Inner and Outer Reachability for the Verification of Control Systems

Eric Goubault
LIX, Ecole Polytechnique, CNRS
91128 Palaiseau, France
goubault@lix.polytechnique.fr

Sylvie Putot
LIX, Ecole Polytechnique, CNRS
91128 Palaiseau, France
putot@lix.polytechnique.fr

ABSTRACT

We investigate the information and guarantees provided by different inner and outer approximated reachability analyses, for proving properties of dynamical systems. We explore the connection of these approximated sets with the maximal and minimal reachable sets of Mitchell [31], with an additional notion of robustness to disturbance. We demonstrate the practical use of a specific computation of these approximated reachable sets. We revisit in particular the reach-avoid properties.

KEYWORDS

reachability analysis, inner-approximation, under-approximation, robustness, safety verification, abstractions, Taylor models

ACM Reference Format:
Eric Goubault and Sylvie Putot. 2019. Inner and Outer Reachability for the Verification of Control Systems. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '19), April 16–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3302504.3311794

1 INTRODUCTION

Verifying properties of control systems usually involves rigorously proving that a dynamical system, subject to uncertain initial conditions, parameters, and environment, will eventually reach a region of the state-space, while avoiding some unsafe set of states. Analytical verification of such properties is generally impossible, as well as computing exact reachable sets for nonlinear systems. Different algorithms have been proposed to compute safe outer (or over) approximations of reachable states of the system. When the outer-approximations are tight enough, they are often sufficient to prove the property. However, when the property cannot be proved, we are facing the question of whether this is a false alarm, or the property is indeed not satisfied. Computing an inner (or under) approximation of the reachable set is a possible though still very little explored way to prove that there exist executions of the system that are guaranteed to reach an unsafe state.

For systems involving external disturbances, a stronger property is proving that some (unsafe) states are always reached, whatever these disturbances, for some control signal or input parameters. This is what we define as robust inner-approximations, and we propose a general algorithm to compute them for non-linear dynamical systems. This algorithm extends the approach of [19] in two ways. First, we introduce here the notion of robustness to a possible disturbance. Second, we allow the input signal to be time-dependent.

Another contribution of this work is to relate the notions of inner-approximating reachable sets that we introduce, to the notions of minimal and maximal reachable sets of Mitchell [31]. This constitutes a starting point to demonstrate how the combination of inner and outer approximations of reachable sets can be used to prove or falsify reach-avoid properties, where regions to reach or avoid can be moving regions, and possibly in presence of a disturbance in the system. We also demonstrate that we can prove some new properties, such as the sweep-avoid property, where the target region is proved to be fully covered by executions of the system. We illustrate these contributions using our prototype implementation.

Related work. Reachability properties have been extensively studied for a wide number of system models, ODEs, DDEs, discrete systems, hybrid systems. As they are in general undecidable, numerous methods have been proposed to outer-approximate (or over-approximate) flowpipes and reachable sets. Fewer methods have been proposed for inner-approximations. These methods follow either a Lagrangian approach, which follows the flow of the system, or an Eulerian method, which models the dynamics of a system by looking at how it flows through fixed sets.

Lagrangian methods are generally based on set-based methods, and are generally scalable. For linear ODEs, sub-polyhedral or ellipsoidal abstractions are generally used for outer-approximations [13, 14] and for inner-approximations [14, 26]. Several approaches exist for outer-approximations of non-linear ODEs [1, 5, 9, 33, 34]. For inner-approximations, both forward Taylor model based [19] and backward methods [6, 39] have been recently proposed. These methods have also been extended to Delay Differential Equations [20, 38], that appear naturally when modeling networked control systems, where delays are introduced in the feedback loop.

Eulerian methods, generally based on Hamilton-Jacobi-Bellman's equation [3] are known to be in general less tractable, but more expressive, solving generalized reachability problems, such as reach-avoid properties [11] and extensions to differential games such as pursuit-evasion, reach-avoid-capture, and control/path-planning synthesis [40]. For polynomial systems of ODEs, computations of inner-approximations of the region of attraction [25] and of the reachable set [37], based on the formulation as solutions to the Hamilton-Jacobi partial differential equations, have been proposed.

Important verification properties also include stability or controllability, and the computation of invariants or viability kernels.

HSCC '19, April 16–18, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6282-5/19/04…$15.00
https://doi.org/10.1145/3302504.3311794

Let us mention related work that involve both outer and inner-approximation. Approximations of reachable sets can be used to characterize these invariants or viability kernels, see e.g. [23], where the authors compute inner-approximations of the viability kernel by backward inner-approximated reachability, using the ellipsoidal methods of [26]. Recently, an interval-based method [30] was introduced for bracketing between inner and outer approximations the positive invariant set of a system without relying on integration. However, it relies on space discretization and has only been applied successfully, as far as we know, to low dimensional systems.

Reachability properties naturally concern systems with uncertainties. Whether these should be seen as controllable, non-deterministic, or even a stochastic noise, has also been discussed in some papers, e.g. [24, 29, 31, 35], where so-called minimal and maximal reachable sets have been introduced. The natural question of what these - forward or backward - reachable sets can help prove about control systems is also discussed there.

Our work proposes a set-based Lagrangian approach to semi-decide verification properties such as target reachability while avoiding unsafe regions, extending the previous Lagrangian approaches to more general, possibly time-varying, uncertainties, including a controllable part and non-controllable disturbances.

2 MINIMAL, ROBUST AND MAXIMAL REACHABLE SETS

We consider general systems of parametric ODEs, possibly non-linear, or even non-polynomial, of the form:

$$\begin{cases} \dot{z}(t) = f(z(t), u(t)) & \text{if } t \geq 0 \\ z(t) = z_0 & \text{if } t = 0 \end{cases} \tag{1}$$

where the continuous vector $z(t)$ belongs to the state-space domain $\mathcal{D} \subseteq \mathbb{R}^n$, the initial value is defined by $z(0) = z_0 \in \mathcal{D}$, and the input signal u belongs to $\mathbb{U} = \{\phi : \mathbb{R}^+ \to \mathcal{U}\}$, where $\mathcal{U} \subseteq \mathbb{R}^m$. Function $f : \mathcal{D} \times \mathcal{U} \to \mathcal{D}$ is assumed sufficiently smooth on $\mathcal{D} \subseteq \mathbb{R}^n$ (at least C^1, and more when we will use higher order Taylor models). Controls $u \in \mathbb{U}$ are also supposed to be sufficiently smooth C^k for some $k \geq 0$ stepwise. This allows discontinuous controls, where the discontinuities can only appear at discrete times t_j, corresponding to general switched systems with time-dependent switches [27].

