [-1, 1]$, $x_2(0) \in [-1, 1]$, and we have limit conditions

$x_1(t) \in [-1, 13]$, $x_2(t) \in \mathbb{R}$ (conditions as in T. Le Mezo's document "viability list of problems")

Sylvie : Si on peut montrer qu'on peut soit reussir a remonter la cite soit rester bloque, un peu comme T. Le Mezo a montre dans sa pres a brest, ca serait chouette. Mais au moins dans l'implem matlab ca explose completement, mais relativement bizarrement: je ne suis qu'a moitiÃl' confiante sur l'AA dedans ...

6. CONCLUSION AND FUTURE WORK

- Hybrid systems (and inner-approximated constraints)
- combination with backward inner-approximated analyses ?
- abstract model-checking ?

7. REFERENCES

[1] X. Chen, S. Sankaranarayanan, and E. Abraham. Under-approximate flowpipes for non-linear continuous systems. In *Proc. of Formal Methods in Computer-Aided Design (FMCAD'14)*, pages 59–66. IEEE/ACM, 2014.

[2] J. L. D. Comba and J. Stolfi. Affine arithmetic and its applications to computer graphics. *Proceedings of SIBGRAPI*, 1993.

[3] G. Frehse, B. H. Krogh, and R. A. Rutenbar. Verifying analog oscillator circuits using forward/backward abstraction refinement. In *Proceedings of the Conference on Design, Automation and Test in Europe: Proceedings*, DATE '06, pages 257–262. European Design and Automation Association, 2006.

[4] A. Girard, C. L. Guernic, and O. Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In *Hybrid Systems: Computation and Control, 9th International Workshop, HSCC 2006, Santa Barbara, CA, USA, March 29-31, 2006, Proceedings*, pages 257–271, 2006.

[5] A. Goldsztejn, D. Daney, M. Rueher, and P. Taillibert. Modal intervals revisited: a mean-value extension to generalized intervals. In *QCP'05*, 2005.

[6] A. Goldsztejn, L. Jaulin, et al. Inner approximation of the range of vector-valued functions. *Reliable Computing*, 14:1–23, 2010.

[7] E. Goubault, M. Kieffer, O. Mullier, and S. Putot. General inner approximation of vector-valued functions. *Reliable Computing*, 18:117–143, 2013.

[8] E. Goubault, O. Mullier, S. Putot, and M. Kieffer. Inner approximated reachability analysis. In *17th International Conference on Hybrid Systems: Computation and Control (part of CPS Week), HSCC'14, Berlin, Germany, April 15-17, 2014*, pages 163–172, 2014.

[9] E. Goubault and S. Putot. Under-approximations of computations in real numbers based on generalized affine arithmetic. In *SAS*, pages 137–152, 2007.

[10] D. Henrion and C. Louembet. Convex inner approximations of nonconvex semialgebraic sets applied to fixed-order controller design. *International Journal of Control*, 85(8):1083–1092, 2012.

[11] A. Kanade, R. Alur, F. Ivančić, S. Ramesh, S. Sankaranarayanan, and K. C. Shashidhar. Generating and analyzing symbolic traces of simulink/stateflow models. In *CAV'09*. Springer, 2009.

[12] E. Kaucher. Interval analysis in the extended interval space IR. *Comput. (Supplementum) 2*, 1980.

[13] C. Le Guernic. *Reachability Analysis of Hybrid Systems with Linear Continuous Dynamics*. PhD thesis, University Joseph Fourier, 2009.

[14] M. Maïga, N. Ramdani, L. Travé-Massuyès, and C. Combastel. A csp versus a zonotope-based method for solving guard set intersection in nonlinear hybrid reachability. *Mathematics in Computer Science*, 8(3):407–423, 2014.

[15] N. S. Nedialkov, K. R. Jackson1, and G. F. Corliss. Validated solutions of initial value problems for ordinary differential equations. *Appl. Math. Comput.*, 105(1):21–68, Oct. 1999.

[16] T. Nghiem, S. Sankaranarayanan, G. Fainekos, F. Ivancić, A. Gupta, and G. J. Pappas. Monte-carlo techniques for falsification of temporal properties of non-linear hybrid systems. In *HSCC'10*. ACM, 2010.

[17] B. Xue, Z. She, and A. Easwaran. Under-approximating backward reachable sets by polytopes. In *CAV*, May 2016.