Tractable higher-order under-approximating AE extensions for non-linear systems

Eric Goubault, Sylvie Putot

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 54-5 (2021) 235–240

Tractable higher-order under-approximating AE extensions for non-linear systems

Eric Goubault * **Sylvie Putot** *

* *LIX, CNRS, Ecole Polytechnique, Institut Polytechnique de Paris, France (email: author@lix.polytechnique.fr)*

Abstract: We consider the problem of under and over-approximating the image of general vector-valued functions over bounded sets, and apply the proposed solution to the estimation of reachable sets of uncertain non-linear discrete-time dynamical systems. Such a combination of under and over-approximations is very valuable for the verification of properties of controlled systems. Over-approximations prove properties correct, while under-approximations can be used for falsification. Coupled, they provide a measure of the conservatism of the analysis. This work introduces a general framework relying on approximations of robust ranges of vector-valued functions, formulated as AE extensions, that can be interpreted as quantified propositions where universal quantifiers (A) precede existential quantifiers (E). This framework allows us to extend for under-approximation many precision refinements that are classically used for over-approximations, such as affine approximations, Taylor models, quadrature formulae and preconditioning methods. We end by evaluating the efficiency and precision of our approach, focusing on the application to the analysis of discrete-time dynamical systems.

Keywords: Uncertain systems, Computer-aided control design

1. INTRODUCTION

Guaranteed state estimation and reachability analysis are central to many problems in control, such as robust and optimal control of dynamical systems, set invariance, safety verification, or control synthesis. This ultimately relies on computing ranges of functions over a domain, that we have to approximate since this is an intractable problem.

Much of the existing work focuses on over-approximations of images of functions, or of reachable sets, generally based on convex set representations (intervals, ellipsoids, polyhedra...). We are interested here in the much less studied problem of computing under-approximations, that is, sets of states guaranteed to be reached. Combining over and under approximations is fundamental for the validation of control systems.When the over-approximation is not sufficient to prove a property, an under-approximation is helpful to state the quality of the over-approximation. Additionally, when an under-approximation of the reachable set intersects the set of error states, it provides a proof of falsification of the property.

For general controlled systems, the reachability properties will depend on the initial conditions of the system, but also on the sensitivity of the system to some control inputs and external disturbances, as reflected by the notions of minimal and maximal reachability Mitchell (2007). We generalize these notions here to robust reachability, considering both control inputs and adversarial disturbances.

Contents and contributions The computation of the reachable set of a dynamical system can be reduced to a series of images of sets by some vector-valued function. In this article, we generalize the first-order approach of Goubault and Putot (2020) to higher-order extensions, and develop more precise quadrature formulas:

- Section 2 recaps the necessary background. Section 3 generalizes the mean-value extension of Goubault and Putot (2020) and proposes new higher-order Taylor extensions for under-approximating robust ranges of sufficiently smooth real-valued functions. These extensions for the robust range are the basis for under-approximation of elementary vector-valued functions;
- Section 4 proposes a novel approach to subdivisions for the extensions based on quadrature formulas: this approach improves precision of the computation of under and over-approximations, while still scaling with the dimension of the system;
- Section 5 applies this approach to the approximation of reachable sets of discrete-time dynamical systems, demonstrating its tractability and precision.

Related work Our approach is related to and partially relies on work on modal intervals and mean-value extensions, which applications include the computation of under-approximations of function images as in Goldsztejn (2012a,b). It is also related to over-approximations of nonlinear functions and dynamical systems, on which we rely to compute under-approximations. Many methods

* Work supported by DGA AID project "Validation de drones et essaims de drones autonomes" and the academic chair "Complex Systems Engineering" of Ecole Polytechnique-ENSTA-Telecom-Thales-Dassault-Naval Group-DGA-FX-Fondation ParisTech.

10.1016/j.ifacol.2021.08.504

for over-approximating reachable sets for non-linear systems have been developed, among which Taylor-based or polytopes-based approaches. There exist less methods for the harder problem of under-approximating images of functions or sets of reachable states. Some approaches have been proposed for linear discrete-time systems, such as Kurzhanski and Varaiya (2000); Girard et al. (2006). Interval-based methods, relying on space discretization, have been used for under-approximating the image of non-linear functions Goldsztejn and Jaulin (2010). They were also used to over and under approximate solutions of differential systems with uncertain initial conditions Mézo et al. (2018). Tight approximations for reachable sets of nonlinear continuous systems can be found via expensive Eulerian methods: the zero sub-level set of the Lipschitz viscosity solution to a Hamilton-Jacobi (HJB) partial differential equation gives the (backward) reachable set Chen et al. (2016). Other approaches, using SoS methods and LMI relaxations have been proposed for inner approximations, see e.g. Korda et al. (2013). In Xue et al. (2020), under-approximations for polynomial systems are obtained by solving semi-definite programs. Taylor models are used on the inverse flow map to derive under-approximations Chen et al. (2014), using topological conditions that are checked with interval constraints solving. In Xue et al. (2016), the computation of the under-approximated reachable set is based on a analysis of the boundary of the reachable sets and polytopic approximations. In Kochdumper and Althoff (2020), some non-convex under-approximations are computed with polynomial zonotopes, relying on a computation of the outer-approximation of the reachable set, of an enclosure of the boundary of the reachable set, and a reduction of the outer-approximation until it is fully included in the region delimited by the boundary.

2. BACKGROUND ON AE EXTENSIONS

We recall in this section the results of Goubault and Putot (2020) for mean-value over and under-approximating extensions for scalar and vector-valued functions.

Notations For a continuously differentiable vector-valued function $f : \mathbb{R}^m \to \mathbb{R}^n$, we note f_i its i-th component and $\nabla f = (\nabla_j f_i)_{ij} = (\frac{\partial f_i}{\partial x_j})_{1\le i\le n, 1\le j\le m}$ its Jacobian matrix. We note $\langle x, y\rangle$ the scalar product of vectors x and y, and $|x|$ the absolute value extended componentwise.