We make the assumption through the paper, that given an initial state, and the input signal, there exists a unique solution or trajectory of the dynamical system (1) for all time $t \in \mathbb{T} = [0, T_{\max}]$. Let $\varphi^f(t; z_0, u)$ for time $t \in \mathbb{T}$ denote the *time trajectory* of (1) with initial state $z(0) = z_0$, and for input signal u.

We are interested in the sets of states z reachable by trajectories of the system, starting with z_0 in an initial set Z_0. We call *reachable set* the set of states reachable by trajectories at a specified time t, and *reachable tube* or *flowpipe* the set of states reachable by trajectories over all times prior to and including the specified time.

Following [31], we now define forward maximal and minimal reachability, depending whether the input u is used to maximize or minimize the width of the reachable set.

Maximal reachability. Given a vector of uncertain input signal u defined in the set $\mathbb{U}$, we use the subscript $\mathcal{E}$ to denote the *maximal reachable set or tube*, where we seek the input signal that maximizes the size of the reachable set. In this case, u will correspond to a controllable input signal, which is existentially quantified, hence the $\mathcal{E}$ subscript notation.

$$R^f_{\mathcal{E}}(t; Z_0, \mathbb{U}) = \{z \in \mathcal{D} \mid \exists u \in \mathbb{U}, \exists z_0 \in Z_0,\ z = \varphi^f(t; z_0, u)\}$$

$$R^f_{\mathcal{E}}([0,t]; Z_0, \mathbb{U}) = \{z \in \mathcal{D} \mid \exists u \in \mathbb{U}, \exists z_0 \in Z_0, \\ \exists s \in [0,t], z = \varphi^f(s; z_0, u)\}$$

Minimal reachability. We use the subscript $\mathcal{A}$ to denote the *minimal reachable set*, where we want to compute only states that trajectories will reach whatever the input signal is.

$$R^f_{\mathcal{A}}(t; Z_0, \mathbb{U}) = \{z \in \mathcal{D} \mid \forall u \in \mathbb{U}, \exists z_0 \in Z_0,\ z = \varphi^f(t; z_0, u)\}$$

$$R^f_{\mathcal{A}}([0,t]; Z_0, \mathbb{U}) = \{z \in \mathcal{D} \mid \forall u \in \mathbb{U}, \exists z_0 \in Z_0, \\ \exists s \in [0,t], z = \varphi^f(s; z_0, u)\}$$

In this case, u will correspond to an uncontrollable disturbance, with respect to which the behavior of the system must be robust, and it is universally quantified.

Robust reachability. Finally, we generalize the definitions above by using the subscript $\mathcal{AE}$ to define the reachable set which is maximal with respect to some dimensions of the input (vector) defined by the subset of indices $I_{\mathcal{E}}$, and minimal or robust with respect to the remaining dimensions $I_{\mathcal{A}}$, that represent the disturbance part of the input signal. Let $u = (u_{\mathcal{A}}, u_{\mathcal{E}}) \in \mathbb{U} = (\mathbb{U}_{\mathcal{A}}, \mathbb{U}_{\mathcal{E}})$, where $u_{\mathcal{A}}$ (resp $u_{\mathcal{E}}$) contains the components of u corresponding to indices $I_{\mathcal{A}}$ (resp $I_{\mathcal{E}}$), and $\mathbb{U}_{\mathcal{A}}$ (resp $\mathbb{U}_{\mathcal{E}}$) is the corresponding domain of definition. We define the *robustly reachable set*, robust with respect to $u_{\mathcal{A}}$, by:

$$R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \{z \in \mathcal{D} \mid \forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \\ \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists z_0 \in Z_0,\ z = \varphi^f(t; z_0, u)\}$$

We define $R^f_{\mathcal{AE}}([0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ similarly.

Remark 1. *Note that the order on quantifiers in this notion of robustness is backwards compared to classical formulations [31]. But we can also indirectly revisit expressions with the stronger classical order on quantifiers, as noted in Section 4.4.*

Remark 2. *Consider two partitions $(I^1_{\mathcal{A}}, I^1_{\mathcal{E}})$ and $(I^2_{\mathcal{A}}, I^2_{\mathcal{E}})$ of I. If $I^1_{\mathcal{E}} \subseteq I^2_{\mathcal{E}}$, then $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I^1_{\mathcal{A}}, I^1_{\mathcal{E}}) \subseteq R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I^2_{\mathcal{A}}, I^2_{\mathcal{E}})$. In particular, when there is no controllable component in the input, or $I_{\mathcal{E}} = \emptyset$, we have $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I, \emptyset) = R^f_{\mathcal{A}}(t; Z_0, \mathbb{U})$, and when there is no disturbance in the input, or $I_{\mathcal{A}} = \emptyset$, we have $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, \emptyset, I) = R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$. Then, for any partition $(I_{\mathcal{A}}, I_{\mathcal{E}})$ of I, $R^f_{\mathcal{A}}(t; Z_0, \mathbb{U}) \subseteq R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$.*

Remark 3. *We could also split the parameters that appear in the initial condition in a controllable and a disturbance part, as for the input signal. We chose not to do so to stick to the definitions of the minimal reachable sets of Mitchell [31].*

We are interested here in computable abstractions:

Definition 2.1 (Inner and outer approximations of the reachable sets). Let two sets $\mathcal{I}_{\mathcal{A}\mathcal{E}}$ and $\mathcal{O}_{\mathcal{A}\mathcal{E}}$ such that

$$\mathcal{I}_{\mathcal{A}\mathcal{E}} \subseteq R^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \subseteq \mathcal{O}_{\mathcal{A}\mathcal{E}}.$$

We call $\mathcal{I}_{\mathcal{A}\mathcal{E}}$ a *robust inner-approximation*, and $\mathcal{O}_{\mathcal{A}\mathcal{E}}$ a *robust outer-approximation.* robust with respect to disturbance $u_{\mathcal{A}}$.

When $I_{\mathcal{E}} = \emptyset$, we call $\mathcal{I}_{\mathcal{A}\mathcal{E}} = \mathcal{I}_{\mathcal{A}}$ a *minimal inner-approximation* and $\mathcal{O}_{\mathcal{A}\mathcal{E}} = \mathcal{O}_{\mathcal{A}}$ a *minimal outer-approximation.*

When $I_{\mathcal{A}} = \emptyset$, we call $\mathcal{I}_{\mathcal{A}\mathcal{E}} = \mathcal{I}_{\mathcal{E}}$ a *maximal inner-approximation* and $\mathcal{O}_{\mathcal{A}\mathcal{E}} = \mathcal{O}_{\mathcal{E}}$ a *maximal outer-approximation.*

Example 2.2. We consider a basic PD-controller, controlling a car's position x and velocity v by adjusting its acceleration depending on the current distance to a reference position p_r:

$$\begin{cases} x'(t) = v(t) \\ v'(t) = -K_p\big(x(t) - p_r\big) - K_d\, v(t) \end{cases}$$

with initial condition $(x(0), v(0)) \in [-0.1, 0.1] \times [0, 0.1]$. The parameters K_p and K_d of the PD-controller are uncertain and bounded by $(K_p, K_d) \in [1.95, 2.05] \times [2.95, 3.05]$. The maximal reachable set is the set of states that can be reached for some initialization of x and v, and some value of K_p and K_d. The minimal reachable set is the set of states that can be reached, whatever the values of K_p and K_d, for some initialization of x and v. Finally, we will be interested in the set of states that can be reached, whatever the values of K_d, for some value of K_p and some initialization of x and v. In that last case, only K_p will be considered as a control parameter. Inner and outer-approximations of these sets are represented in Figure 1.

In the next section, we propose a computation of these outer and inner-approximations.

3 COMPUTING INNER AND OUTER APPROXIMATIONS

3.1 Generalized interval computations

Set valued quantities, scalar or vector valued, corresponding to uncertain inputs or parameters, will be noted with bold letters, e.g $\boldsymbol{x}$, throughout the paper. An outer-approximating extension of a function $f : \mathbb{R}^m \to \mathbb{R}^n$ is a function $[\boldsymbol{f}] : \mathcal{P}(\mathbb{R}^m) \to \mathcal{P}(\mathbb{R}^n)$, such that for all $\boldsymbol{x}$ in $\mathcal{P}(\mathbb{R}^m)$, $\mathrm{range}(f, \boldsymbol{x}) = \{f(x), x \in \boldsymbol{x}\} \subseteq [\boldsymbol{f}](\boldsymbol{x})$. Dually, inner-approximations determine a set of values proved to belong to the range of the function over some input set. An 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 $\mathcal{P}(\mathbb{R}^m)$, $]\boldsymbol{f}[(\boldsymbol{x}) \subseteq \mathrm{range}(f, \boldsymbol{x})$. Inner and outer approximations can be interpreted as quantified propositions: $\mathrm{range}(f, \boldsymbol{x}) \subseteq \boldsymbol{z}$ can be written $\forall x \in \boldsymbol{x}, \exists z \in \boldsymbol{z}, f(x) = z$, while $\boldsymbol{z} \subseteq \mathrm{range}(f, \boldsymbol{x})$ can be written $\forall z \in \boldsymbol{z}, \exists x \in \boldsymbol{x}, f(x) = z$.

Classical intervals [32] are used in many situations to rigorously compute with interval domains instead of reals, usually leading to outer-approximations of function ranges over boxes. Intervals are non-relational abstractions, in the sense that they rigorously approximate independently each component of a vector function f. We thus consider in this section 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 interval $\boldsymbol{x}$. Then, the mean-value theorem implies that $\forall x_0 \in \boldsymbol{x}, \forall x \in \boldsymbol{x}, \exists c \in \boldsymbol{x}, f(x) = f(x_0) + f'(c)(x - x_0)$. If we can bound the range of the gradient of f over $\boldsymbol{x}$, by $[\boldsymbol{f'}](\boldsymbol{x})$, then we can derive the following interval enclosure, called the mean-value extension: for any $x_0 \in \boldsymbol{x}$, $\mathrm{range}(f, \boldsymbol{x}) \subseteq f(x_0) + [\boldsymbol{f'}](\boldsymbol{x})(\boldsymbol{x} - x_0)$.

The results introduced here rely on work by Goldsztejn *et al.* [16–18] on modal intervals. Let us first introduce the set of generalized intervals, denoted by $\mathbb{IK} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \in \mathbb{R}, \overline{x} \in \mathbb{R}\}$. Given two real numbers $\underline{x}$ and $\overline{x}$, with $\underline{x} \le \overline{x}$, one can consider two generalized intervals, $[\underline{x}, \overline{x}]$, which is called *proper*, and $[\overline{x}, \underline{x}]$, which is called *improper*. We define $\mathrm{dual}([a, b]) = [b, a]$ and $\mathrm{pro}([a, b]) = [\min(a, b), \max(a, b)]$.

Definition 3.1 ([18]). Let $f : \mathbb{R}^m \to \mathbb{R}$ be a continuous function and $\boldsymbol{x} \in \mathbb{IK}^m$, which we can decompose in $\boldsymbol{x}_{\mathcal{A}} \in \mathbb{IR}^p$ and $\boldsymbol{x}_{\mathcal{E}} \in (\mathrm{dual}\, \mathbb{IR})^q$ with $p + q = m$. A generalized interval $\boldsymbol{z} \in \mathbb{IK}$ is $(f, \boldsymbol{x})$-interpretable if

$$\forall x_{\mathcal{A}} \in \boldsymbol{x}_{\mathcal{A}},\ Q_z z \in \mathrm{pro}\, \boldsymbol{z},\ \exists x_{\mathcal{E}} \in \mathrm{pro}\, \boldsymbol{x}_{\mathcal{E}},\ f(x) = z \qquad (2)$$

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

When all intervals are proper, (2) corresponds to classical interval computation, which gives an outer-approximation of $\mathrm{range}(f, \boldsymbol{x})$, or $\forall x \in \boldsymbol{x}, \exists z \in [\boldsymbol{z}], f(x) = z$. When all intervals are improper, (2) yields an inner-approximation of $\mathrm{range}(f, \boldsymbol{x})$, or $\forall z \in]\,\mathrm{pro}\, \boldsymbol{z}[, \exists x \in \mathrm{pro}\, \boldsymbol{x}, f(x) = z$.