Intervals are used in many situations to rigorously compute with interval domains instead of reals, usually leading to over-approximations of function ranges over boxes. Interval quantities, whether scalar or vector-valued, will be noted with bold letters, e.g $\boldsymbol{x} = [\underline{x}, \overline{x}]$, $\underline{x} \in \mathbb{R}$, $\overline{x} \in \mathbb{R}$. For a (possibly vector-valued) interval $\boldsymbol{x} \in \mathbb{IR}^m$, we note $c(\boldsymbol{x}) = (\underline{x}+\overline{x})/2$ its center and $r(\boldsymbol{x}) = (\overline{x}-\underline{x})/2$ its radius.

An *over-approximating extension*, also called *outer-approximating extension*, of a function $f : \mathbb{R}^m \to \mathbb{R}^n$ is a function $\boldsymbol{f} : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$, where $\mathcal{P}(S)$ denotes the powerset of S, such that for all $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\text{range}(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\} \subseteq \boldsymbol{f}(\boldsymbol{x})$. Dually, under-approximations determine a set of values proved to belong to the range of the function over some input set. An *under-approximating extension*, also called *inner-approximating extension*, of f, is a function $\boldsymbol{f} : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$, such that for all $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\boldsymbol{f}(\boldsymbol{x}) \subseteq \text{range}(f, \boldsymbol{x})$. Under- and over-approximations can be interpreted as quantified propositions: $\text{range}(f, \boldsymbol{x}) \subseteq \boldsymbol{z}$ can be written $\forall x \in \boldsymbol{x}, \exists z \in \boldsymbol{z}, f(x) = z$ while $\boldsymbol{z} \subseteq \text{range}(f, \boldsymbol{x})$ can be written $\forall z \in \boldsymbol{z}, \exists x \in \boldsymbol{x}, f(x) = z$. Both these propositions are what we call *AE propositions*, quantified propositions where universal quantifiers (A) precede existential quantifiers (E).

Mean-value AE extensions for scalar-valued functions We consider a function $f : \mathbb{R}^m \to \mathbb{R}$. 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 a linearization by the mean-value theorem.

Suppose f is differentiable over the box $\boldsymbol{x}$. The mean-value theorem implies that
$\forall x^0 \in \boldsymbol{x}, \forall x \in \boldsymbol{x}, \exists \xi \in \boldsymbol{x}, f(x) = f(x^0) + \langle \nabla f(\xi), x - x^0\rangle.$
If we can bound the range of the gradient of f over $\boldsymbol{x}$, by $\boldsymbol{\nabla f}(\boldsymbol{x})$, then we can derive an interval enclosure, called the mean-value extension. Let us choose x^0 to be the center $c(\boldsymbol{x})$ of $\boldsymbol{x}$ and recall we note $r(\boldsymbol{x}) = (\overline{x} - \underline{x})/2$ its radius.

Theorem 1. (Thm. 1, Goubault and Putot (2020)). Let f be a continuously differentiable function from $\mathbb{R}^m$ to $\mathbb{R}$ and $\boldsymbol{x} \in \mathbb{IR}^m$. Let $\boldsymbol{f^0} = [\underline{f^0}, \overline{f^0}]$ include $f(c(\boldsymbol{x}))$ and $\boldsymbol{\nabla}$ a vector of intervals $\boldsymbol{\nabla_i} = [\underline{\nabla}_i, \overline{\nabla}_i]$ for $i \in \{1, \dots, m\}$ such that $\{|\nabla_i f(c(\boldsymbol{x}_1), \dots, c(\boldsymbol{x}_{i-1}), x_i, \dots, x_m)|, x \in \boldsymbol{x}\} \subseteq \boldsymbol{\nabla}_i$. We have the over- and under-approximating extensions

$$\text{range}(f, \boldsymbol{x}) \subseteq [\underline{f^0}, \overline{f^0}] + \langle \overline{\nabla}, r(\boldsymbol{x})\rangle[-1, 1] \quad (1)$$

$$[\overline{f^0} - \langle \underline{\nabla}, r(\boldsymbol{x})\rangle, \underline{f^0} + \langle \underline{\nabla}, r(\boldsymbol{x})\rangle] \subseteq \text{range}(f, \boldsymbol{x}) \quad (2)$$

Example 1. Let us consider the range of f defined by $f(x) = x^2 - x$ over $\boldsymbol{x} = [2, 3]$. We can compute $f(2.5) = 3.75$ and $|\nabla f([2, 3])| \subseteq [3, 5]$. Then (1) and (2) yield $3.75 + 1.5[-1, 1] \subseteq \text{range}(f, [2, 3]) \subseteq 3.75 + 2.5[-1, 1]$, from which we deduce $[2.25, 5.25] \subseteq \text{range}(f, [2, 3]) \subseteq [1.25, 6.25]$.

We refer to extensions (1) and (2) as *AE extensions*, as they can be interpreted as *AE propositions*. Note that the under-approximation can become empty if the width $\overline{f_0} - \underline{f_0}$ of the approximation of $f(c(\boldsymbol{x}))$ exceeds $2\langle \overline{\nabla}, r(\boldsymbol{x})\rangle$: in this case the lower bound of the resulting interval is larger than the upper bound, which by convention we identify with the empty interval. A special attention to the practical evaluation of these extensions over the region $\boldsymbol{x}$ of interest is thus crucial, this is the object of Section 4.