Kaucher arithmetic [22] provides a computation on generalized intervals that is $(f, \boldsymbol{x})$-interpretable in some simple cases. Kaucher addition extends addition on classical intervals by $\boldsymbol{x} + \boldsymbol{y} = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $\boldsymbol{x} - \boldsymbol{y} = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$. For multiplication, let us decompose $\mathbb{IK}$ 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 $\mathrm{dual}\, \mathcal{Z} = \{\boldsymbol{x} = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$. Kaucher multiplication $\boldsymbol{xy}$ extends the classical multiplication to all possible combinations of $\boldsymbol{x}$ and $\boldsymbol{y}$ belonging to these sets. We refer to [18, 22] for more details. Kaucher arithmetic defines a generalized interval natural extension:

Proposition 3.2 ([16, 18]). *Let $f : \mathbb{R}^m \to \mathbb{R}$ be a function, given by an arithmetic expression where each variable appears syntactically only once (and with degree 1). Then for $\boldsymbol{x} \in \mathbb{IK}^m$, $f(\boldsymbol{x})$, computed using Kaucher arithmetic, is $(f, \boldsymbol{x})$-interpretable.*

In some cases, Kaucher arithmetic can thus be used to compute an inner-approximation of $\mathrm{range}(f, \boldsymbol{x})$. But the restriction to f with single occurrences of variables, that is with no dependency, prevents a wide use. A generalized interval mean-value extension allows us to overcome this limitation:

Theorem 3.3 ([17, 18]). *Let $f : \mathbb{R}^m \to \mathbb{R}$ be differentiable, $\boldsymbol{x} \in \mathbb{IK}^m$. Suppose that for each $i \in \{1, \dots, m\}$, we can compute $\boldsymbol{\Delta}_i \in \mathbb{IR}$ such that*

$$\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \mathrm{pro}\, \boldsymbol{x} \right\} \subseteq \boldsymbol{\Delta}_i. \qquad (3)$$

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

$$\tilde{f}(\boldsymbol{x}) = f(\tilde{x}) + \sum_{i=1}^{n} \boldsymbol{\Delta}_i(\boldsymbol{x}_i - \tilde{x}_i). \qquad (4)$$

When using (4) for inner-approximation, we can only get the following subset of possible cases in the Kaucher multiplication table: $(\boldsymbol{x} \in \mathcal{P}) \times (\boldsymbol{y} \in \text{dual}\,\mathcal{Z}) = [\underline{x}\underline{y}, \underline{x}\overline{y}]$, $(\boldsymbol{x} \in -\mathcal{P}) \times (\boldsymbol{y} \in \text{dual}\,\mathcal{Z}) = [\overline{x}\overline{y}, \overline{x}\underline{y}]$, and $(\boldsymbol{x} \in \mathcal{Z}) \times (\boldsymbol{y} \in \text{dual}\,\mathcal{Z}) = 0$. Indeed, for an improper $\boldsymbol{x}$, and $\tilde{x} \in \text{pro}\,\boldsymbol{x}$, it holds that $(\boldsymbol{x} - \tilde{x})$ is in $\text{dual}\,\mathcal{Z}$. The outer-approximation Δ_i of the Jacobian is a proper interval, in $\mathcal{P}$, $-\mathcal{P}$ or $\mathcal{Z}$. We deduce from the multiplication rules that the inner-approximation is non empty only if Δ_i does not contain 0.

Example 3.4. Let $f(x) = x^2 - x$, we want an inner-approximation of its range over $\boldsymbol{x} = [2, 3]$. Due to the two occurrences of x, $f(\text{dual}\,\boldsymbol{x})$, computed with Kaucher arithmetic, is not $(f, \boldsymbol{x})$-interpretable. The interval $\tilde{f}(\boldsymbol{x}) = f(2.5) + f'([2, 3])(\boldsymbol{x} - 2.5) = 3.75 + [3, 5](\boldsymbol{x} - 2.5)$ 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 $\mathcal{P} \times \text{dual}\,\mathcal{Z}$, we get

$$\begin{aligned} \tilde{f}(\boldsymbol{x}) &= 3.75 + [3, 5]([3, 2] - 2.5) = 3.75 + [3, 5][0.5, -0.5] \\ &= 3.75 + [1.5, -1.5] = [5.25, 2.25] \end{aligned} \quad (5)$$

Thus, $[2.25, 5.25]$ is an inner-approximation of $\text{range}(f, [2, 3])$.

3.2 Application to reachable sets

In this section, we express maximal, minimal and robust inner and outer approximations for reachable sets as quantified $\mathcal{AE}$ expressions, where universal (forall) quantifiers always precede existential (exists) quantifiers, such as defined in Section 3.1. This will then allow us to use Theorem 3.3 with f being each component (for a n-dimensional system) of the trajectories of system (1), in order to compute minimal robust and maximal inner, and maximal outer, approximations for reachable sets. An additional argument allows us to extend this computation in Proposition 3.7 to robust and minimal outer-approximations.

We consider here the approximation of reachable sets, at a given t, but the approach can be generalized to the approximation of reachable tubes or flowpipes.

Lemma 3.5. *Let $\mathcal{I}_{\mathcal{AE}}$ be a set such that $\forall z \in \mathcal{I}_{\mathcal{AE}}$, $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, $\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$, $\exists z_0 \in Z_0$, $\varphi^f(t; z_0, u) = z$. Then $\mathcal{I}_{\mathcal{AE}}$ is a robust inner-approximation, robust to disturbances $u_{\mathcal{A}}$, in the sense of Definition 2.1. Furthermore, such sets $\mathcal{I}_{\mathcal{AE}}$ have a supremum, equal to $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.*

This includes the particular cases of minimal and maximal innner-approximations. When $I_{\mathcal{E}} = \emptyset$, then $\mathcal{I}_{\mathcal{AE}} = \mathcal{I}_{\mathcal{A}}$ such that $\forall z \in \mathcal{I}_{\mathcal{A}}$, $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, $\exists z_0 \in Z_0$, $\varphi^f(t; z_0, u) = z$ defines a minimal inner-approximation (an inner-approximation of the minimal reachable set $R^f_{\mathcal{A}}$). When $I_{\mathcal{A}} = \emptyset$, then $\mathcal{I}_{\mathcal{AE}} = \mathcal{I}_{\mathcal{E}}$ such that $\forall z \in \mathcal{I}_{\mathcal{E}}$, $\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$, $\exists z_0 \in Z_0$, $\varphi^f(t; z_0, u) = z$ defines a maximal inner-approximation (an inner-approximation of the maximal reachable set $R^f_{\mathcal{E}}$).

The situation is a little more subtle for robust outer-approximations: Lemma 3.6 is weaker than its counterpart Lemma 3.5 for robust inner-approximations.

Lemma 3.6. *Let $\mathcal{O}_{\mathcal{AE}}$ be a set such that $\forall u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$, $\forall z_0 \in Z_0$, $\exists u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, $\exists z \in \mathcal{O}_{\mathcal{AE}}$, $\varphi^f(t; z_0, u) = z$. In the case when $I_{\mathcal{A}} = \emptyset$, set $\mathcal{O}_{\mathcal{AE}} = \mathcal{O}_{\mathcal{E}}$ is such that $\forall u \in \mathbb{U}$, $\forall z_0 \in Z_0$, $\exists z \in \mathcal{O}_{\mathcal{E}}$, $\varphi^f(t; z_0, u) = z$ and defines a maximal outer-approximation (an outer-approximation of the maximal reachable set $R^f_{\mathcal{E}}$). Moreover, the infimum of sets $\mathcal{O}_{\mathcal{E}}$ is equal to $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$.*

In the general case of non empty $I_{\mathcal{A}}$, we can only state that outer-approximations of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ can be expressed as such quantified sets $\mathcal{O}_{\mathcal{AE}}$ (but not that all such $\mathcal{O}_{\mathcal{AE}}$ define robust outer-approximations). However, the particular set $\mathcal{O}_{\mathcal{AE}}$ computed by the generalized mean-value extension of Theorem 3.3 yields a robust outer-approximation:

Proposition 3.7 (Computing a robust outer-approximation). *Under the hypotheses of Theorem 3.3, with $\boldsymbol{x} = (\boldsymbol{x}_{\mathcal{A}}, \boldsymbol{x}_{\mathcal{E}}) \in \mathbb{IR}^m$. For any $\tilde{x} \in \boldsymbol{x}$, if $\mathcal{O}^f_{\mathcal{AE}}(\boldsymbol{x}, \tilde{x})$ defined by*

$$\mathcal{O}^f_{\mathcal{AE}}(\boldsymbol{x}, \tilde{x}) = f(\tilde{x}) + \Delta_{\mathcal{A}}(\text{dual}\,\boldsymbol{x}_{\mathcal{A}} - \tilde{x}_{\mathcal{A}}) + \Delta_{\mathcal{E}}(\boldsymbol{x}_{\mathcal{E}} - \tilde{x}_{\mathcal{E}}) \quad (6)$$

evaluated with Kaucher interval arithmetic, is proper, then it is an outer-approximation of $\{z \mid \forall x_{\mathcal{A}} \in \boldsymbol{x}_{\mathcal{A}}, \exists x_{\mathcal{E}} \in \boldsymbol{x}_{\mathcal{E}}, z = f(x)\}$.

In the next section, we will obtain a robust outer-approximation of the reachable set $R^f_{\mathcal{AE}}([0, t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ by applying Proposition 3.7 to f being the solution φ^f of the uncertain system. Let us first exemplify Proposition 3.7 on a simple function f.

Example 3.8. Let $f(x_{\mathcal{A}}, x_{\mathcal{E}}) = x_{\mathcal{A}} x_{\mathcal{E}}$, we want to compute inner and outer approximations of $\mathcal{R}^f_{\mathcal{AE}}([3, 5] \times [1, 3]) = \{z \mid \forall x_{\mathcal{A}} \in \boldsymbol{x}_{\mathcal{A}} = [3, 5], \exists x_{\mathcal{E}} \in \boldsymbol{x}_{\mathcal{E}} = [1, 3], z = f(x)\}$. It is easy to verify that $\mathcal{R}^f_{\mathcal{AE}}([3, 5] \times [1, 3]) = [5, 9]$, and that the range of f on $[3, 5] \times [1, 3]$ is $[3, 15]$. From Proposition 3.7, taking $\tilde{x}$ to be the center $(4, 2)$ of box $\boldsymbol{x} = [3, 5] \times [1, 3]$, we define

$$\mathcal{O}^f_{\mathcal{AE}} = 2 \times 4 + \Delta_{\mathcal{A}}([5, 3] - 4) + \Delta_{\mathcal{E}}([1, 3] - 2),$$

where we can substitute $\Delta_{\mathcal{A}} = [1, 3]$ and $\Delta_{\mathcal{E}} = [3, 5]$, yielding

$$\begin{aligned} \mathcal{O}^f_{\mathcal{AE}} &= 8 + [1, 3]([1, -1]) + [3, 5]([-1, 1]) = 8 + [1, -1] + [-5, 5] \\ &= [4, 12] \supseteq [5, 9] = \mathcal{R}^f_{\mathcal{AE}}([3, 5] \times [1, 3]). \end{aligned}$$

We can also use Theorem 3.3 for robust inner-approximation: if $\mathcal{I}^f_{\mathcal{AE}} = 8 + [1, 3](\boldsymbol{x}_{\mathcal{A}} - \tilde{x}_{\mathcal{A}}) + [3, 5](\text{dual}\,\boldsymbol{x}_{\mathcal{E}} - \tilde{x}_{\mathcal{E}})$ is an improper interval, then it gives an inner-approximation of $\mathcal{R}^f_{\mathcal{AE}}(\boldsymbol{x})$. Here, the robust inner-approximation is reduced to a point:

$$\mathcal{I}^f_{\mathcal{AE}} = 8 + [1, 3]([3, 5] - 4) + [3, 5]([3, 1] - 2) = 8 + [-3, 3] + [3, -3] = 8.$$

Still with Theorem 3.3, but taking both input components as improper (existentially quantified), we can also compute a maximal inner-approximation: if $\mathcal{I}^f_{\mathcal{E}} = 8 + [1, 3]([5, 3] - 4) + [3, 5]([3, 1] - 2)$ is an improper interval, then its proper counterpart is an inner-approximation of the range of f over box $\boldsymbol{x}$. We obtain $\mathcal{I}^f_{\mathcal{AE}} = 8 + [1, -1] + [3, -3] = [12, 4]$, proving that $[4, 12]$ is an inner-approximation of the range of f on $[3, 5] \times [1, 3]$ (the exact range being $[3, 15]$).

3.3 Computing robust inner and outer approximated reachable sets

We now use Theorem 3.3 to compute inner-approximations from outer-approximations, following [19]. We also show, as a novelty compared to [19], that we can compute inner-approximations of minimal, robust and maximal reachable sets. Additionally, we use Proposition 3.7 to obtain robust and minimal outer-approximations (maximal outer-approximations being obtained classically with Taylor models, as described in Section 3.3.1). We first consider the case where the input $u(t)$ is constant in time, and is simply noted u. We then discuss the case of time dependent signal in Section 3.3.4.

The main idea is to instantiate in the generalized mean-value theorem, the function f as the solution of system (1), and parameter x as the uncertain initial condition z_0 and input u. We first need to compute:

1. a maximal outer-approximation $\tilde{O}^f_{\mathcal{E}}(t)$ of the trajectory $\varphi^f(t;\tilde{z_0},\tilde{u})$ for a given $(\tilde{z_0},\tilde{u}) \in \boldsymbol{Z}_0 \times \boldsymbol{U}$.
2. a maximal outer-approximation $O^F_{\mathcal{E}}(t)$ of the sensitivity or Jacobian matrix $J(t;\boldsymbol{Z}_0,\boldsymbol{U})$ with respect to uncertain initial condition z_0 and input u, over the range $\boldsymbol{Z}_0 \times \boldsymbol{U}$.