Mean-value AE extensions of the robust range Mean-value AE extensions can be generalized to compute ranges that are robust to disturbances, identified as some input components. Let us partition the indices of the input space in two subsets $I_{\mathcal{A}}$ and $I_{\mathcal{E}}$, where $I_{\mathcal{A}}$ defines the indices of the inputs that correspond to disturbances, and $I_{\mathcal{E}}$ the remaining dimensions. We decompose the input box $\boldsymbol{x}$ accordingly by $\boldsymbol{x} = \boldsymbol{x}_{\mathcal{A}} \times \boldsymbol{x}_{\mathcal{E}}$. We define the robust range of function f on $\boldsymbol{x}$, robust on $\boldsymbol{x}_{\mathcal{E}}$ with respect to disturbances $\boldsymbol{x}_{\mathcal{A}}$, as $\text{range}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \{z \,|\, \forall w \in \boldsymbol{x}_{\mathcal{A}}, \exists u \in \boldsymbol{x}_{\mathcal{E}}, z = f(w, u)\}$. Intuitively, u will be control components, w disturbances to which the output range should be robust.

Theorem 2. (Thm. 2, Goubault and Putot (2020)). Let f be continuously differentiable function from $\mathbb{R}^m$ to $\mathbb{R}$ and $\boldsymbol{x} = \boldsymbol{x}_{\mathcal{A}} \times \boldsymbol{x}_{\mathcal{E}} \in \mathbb{IR}^m$. Let $\boldsymbol{f}^0$, $\boldsymbol{\nabla}_w$ and $\boldsymbol{\nabla}_u$ be vectors of intervals such that $f(c(\boldsymbol{x})) \subseteq \boldsymbol{f}^0$, $\{|\nabla_w f(w, c(\boldsymbol{x}_{\mathcal{E}}))|, w \in$

$\boldsymbol{x}_{\mathcal{A}}\} \subseteq \boldsymbol{\nabla}_w$ and $\{|\nabla_u f(w,u)|, w \in \boldsymbol{x}_{\mathcal{A}}, u \in \boldsymbol{x}_{\mathcal{E}}\} \subseteq \boldsymbol{\nabla}_u$. We have:

$$\text{range}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq [\underline{f^0} - \langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \overline{f^0} + \langle \overline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \underline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle] \quad (3)$$

$$[\overline{f^0} - \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \underline{f^0} + \langle \underline{\nabla}_u, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \overline{\nabla}_w, r(\boldsymbol{x}_{\mathcal{A}})\rangle] \subseteq \text{range}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}) \quad (4)$$

AE extensions for vector-valued functions Following Goubault and Putot (2020), we now detail how full n-dimensional boxes can be included in the image of vector-valued functions $f : \mathbb{R}^m \to \mathbb{R}^n$, for $m \geq n$, using AE extensions of robust ranges.

The mean-value extensions of Theorem 1 or the generalization of Theorem 5 give us under and over-approximations of projections of the image of the function. The Cartesian product of the over-approximations of each component provides an over-approximation of a vector-valued function $f : \mathbb{R}^m \to \mathbb{R}^n$. This is however not the case for under-approximation. Suppose for example that we have $\forall z_1 \in \boldsymbol{z}_1, \exists x_1 \in \boldsymbol{x}_1, \exists x_2 \in \boldsymbol{x}_2, z_1 = f_1(x)$ and $\forall z_2 \in \boldsymbol{z}_2, \exists x_1 \in \boldsymbol{x}_1, \exists x_2 \in \boldsymbol{x}_2, z_2 = f_2(x)$. We cannot deduce directly that for all $\forall z_1 \in \boldsymbol{z}_1$ and $\forall z_2 \in \boldsymbol{z}_2$ there exists x_1 and x_2 such that $z = f(x)$. Suppose now that we have: $\forall z_1 \in \boldsymbol{z}_1, \forall x_1 \in \boldsymbol{x}_1, \exists x_2 \in \boldsymbol{x}_2, z_1 = f_1(x)$ and $\forall z_2 \in \boldsymbol{z}_2, \forall x_2 \in \boldsymbol{x}_2, \exists x_1 \in \boldsymbol{x}_1, z_2 = f_2(x)$ with continuous selections x_2 and x_1. Then there exists functions $g_2(z_1, x_1) : \boldsymbol{z}_1 \times \boldsymbol{x}_1 \to \boldsymbol{x}_2$ and $g_1(z_2, x_2) : \boldsymbol{z}_2 \times \boldsymbol{x}_2 \to \boldsymbol{x}_1$ that are continuous in x_1 (resp. x_2), and such that $\forall (z_1, z_2) \in \boldsymbol{z}, \forall (x_1, x_2) \in \boldsymbol{x}$, $z_1 = f_1(x_1, g_2(z_1, x_1))$ and $z_2 = f_2(g_1(z_2, x_2), x_2)$. Using the Brouwer fixed point theorem on the continuous map $g : (x_1, x_2) \to (g_1(z_2, x_2), g_2(z_1, x_1))$ on the compact set $\boldsymbol{x}_1 \times \boldsymbol{x}_2$, then $\forall (z_1, z_2) \in \boldsymbol{z}, \exists (x_1^z, x_2^z) \in \boldsymbol{x}$ such that $(z_1, z_2) = f(x_1^z, x_2^z)$. This result can be generalized:

Theorem 3. (Theorem 3 Goubault and Putot (2020)). Let $f : \mathbb{R}^m \to \mathbb{R}^n$ be an elementary function and $\pi : [1 \dots m] \to [1 \dots n]$ Let us note, for all $i \in [1 \dots n]$, $J_E^{(z_i)} = \{j \in [1 \dots m], \pi(j) = i\}$ and $J_A^{(z_i)} = \{j \in [1 \dots m]\} \setminus J_E^{(z_i)}$. Consider the n AE-extensions $i \in [1 \dots n]$ built from Theorems 2, 4 or 5 and such that

$$\forall z_i \in \boldsymbol{z}_i, \ (\forall x_j \in \boldsymbol{x}_j)_{j \in J_A^{(z_i)}}, \ (\exists x_j \in \boldsymbol{x}_j)_{j \in J_E^{(z_i)}}, \ z_i = f_i(x)$$

Then $\boldsymbol{z} = \boldsymbol{z}_1 \times \boldsymbol{z}_2 \times \dots \times \boldsymbol{z}_n$, if non-empty, is an under-approximation of the image of f: $\forall z \in \boldsymbol{z}, \exists x \in \boldsymbol{x}, z = f(x)$.