Computing these maximal outer-appproximations is classical, we can for instance use Taylor model methods, as described in Section 3.3.1. In Section 3.3.2, we explicit the differential system satisfied by the sensitivity matrix: the method of Section 3.3.1 can again be used to compute a maximal outer-approximation of its dynamics.

3.3.1 Taylor models for outer enclosure of the maximal reachable set. Consider the uncertain dynamical system (1). We define a time grid $t_0 = 0 < t_1 < \ldots < t_N$. Taylor methods for guaranteed set integration, see [33] for a review, compute on each time interval $[t_j, t_{j+1}]$ of the grid, a Taylor model (7) that defines a flowpipe guaranteed to contain the maximal reachable set $R^f_{\mathcal{E}}(t;\boldsymbol{Z}_0,\mathbb{U})$ for all time t in $[t_j, t_{j+1}]$, initializing $z_0 = \boldsymbol{Z}_0$ at time t_0.

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 the solution $z(t)$ for all t in $[t_j, t_{j+1}]$. A tighter enclosure valid for t in $[t_j, t_{j+1}]$ is then computed using a Taylor-Lagrange expansion of order k of the solution at t_j, where $\boldsymbol{r}_{j+1}$ is used to enclose the remainder:

$$\begin{aligned} z(t;z_j,t_j,u) = z_j + \sum_{i=1}^{k-1}(t-t_j)^i \boldsymbol{f}^{[i]}(z_j,\boldsymbol{u}(t_j)) \\ + (t-t_j)^k \boldsymbol{f}^{[k]}(\boldsymbol{r}_{j+1},\boldsymbol{u}([t_j,t_{j+1}])), \end{aligned} \tag{7}$$

where the (set extensions of the) Taylor coefficients

$$\boldsymbol{f}^{[i]} := \frac{\boldsymbol{z}^{(i)}}{i!}$$

are defined inductively, and can be computed by automatic differentiation. In the classical case where u is a constant parameter, the Taylor coefficients are given, starting with $\boldsymbol{f}^{[1]} = \boldsymbol{f}$, by:

$$\boldsymbol{f}^{[i+1]} = \frac{1}{i+1}\frac{\partial \boldsymbol{f}^{[i]}}{\partial z}.\boldsymbol{f}$$

If we consider the more general case where u is a function of time, sufficiently smooth on each time interval $[t_j, t_{j+1}]$, and with bounded time derivatives $u^{(i)}$, then $\boldsymbol{f}^{[i+1]}$ can be computed by:

$$\boldsymbol{f}^{[i+1]} = \frac{1}{i+1}\left(\frac{\partial \boldsymbol{f}^{[i]}}{\partial z}.\boldsymbol{f} + \sum_{l=0}^{i-1}\frac{\partial \boldsymbol{f}^{[i]}}{\partial u^{(l)}}.\boldsymbol{u}^{(\boldsymbol{l}+\boldsymbol{1})}\right)$$

Hence, $f^{[i+1]}$ depends on function u and its time derivatives $u^{(l)}$ up to order $l = i$. Then, for an order k Taylor model, we need bounds on u and its time derivatives up to order k.

Finally, we use enclosure $\boldsymbol{z}_{j+1} = [z](t_{j+1},t_j,\boldsymbol{z}_j)$ as initial solution set at time t_{j+1} to derive the interval Taylor model on the next time step.

This scheme yields an outer-approximation $O^f_{\mathcal{E}}(t;\boldsymbol{Z}_0,\mathbb{U})$ of the maximal reachable set. By Remark 2, this scheme also outer-approximates all robust reachable sets. If evaluated plainly in interval arithmetic, it yields enclosures of increasing width. A classical way to control the loss of accuracy due to the loss of correlation, called wrapping effect, is a method introduced by Lohner, that uses QR-factorization [33]. Alternatively, we choose here to control wrapping using affine arithmetic [7] instead of interval arithmetic, following [19].

3.3.2 Maximal outer-approximation of the sensitivity matrix. We suppose that the initial condition z_0 of the n-dimensional system (1) depends on a p-dimensional vector of parameters β. The constant but uncertain input u, is a vector of dimension m. The Jacobian matrix of the solution $z = (z_1,\ldots,z_n)$ of this system with respect to $\beta = (\beta_1,\ldots,\beta_p)$ and $u = (u_1,\ldots,u_m)$, is a matrix $J = \begin{pmatrix} J^\beta \; J^u \end{pmatrix}$ of dimension $n \times (p+m)$, such that

$$J^\beta_{ij}(t) = \frac{\partial z_i}{\partial \beta_j}(t),\; J^u_{ik}(t) = \frac{\partial z_i}{\partial u_k}(t)$$

for $1 \le i \le n$, $1 \le j \le p$, and $1 \le k \le m$. Differentiating (1), the coefficients of the Jacobian matrix of the flow satisfy:

$$\dot{J}^\beta_{ij}(t) = \sum_{l=1}^{n}\frac{\partial f_i}{\partial z_l}(z,u).J^\beta_{lj}(t) \tag{8}$$

$$\dot{J}^u_{ik}(t) = \sum_{l=1}^{n}\frac{\partial f_i}{\partial z_l}(z,u).J^u_{lj}(t) + \frac{\partial f_i}{\partial u_k}(z,u)(t) \tag{9}$$

with initial condition $J(0) = (\frac{\partial z_0}{\partial \beta}\; 0_{n\times m})$. This defines J as the solution of an initial value problem of the form (1).

We can thus use the method of Section 3.3.1 to compute outer-approximations of its maximal reachable set.

3.3.3 Inner- and outer-approximations.

Proposition 3.9. *Let $\tilde{O}^f_{\mathcal{E}}(t)$ a maximal outer-approximation of the solution of the system, $O^{F^\beta}_{\mathcal{E}}(t)$ a maximal outer-approximation of the components of J corresponding to the partial derivatives with respect to the parameters β involved in the initial condition z_0, where F^β is the second member of (8), $O^{F^u_{\mathcal{A}}}_{\mathcal{E}}(t)$ and $O^{F^u_{\mathcal{E}}}_{\mathcal{E}}(t)$ maximal outer-approximations of the components of J corresponding to the partial derivatives with respect to inputs $u_{\mathcal{A}}$ and $u_{\mathcal{E}}$ respectively, where F^u is the second member of (9). Then for each component z_i of vector z:*

(i) if

$$\begin{aligned} \mathcal{I}^f_{\mathcal{AE}}(t;\boldsymbol{Z}_0,\boldsymbol{U},I_{\mathcal{A}},I_{\mathcal{E}}) = \tilde{O}^f_{\mathcal{E}}(t) + O^{F^\beta}_{\mathcal{E}}(t)(\mathrm{dual}\,\boldsymbol{\beta} - \tilde{\beta}) + \\ O^{F^u_{\mathcal{A}}}_{\mathcal{E}}(t)(\boldsymbol{u}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}}) + O^{F^u_{\mathcal{E}}}_{\mathcal{E}}(t)(\mathrm{dual}\,\boldsymbol{u}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}}) \end{aligned} \tag{10}$$

is an improper interval, then its proper counterpart is an inner-approximation of the set $R^f_{\mathcal{AE}}(t;\boldsymbol{Z}_0,\mathbb{U},I_{\mathcal{A}},I_{\mathcal{E}})$. Otherwise the result *cannot be interpreted as an inner-approximation.*

$$(ii)\quad \textit{if } \mathcal{O}^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \boldsymbol{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \tilde{\mathcal{O}}^f_{\mathcal{E}}(t) + \mathcal{O}^{F^\beta}_{\mathcal{E}}(t)(\boldsymbol{\beta} - \tilde{\beta}) + \mathcal{O}^{F^u_{\mathcal{A}}}_{\mathcal{E}}(t)(\mathrm{dual}\, \boldsymbol{u}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}}) + \mathcal{O}^{F^u_{\mathcal{E}}}_{\mathcal{E}}(t)(\boldsymbol{u}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}}) \quad (11)$$

is a proper interval, then it is an outer-approximation of the set $R^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

A unique outer-approximation of a center solution and the Jacobian matrix can be used to infer different interpretations as inner-approximations or robust inner-approximations:

Lemma 3.10. *The approximations defined by (10) and (11) are such that if* $I^1_{\mathcal{E}} \subseteq I^2_{\mathcal{E}}$, *then*

$$\mathcal{I}^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I^1_{\mathcal{A}}, I^1_{\mathcal{E}}) \subseteq \mathcal{I}^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I^2_{\mathcal{A}}, I^2_{\mathcal{E}})$$

$$\mathcal{O}^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I^1_{\mathcal{A}}, I^1_{\mathcal{E}}) \subseteq \mathcal{O}^f_{\mathcal{A}\mathcal{E}}(t; Z_0, \mathbb{U}, I^2_{\mathcal{A}}, I^2_{\mathcal{E}})$$

In particular, the minimal approximations will always be included in the robust approximations, which will always be included in the maximal approximations.

Remark 4. *We have no guarantee of inclusion between minimal outer-approximations and robust inner-approximations, or between robust outer-approximations and maximal inner-approximations.*

Remark 5. *The computation of the inner-approximations and robust outer-approximations fully relies on the outer-approximations. Thus we can soundly implement most of our approach using classical interval-based methods: outward rounding should be used for the outer approximations of flows and Jacobians. Only the final computation by Kaucher arithmetic of improper intervals should be done with inward rounding. This also means that the potential conservatism in the interval-based computation of the inner-approximations does not propagate as time progresses. On contrary, if the distance between inner and outer-approximations becomes large, indicating a loss of precision, then the approximation could be dynamically refined, using higher order Taylor models or smaller time step.*

3.3.4 *The case of time dependent input.* In this section, input u is now time dependent, a case that, as far as we know, was not handled in previous work on inner-approximation. For simplicity's sake, we consider here only inner-approximations of maximal reachable sets, but this naturally extends to robust reachable sets.

For inner-approximations, we can restrict $\mathbb{U}$ to the space of m piecewise polynomials of degree l on each interval $[t_j, t_{j+1}]$, as considering less controls means inner-approximating the reachability sets. The set of polynomials of degree l defined over $[t_j, t_{j+1}]$ is denoted by $\mathcal{P}^l_j$ and is parameterized by $l+1$ coefficients noted u^i_j, $i = 0, \ldots, l$. Such a $(l+1)$-uple of coefficients describes the following polynomial in $\mathcal{P}^l_j$:

$$p_{(u^i_j)}(t) = \sum_{q=0}^{l} u^q_j \frac{(t - t_j)^q}{q!} \quad (12)$$

for $t \in [t_j, t_{j+1}]$. The i-th time derivative of $p_{(u^i_j)}$ at time t_j is equal to u^i_j. Each of the m components of the control in this space can thus be identified with a sequence (u^i_j), $i = 0, \ldots, l$, $j = 0, \ldots, r$.

We now extend ODE (1) by adding variable z_{n+1}, identified with time, solution of $\dot{z}_{n+1} = 1$, $z_{n+1}(0) = 0$. Replacing each control component by expressions (12), and t with z_{n+1}, we obtain a new ODE system. For simplicity's sake, we now renumber parameters (u^i_j), as (u_j), $j = 1, \ldots, m \times (l+1) \times (r+1)$.

We suppose as in Section 3.3 that the initial condition z_0 of the n-dimensional system (1) depends on a p-dimensional vector of uncertain parameters β, independent of u. The Jacobian matrix of the solution $z = (z_1, \ldots, z_{n+1})$ of this system with respect to $\beta = (\beta_1, \ldots, \beta_p)$ and $u = (u_j)$, is identified with a matrix $J = \begin{pmatrix} J^\beta & J^u \end{pmatrix}$ of dimension $n \times (p + m \times (r+1) \times l)$, such that

$$J^\beta_{ij}(t) = \frac{\partial z_i}{\partial \beta_j}(t),\ J^u_{ik}(t) = \frac{\partial z_i}{\partial u_k}(t)$$

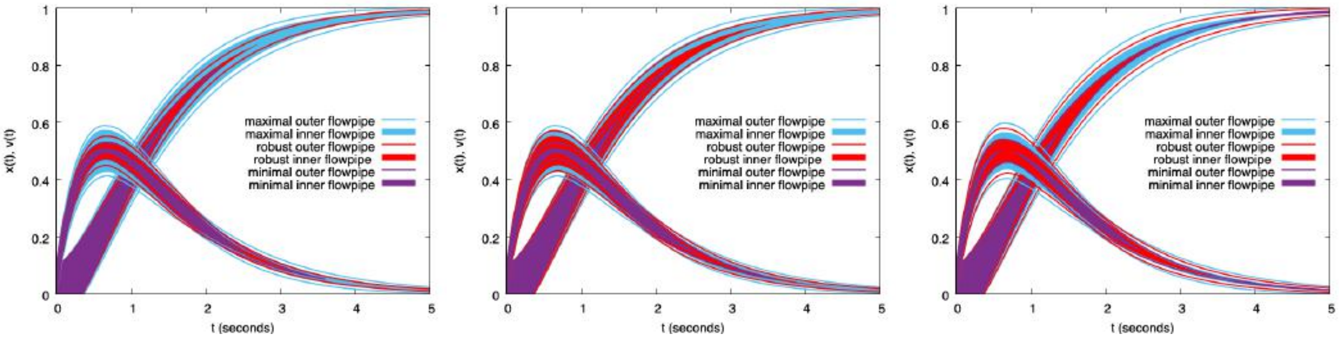
for $1 \le i \le n$, $1 \le j \le p$, and $1 \le k \le m$. Differentiating (1) as in Section 3.3, the coefficients of J also satisfy Equations (8) and (9) with the same initial condition.