Theorem 3 gives us directly a computation of an under-approximation of range$(f, \boldsymbol{x})$ for $f : \mathbb{R}^m \to \mathbb{R}^n$. It can also be used to compute an under-approximation of the robust range range$(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$. For this, we need to choose $\pi : [1 \dots m] \to ([1 \dots n] \setminus I_{\mathcal{A}})$, which corresponds to the fact that the disturbance part of the input components will always be quantified universally. We define below the result of this process, which will be later used in reachability algorithms for discrete-time dynamical systems.

Definition 1. Let $f : \mathbb{R}^m \to \mathbb{R}^n$ and $\pi : [1 \dots m] \to ([1 \dots n] \setminus I_{\mathcal{A}})$. We define $\mathcal{I}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}, \pi)$ an under-approximation of range$(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$ obtained using Theorem 3 with function π, where the under-approximation of each component is obtained with Theorem 2 or Corollary 1. We define $\mathcal{O}(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}}, \pi)$ the over-approximation obtained with Theorem 2 component-wise.

3. GENERALIZATION TO NEW AE EXTENSIONS

We now introduce new robust AE extensions for a function $f : \mathbb{R}^m \to \mathbb{R}$, which are no longer necessarily based on the mean-value theorem [1].

Theorem 4. Suppose we have an approximation function g for f, which is an elementary [2] function in the sense of Goldsztejn (2012a), satisfying $\forall w \in \mathbf{x}_{\mathcal{A}}, \ \forall u \in \mathbf{x}_{\mathcal{E}}, \ \exists \xi \in \mathbf{x}, \ f(w, u) = g(w, u, \xi)$. Then any under-approximation (resp. over-approximation) of the robust range of g with respect to $x_{\mathcal{A}}$ and ξ, $\mathcal{I}_g \subseteq \text{range}(g, \mathbf{x} \times \mathbf{x}, I_{\mathcal{A}} \cup \{m+1, \dots, 2m\}, I_{\mathcal{E}})$ is an under-approximation (resp. over-approximation) of the robust range of f with respect to $x_{\mathcal{A}}$, i.e. $\mathcal{I}_g \subseteq \text{range}(f, \mathbf{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

For instance, for a continuously $(n+1)$-differentiable f, the following g, obtained by a Taylor-Lagrange expansion and noting $x = (w, u)$, is an approximation function for f

$$g(x, \xi) = f(x^0) + \sum_{i=1}^{n} \frac{(x - x^0)^i}{i!} D^i f(x^0) + D^{n+1} f(\xi) \frac{(x - x^0)^{n+1}}{(n+1)!} \quad (5)$$

where $D^\alpha f$ denotes the higher order partial derivative of f. For $n = 0$, g is the mean-value approximation.

Example 2. Consider function $f(x) = x^3 + x^2 + x + 1$ on $[-\frac{1}{4}, \frac{1}{4}]$. Its exact range is $[0.796875, 1.328125]$. Let us approximate f using an order 2 Taylor-Lagrange expansion: we compute $f^{(1)}(x) = 3x^2 + 2x + 1$ and $f^{(2)}(x) = 6x + 2$ and deduce $g(x, \xi) = 1 + x + x^2(3\xi + 1)$. By Theorem 4, the range of f over $[-\frac{1}{4}, \frac{1}{4}]$ is under (resp. over) approximated by any under (resp. over) approximation of the robust range with respect to ξ of $g(x, \xi)$.

Theorem 5 gives a simple way for computing the under-approximated robust range of g, which is well suited in particular for quadratic Taylor-based approximations.

Theorem 5. Let g be an elementary function $g(w, u, \xi) = \alpha(w, u) + \beta(w, u, \xi)$ over $x = (w, u) \in \mathbf{x} \subseteq \mathbb{IR}^m$ and $\xi \in \mathbf{x}$. Let $\mathcal{I}_\alpha$ be an under-approximation of the robust range of α with respect to w, i.e. range$(\alpha, \mathbf{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$, and $\mathcal{O}_\beta$ an over-approximation of the range of β, i.e. range$(\beta, \mathbf{x} \times \mathbf{x}, \emptyset, \{1, \dots, 2m\})$. The robust range of g with respect to $w \in \mathbf{x}_{\mathcal{A}}$ and $\xi \in \mathbf{x}$, i.e. range$(g, \mathbf{x} \times \mathbf{x}, I_{\mathcal{A}} \cup \{m+1, \dots, 2m\}, I_{\mathcal{E}})$, is under-approximated by $\mathcal{I}_g = [\underline{\mathcal{I}}_\alpha + \overline{\mathcal{O}}_\beta, \overline{\mathcal{I}}_\alpha + \underline{\mathcal{O}}_\beta]$.

This is the case of Taylor expansions (5), where α is the degree n polynomial, and β the degree $n+1$ remainder. A direct consequence is a simple order 2 method:

Corollary 1. Consider $f : \mathbb{R}^m \to \mathbb{R}$ a function in C^2. Let $\boldsymbol{f}^0$, $\boldsymbol{\nabla}_w^0$ and $\boldsymbol{\nabla}_u^0$ be such that $f(x^0) \subseteq \boldsymbol{f}^0$, $|\nabla_w f(x^0)| \subseteq \boldsymbol{\nabla}_w^0$ and $|\nabla_u f(x^0)| \subseteq \boldsymbol{\nabla}_u^0$ with $x^0 = c(\boldsymbol{x})$. Then range$(f, \boldsymbol{x}, I_{\mathcal{A}}, I_{\mathcal{E}})$ is under-approximated by $[\underline{\mathcal{I}}_\alpha + \overline{\mathcal{O}}_\beta, \overline{\mathcal{I}}_\alpha + \underline{\mathcal{O}}_\beta]$ where $\mathcal{I}_\alpha = [\overline{f^0} - \langle \underline{\nabla}_u^0, r(\boldsymbol{x}_{\mathcal{E}})\rangle + \langle \overline{\nabla}_w^0, r(\boldsymbol{x}_{\mathcal{A}})\rangle, \underline{f^0} + \langle \underline{\nabla}_u^0, r(\boldsymbol{x}_{\mathcal{E}})\rangle - \langle \overline{\nabla}_w^0, r(\boldsymbol{x}_{\mathcal{A}})\rangle]$ and $\mathcal{O}_\beta$ is any over-approximation of $\{\frac{1}{2} D^2 f(x)(r(\boldsymbol{x}))^2, x \in \boldsymbol{x}\}$.

[1] Extended version with proofs in arXiv:2101.11536

[2] Elementary functions are compositions of +, -, ×, /, sine, cosine, log, exp functions in particular.

Example 3. We carry on with Example 2. The under approximation of the range of $1 + x$ over $[-\frac{1}{4}, \frac{1}{4}]$ is $[\frac{3}{4}, \frac{5}{4}]$. Standard interval computation yields $[0, \frac{1}{16}][\frac{1}{4}, \frac{7}{4}] = [0, \frac{7}{64}]$ as over approximation of the range of $x^2(3\xi + 1)$ for x and ξ in $[-\frac{1}{4}, \frac{1}{4}]$. We deduce $[0.859375, 1.25] \subseteq \text{range}(f, \boldsymbol{x})$. In comparison, the mean-value AE extension of Theorem 2 yields the less precise under-approximation $[0.875, 1.125]$.

4. PRECONDITIONING AND QUADRATURE

The n-dimensional inner boxes that we compute with the techniques of Section 2 can sometimes be small or empty, even when the projected inner-approximations on each component are tight. We propose here some solutions.

Preconditioning for computing inner skewed boxes The image of the vector-valued function cannot always be precisely approximated by a centered box.

Example 4. We consider $f(x) = (2x_1^2 - x_1x_2 - 1, x_1^2 + x_2^2 - 2)^\intercal$ with $\boldsymbol{x} = [0.9, 1.1]^2$. The under-approximated projections on the two components, $[-0.38, 0.38]$ and $[-0.38, 0.38]$, are close to the over-approximated range $[-0.42, 0.42]^2$, but we only find empty inner boxes.

This can be partly solved by computing a skewed box, or the image of a box by a linear map, instead of a box. Let $C \in \mathbb{R}^{n\times n}$ be a non-singular matrix. If $\boldsymbol{z}$ is an interval vector such that $\boldsymbol{z} \subseteq \text{range}(Cf, \boldsymbol{x})$, we can deduce a skewed box to be in the range of f, by $\{C^{-1}z | z \in \boldsymbol{z}\} \subseteq \text{range}(f, \boldsymbol{x})$. A natural choice for C is the inverse of the center of the interval Jacobian matrix $C = (c(\boldsymbol{\nabla}))^{-1}$.

Example 5. On Example 4, using this preconditioning and $\pi : (1 \to 1, 2 \to 2)$, we obtain the yellow under-approximating parallelotope of Figure 1a. We estimate the image $\text{range}(f, \boldsymbol{x})$ by sampling points in the input domain. This sampling-based estimation is represented as the dark dots-filled region. The green parallelotope and box are the over-approximations with and without preconditioning.

Quadrature formulae for the mean-value extension The mean-value interval extension can yield rough approximations. This is especially the case when the variation of the gradient is important over the input range.Using simple quadrature formulae partially solves this problem.

Let $f : \mathbb{R}^m \to \mathbb{R}$. We partition each dimension $j = [1 \dots m]$ of the m-dimensional input box $\boldsymbol{x} = \boldsymbol{x}_1 \times \dots \times \boldsymbol{x}_m$ in $2k$ sub-intervals and define, for all $j = [1 \dots m]$, $x_j^{-k} \leq x_j^{-(k-1)} \leq \dots \leq x_j^0 \leq \dots \leq x_j^k$, with $x_j^{-k} = \underline{\boldsymbol{x}_j}$, $x_j^0 = c(\boldsymbol{x}_j)$, $x_j^k = \overline{\boldsymbol{x}_j}$. We note $dx^i = x^i - x^{i-1}$ the vector-valued deviation. The first natural idea is to compute an under-approximation for each sub-box obtained as product of sub-intervals in each dimension. But the convex union of the under-approximating boxes is in general not an under-approximation of $\text{range}(f, \boldsymbol{x})$. We propose below a scheme that avoids these unions, and remains linear in k with respect to the non-partitioned case. We note $\boldsymbol{x}^1 = [x_1^{-1}, x_1^1] \times [x_2^{-1}, x_2^1] \times \dots \times [x_m^{-1}, x_m^1]$, and for all i between 2 and k, $\boldsymbol{x}^i = [x_1^{-i}, x_1^i] \times \dots \times [x_m^{-i}, x_m^i] \setminus \mathring{\boldsymbol{x}}^{i-1}$, where $\setminus$ denotes the set difference and $\mathring{\boldsymbol{x}}$ the interior of $\boldsymbol{x}$. This partition is represented in Figure 1b for a two-dimensional space. In practice, each "square ring" $\boldsymbol{x}^i$ will be decomposed in $2n$ sub-boxes for the Jacobian evaluation.

By the mean-value theorem, $\forall x \in [x^{-1}, x^1]$, $\exists \xi^1 \in [x^{-1}, x^1]$, $f(x) = f(x^0) + \langle \nabla f(\xi^1), x - x^0 \rangle$. Let $\boldsymbol{f}^0 \supseteq f(x^0)$ and $\boldsymbol{\nabla}^i$ for i in $[1, k]$ such that $\{|\nabla f(x)|, x \in \boldsymbol{x}^i\} \subseteq \boldsymbol{\nabla}^i$. We have $\text{range}(f, \boldsymbol{x}^1) \subseteq \boldsymbol{f}^0 + \langle \overline{\nabla}^1, dx^1 \rangle [-1, 1]$ and $[\overline{f^0} - \langle \underline{\nabla}^1, dx^1 \rangle, \underline{f^0} + \langle \underline{\nabla}^1, dx^1 \rangle] \subseteq \text{range}(f, [x^{-1}, x^1])$. Let us now take $x \in \boldsymbol{x}^2$. We can iterate the mean-value theorem on the adjacent subdivision and write that for all $x \in \boldsymbol{x}^2$, there exist $x^1 \in \boldsymbol{x}^1 \cap \boldsymbol{x}^2$, $\xi^2 \in \boldsymbol{x}^2$ such that $f(x) = f(x^1) + \langle \nabla f(\xi^2), x - x^1 \rangle$ and $|x_1 - x_1^1| \leq dx_1^2$ and $|x_2 - x_2^1| \leq dx_2^2$. (take for example for x^1 the intersection of the line from x^0 to x with the border between $\boldsymbol{x}^1$ and $\boldsymbol{x}^2$). We have $\text{range}(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2) \subseteq \boldsymbol{f}^0 + \langle \overline{\nabla}^1, dx^1 \rangle [-1, 1] + \langle \overline{\nabla}^2, dx^2 \rangle [-1, 1]$. There also exists $(x, x^1) \in \boldsymbol{x}^2 \times \boldsymbol{x}^1$ such that $|x_1 - x_1^1| = dx_1^2$ and $|x_2 - x_2^1| = dx_2^2$ (take the corners of the boxes $\boldsymbol{x}^1$ and $\boldsymbol{x}^2$), so that we also have $[\overline{f^0} - \langle \underline{\nabla}^1, dx^1 \rangle - \langle \underline{\nabla}^2, dx^2 \rangle, \underline{f^0} + \langle \underline{\nabla}^1, dx^1 \rangle + \langle \underline{\nabla}^2, dx^2 \rangle] \subseteq \text{range}(f, \boldsymbol{x}^1 \cup \boldsymbol{x}^2)$. This generalizes to the k subdivisions, for instance for the under-approximation: $[\overline{f^0} - \sum_{i=1}^k \langle \underline{\nabla}^i, dx \rangle, \underline{f^0} + \sum_{i=1}^k \langle \underline{\nabla}^i, dx \rangle] \subseteq \text{range}(f, \boldsymbol{x})$. The same applies to the estimation of robust ranges. Naturally, other quadrature schemes could be used.

Example 6. We consider $f(x) = (2x_1^2 + 2x_2^2 - 2x_1x_2 - 2, x_1^3 - x_2^3 + 4x_1x_2 - 3)^\intercal$ with $\boldsymbol{x} = [0.9, 1.1]^2$. The results are represented in Figure 1c. The sampling-based estimation of the image is the dark dots-filled region. We choose $\pi : (1 \to 1, 2 \to 2)$. Using the preconditioned mean-value extension without partitioning, the over-approximation is the largest green parallelotope and the under-approximation for the joint range is empty. The quadrature formula for the mean-value extension with $k = 10$ partitions on one hand, and the order 2 extension of Corollary 1 on the other hand, yield two very similar under-approximating yellow parallelotopes. They also yield two very similar green over-approximating parallelotopes. The light green box is the order 2 over-approximation without preconditioning.

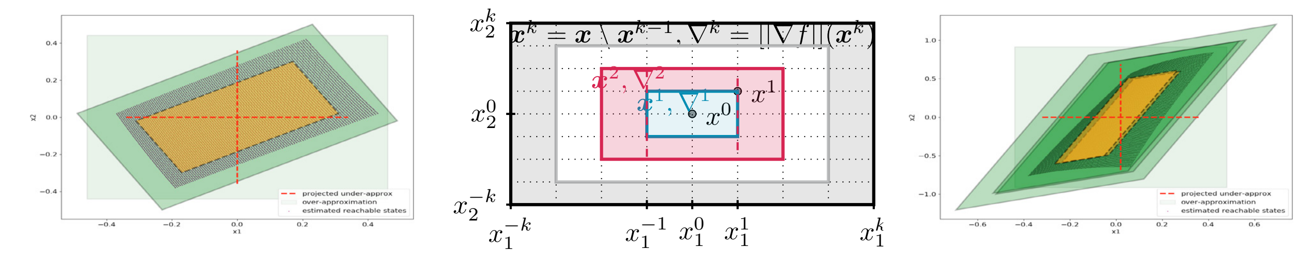
Remark 1. The approach yields approximations centered at $f(x^0)$. We observe that the under-approximating skewed box is very close to the largest skewed box entirely included in the image, given a fixed skewing and a center at $f(x^0)$.

Finally, as sound under-approximations are still obtained by considering sub-regions of the input set, refinements can be obtained by filtering out sub-regions where Jacobian coefficients are very sensitive to the inputs or close to zero.

Bounding the Jacobian matrix The approach relies on computing over-approximations of $\nabla f(x)$ over some subsets of input box $\boldsymbol{x}$, namely $\boldsymbol{\nabla}^i$ for i in $[1, k]$ such that $\{|\nabla f(x)|, x \in \boldsymbol{x}^i\} \subseteq \boldsymbol{\nabla}^i$. Automatic differentiation allows to compute the derivatives, but needs to be combined with set-membership methods. The combination of automatic differentiation with an evaluation in affine arithmetic provides a good trade-off between efficiency and precision. Also, affine forms provide a combination of parameterization and set-based estimation: a parametric approximate form for $\nabla f(x)$ valid on all box $\boldsymbol{x}$ is computed, that can be instantiated on $\boldsymbol{x}^i$ to yield over-approximation ∇^i, avoiding several differentiations.

5. APPLICATION TO DISCRETE-TIME SYSTEMS

We consider the reachability of discrete-time non-linear dynamical systems with inputs of the form



(a) Example 5: under- (dotted lines) and over-approximation (plain lines)

(b) Partitioning the input domain

(c) Example 6: approximations for quadrature and order 2 extensions

Fig. 1. Illustrations for Sections 2 and 4

$$\begin{cases} z^{k+1} = f(z^k, u^k) \\ z^0 \in \boldsymbol{z}^0 \end{cases} \quad (6)$$

where $f : \mathbb{R}^m \to \mathbb{R}^n$ is a vector-valued non-linear function with $m \geq n$, $z \in \mathbb{R}^n$ the vector of state variables, $u \in \boldsymbol{u} \subseteq \mathbb{R}^{m-n}$ the input signal, and $\boldsymbol{z}^0$ the initial set.

Given an initial set $\boldsymbol{z}^0$, we want to compute the bounded time reachable set of the dynamical system, i.e, the set of states visited by the dynamical system up to a fixed time horizon $K \in \mathbb{N}$. The computation of the reachable set can be seen as a series of images of sets by vector-valued function f. We thus can use the results of Sections 2 to 4.

For conciseness, we consider systems without disturbances and compute maximal (or classical) reachable sets. The algorithms can be straightforwardly extended to robust reach set of systems with disturbances, basically replacing ranges by robust ranges. This allows us to use the lighter notations $\mathcal{I}(f, \boldsymbol{x}, \pi)$ and $\mathcal{O}(f, \boldsymbol{x}, \pi)$ to note the under and over-approximating sets introduced in Definition 1.

Method 1 the first method consists in iteratively computing function image, with as input the previously computed approximation of the image. We compute under and over-approximations I^k and O^k of the reachable set $\boldsymbol{z}^k$ by

$$\begin{cases} I^0 = \boldsymbol{z}^0, \; O^0 = z^0 \\ I^{k+1} = \mathcal{I}(f, I^k, \pi), \; O^{k+1} = \mathcal{O}(f, O^k, \pi) \end{cases} \quad (7)$$

This yields Algorithm 1. At each step k, under and

Algorithm 1 Iterated discrete-time reachability

Input: $f : \mathbb{R}^n \to \mathbb{R}^n$, $\boldsymbol{z}^0 \subseteq \mathbb{IR}^n$ initial state, $K \in \mathbb{N}^+$, an over-approximating extension $[\nabla f]$ (see Section 4)
Output: I^k and O^k for $k \in [1, K]$
$I^0 := \boldsymbol{z}^0, O^0 := \boldsymbol{z}^0$; choose $\pi : [1 \ldots n] \mapsto [1 \ldots n]$
for k from 0 to $K-1$ **do**
$\boldsymbol{\nabla}_I^k := |[\nabla f](I^k)|$, $\boldsymbol{\nabla}_O^k := |[\nabla f](O^k)|$
$A_I^k := c(\boldsymbol{\nabla}_I^k)$, $A_O^k := c(\boldsymbol{\nabla}_O^k)$ (supposed non-singular)
$C_I^k := (A_I^k)^{-1}$, $C_O^k := (A_O^k)^{-1}$
$\boldsymbol{z}_I^{k+1} := \mathcal{I}(C_I^k f, I^k, \pi)$, $\boldsymbol{z}_O^{k+1} := \mathcal{O}(C_O^k f, O^k, \pi)$
if $\boldsymbol{z}_I^k = \emptyset$ **then**
return
end
$I^{k+1} := A_I^k \boldsymbol{z}_I^{k+1}$, $O^{k+1} := A_O^k \boldsymbol{z}_O^{k+1}$
end for

over-approximations I^k and O^k of the joint range, which computation are fully decoupled, are used as input for the next step. It is thus particularly important to compute tight approximations of this vector-valued range, and in particular use preconditioning. At each step k, $\boldsymbol{z}_I^{k+1}$ is an interval vector such that, if it is non empty, $I^{k+1} = A_I^k \boldsymbol{z}_I^{k+1} \subseteq \text{range}(f, I^k) \subseteq \text{range}(f^{k+1}, \boldsymbol{z}^0)$.

Method 2 the second method consists in computing the sensitivity to initial state by approximating the gradient of the iterated function. At each step k, we compute the under and over-approximation of range$(f^k, \boldsymbol{z}^0)$, i.e. the loop body f iterated k times, starting from the initial state $\boldsymbol{z}^0$. This yields the schematic Algorithm 2. At each step

Algorithm 2 Discrete-time reachability computed on f^k

for k from 0 to $K-1$ **do**
$I^{k+1} := \mathcal{I}(f^{k+1}, \boldsymbol{z}^0, \pi)$, $O^{k+1} := \mathcal{O}(f^{k+1}, \boldsymbol{z}^O, \pi)$
end for

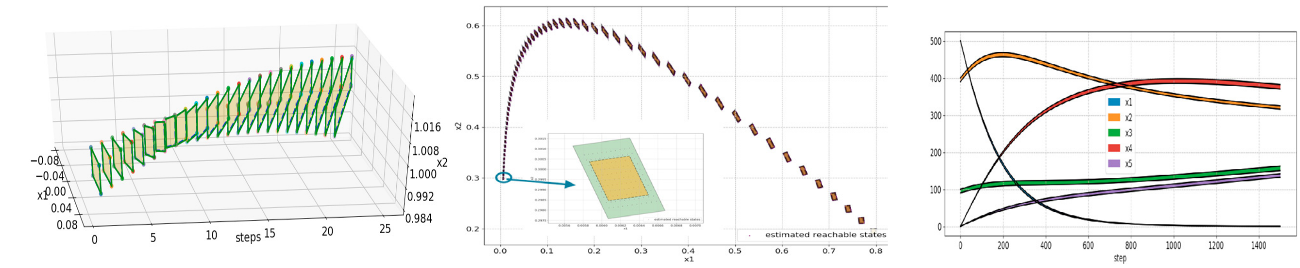
k, the under- and over-approximation are both obtained from over-approximations of f^{k+1} and its gradient.

Discussion While relying on the same techniques for range estimation, Algorithm 1 and 2 are different: Algorithm 1 needs at each step a non-empty under-approximating box or skew box of the vector-valued reachable set of states, and precision will be lost and not recovered when this set is not well approximated by a skew box. Algorithm 2 relies only on the propagation of over-approximations to deduce under-approximations. In particular, the under-approximation may be empty at some step, and become non-empty again at further steps (a similar remark was made for continuous systems in Goubault and Putot (2017)). Algorithm 2 is more costly as it requires a differentiation of the iterated function.

6. IMPLEMENTATION AND EXAMPLES

The approach is implemented as part of the RINO prototype, available from `https://github.com/cosynus-lix/RINO`. The prototype performs function range estimations, discrete-time and continuous-time reachability.

Test Model We consider the test model of Dreossi et al. (2016), with same initial conditions and parameter values. Figure 2a shows the under and over-approximated reachable sets (respectively the filled yellow region and green parallelotope) over time up to 25 steps with Algorithm 1. They are obtained in 0.02 seconds. The under and over-approximations are very close one to another, confirming the accuracy of the results.



(a) Skewed box approximations (Algorithm 1) for the test model

(b) Skewed box approximations (Algorithm 1) for the SIR epidemic model

(c) Projected approximations (Algorithm 2) for the bees model

Fig. 2. Under and over-approximations for the 3 discrete systems

SIR Epidemic Model We consider the SIR epidemic model with the parameters of Dreossi et al. (2016). We compute the reachable set up to 60 steps from the initial box $(x_1, x_2, x_3) \in [0.79, 0.80] \times [0.19, 0.20] \times [0, 0.1]$. The vector-valued reachable sets (x_1, x_2) computed in 0.05 seconds with Algorithm 1 up to 60 steps are represented in Figure 2b. We can note in particular from the zoomed reachable set in the figure, which corresponds to last step (60), that the under-approximation (in yellow) is still of good quality (the purple dots correspond to sample executions). However, only Algorithm 2 is able to compute, also in 0.05 seconds, non-empty (and actually very tight) approximations when taking as initial condition $x_3 = 0$ which is of empty interior, instead of $x_3 \in [0, 0.1]$.

Honeybees Site Choice Model We consider the reachable sets up to 1500 steps of the 5-dimensional Honeybees model studied in Dreossi et al. (2016). Algorithm 1 takes only 1.7 seconds but yields rather imprecise results. Algorithm 2 takes 57 seconds, but the projected under-approximations are very tight, close to the over-approximations, as can be seen on Figure 2c which represents the approximations for all components as functions of steps. These results can be compared to Figure 7 in Dreossi et al. (2016), obtained in 81 seconds. Our approach is slightly faster and provides tighter over-approximation while solving the much more involved under-approximation problem.

7. CONCLUSION AND FUTURE WORK

We focused on new AE under-approximating extensions and their accurate practical evaluation for non-linear vector-valued functions, and exemplified their interest for the reachability of discrete-time systems. These techniques can also be used for the reachability analysis of continuous-time systems, improving for instance over Goubault and Putot (2019); Goubault and Putot (2020).

REFERENCES

Chen, M., Herbert, S., and Tomlin, C.J. (2016). Exact and efficient Hamilton-Jacobi-based guaranteed safety analysis via system decomposition.

Chen, X., Sankaranarayanan, S., and Ábrahám, E. (2014). Under-approximate flowpipes for non-linear continuous systems. In *FMCAD*.

Dreossi, T., Dang, T., and Piazza, C. (2016). Parallelotope bundles for polynomial reachability. In *HSCC*.

Girard, A., Le Guernic, C., and Maler, O. (2006). Efficient computation of reachable sets of linear time-invariant systems with inputs. In *HSCC*, 257–271.

Goldsztejn, A. (2012a). Modal intervals revisited, part 1: A generalized interval natural extension. *Reliable Computing*, 16, 130–183.

Goldsztejn, A. (2012b). Modal intervals revisited, part 2: A generalized interval mean value extension. *Reliable Computing*, 16, 184–209.

Goldsztejn, A. and Jaulin, L. (2010). Inner approximation of the range of vector-valued functions. *Reliable Computing*, 14.

Goubault, E. and Putot, S. (2017). Forward inner-approximated reachability of non-linear continuous systems. In *HSCC*. ACM.

Goubault, E. and Putot, S. (2019). Inner and outer reachability for the verification of control systems. In *HSCC*.

Goubault, E. and Putot, S. (2020). Robust under-approximations and application to reachability of non-linear control systems with disturbances. *IEEE Control Systems Letters*, 4(4), 928–933.

Kochdumper, N. and Althoff, M. (2020). Computing non-convex inner-approximations of reachable sets for nonlinear continuous systems. In *CDC*.

Korda, M., Henrion, D., and Jones, C.N. (2013). Inner approximations of the region of attraction for polynomial dynamical systems. In *NOLCOS*.

Kurzhanski, A.B. and Varaiya, P. (2000). Ellipsoidal techniques for reachability analysis. In *HSCC*, 202–214.

Mitchell, I.M. (2007). Comparing forward and backward reachability as tools for safety analysis. In *HSCC*.

Mézo, T.L., Jaulin, L., and Zerr, B. (2018). Bracketing the solutions of an ordinary differential equation with uncertain initial conditions. *Applied Mathematics and Computation*, 318.

Xue, B., Fränzle, M., and Zhan, N. (2020). Inner-approximating reachable sets for polynomial systems with time-varying uncertainties. *IEEE Transactions on Automatic Control*, 65(4), 1468–1483.

Xue, B., She, Z., and Easwaran, A. (2016). Under-approximating backward reachable sets by polytopes. In *Computer Aided Verification*.