Generally, the set of controls $\mathbb{U}$ is defined by bounds on its values and its derivatives up to some degree l. This translates as constraints on the parameters (u_j). We can then derive an inner-approximation of the maximal reachable sets for time-dependent controls.

3.4 Experiments

The approach is implemented in a prototype, available from https://github.com/cosynus-lix/RINO. In this section, we use this prototype to illustrate these different reachable set approximations.

3.4.1 *Illustrating example: the car controller.* Let us illustrate on Example 2.2 these different inner and outer-approximating schemes. On each sub-plot of Figure 1, we represent the maximal outer- and inner-approximations, robust outer- and inner-approximations, and minimal outer- and inner-approximations until time $T = 5$, for different hypotheses on K_p and K_d, although always taken in $[1.95, 2.05] \times [2.95, 3.05]$. Outer-approximations are delimited by plain lines, while inner-approximations are represented as filled region. As noted in Section 3.3, a unique computation of the Taylor models (here obtained in 1 second, with order 3 Taylor models and a time step of 0.02) yields the different AE interpretations of Equations (10) and (11). In Figure 1(a) and (b), K_p and K_d are uncertainly known but constant in time. In Figure 1(a), the robust approximation (in red) is robust with respect to the uncertainty in K_p: it contains only states that are guaranteed to be reached, whatever the values of K_p in $[1.95, 2.05]$, for some initialization of x and v in $[-0.1, 0.1] \times [0, 0.1]$, and some K_d in $[2.95, 3.05]$. In Figure 1(b), the robust approximations are robust with respect to the uncertainty in K_p. We note that the robust approximations in Figure 1(b) are wider than that in Figure 1(a), which can be interpreted as the system being less sensitive to uncertainty in K_p than uncertainty in K_d. Minimal and maximal (outer and inner) approximations are naturally identical in Figure 1(a) and (b). The minimal approximations are robust to both K_p and K_d in both cases, while the maximal approximations are robust to neither K_p and K_d. As expected, the minimal approximations are included in the robust approximations, which in turn are included in the maximal approximations. In Figure 1(c), K_p and K_d are now time-dependent, while still being bounded in $[1.95, 2.05] \times [2.95, 3.05]$. Their first-order time derivatives are bounded in $[-2, 2]$ and higher order derivatives



(a) constant K_d, K_p, robustness to K_p **(b) constant K_d, K_p, robustness to K_d** **(c) time-dependent K_d, K_p, robustness to K_d**

Figure 1: Velocity $v(t)$ and position $x(t)$ of the car in Example 2.2

equal to 0. We consider, as in Figure 1(b), robustness to disturbance in K_d. As more input signals u are possible than in the constant case, the outer-approximation is larger than in Figure 1(b). For inner-approximations, we restrict K_p to be piecewise constant, that is constant on each time step. The robust inner-approximation is robust to piecewise linear signals K_d, with magnitude and slopes as described above. They will become a good approximation of the continuous input signals only when the time step tends towards zero, otherwise we can get a poor quality of inner-approximation. On this simple experiment, it is clear that the innner-approximations and outer-approximations are not so close from one another than in the case of constant parameters, indicating a loss of imprecision. We intend to further investigate the handling of variable input signal in the future. We observe here an illustration of Remark 4: for example, the robust outer-approximations is not included in the maximal inner-approximations.

3.4.2 Benchmark example: a quadrotor controller. We now exemplify the scalability of our approach by computing the maximal inner and outer reachable sets on the dynamics of the full non linear model of a quadrotor (the Crazyflie 2.0), with its attitude controller [12, 28]. We are interested here in a takeoff maneuver, and thus study the dynamic on the vertical axis and the pitch rate, roll rate and yaw rate control, with the following state variables:

- the *vertical position in the world frame* z,
- the *linear velocity of the center of gravity (CoG) in the body-fixed frame with respect to the inertial frame* $[u \quad v \quad w]^T$,
- the *angular orientation is represented by the Euler angles*: $[\phi \quad \theta \quad \psi]$ where ϕ is the roll angle, θ is the pitch angle and ψ is the yaw angle,
- the *angular velocity with respect to the body frame*: $[p \quad q \quad r]^T$ with p the *roll rate*, q the *pitch rate* and r the *yaw rate*.

Given setpoints z_{sp}, p_{sp}, q_{sp} and r_{sp}, the quadrotor is controlled using a set of PI controllers given by Equation (13).

$$\begin{cases} thrust & = 1000 * (25(2(z_{sp} - z) - w) \\ & +15 \int (2(z_{sp} - z) - w)dt) + 36000 \\ cmd_\phi & = 250(p_{sp} - p) + 500 \int (p_{sp} - p)dt \\ cmd_\theta & = 250(q_{sp} - q) + 500 \int (q_{sp} - q)dt \\ cmd_\psi & = 120(r_{sp} - r) + 16.7 \int (r_{sp} - r)dt \end{cases} \tag{13}$$

These values are used to deduce the PWM values to apply to each motors. A linear relation links the PWM to rotation rates. Finally, we deduce the input force F and moments M_x, M_y, M_z:

$$\begin{aligned} M_x &= 4C_T C_1 d(C_1 thrust + C_2)cmd_\phi - (4C_1^2 C_T d)cmd_\theta cmd_\psi \\ M_y &= (-4C_1^2 C_T d)cmd_\phi cmd_\psi + 4C_T C_1 d(C_1 thrust + C_2)cmd_\theta \\ M_z &= (-2C_1^2 Cd)cmd_\phi cmd_\theta + 8C_D C_1(C_1 thrust + C_2)cmd_\psi \\ F &= C_T C_1^2 cmd_\theta^2 + C_T C_1^2 cmd_\phi^2 + 4C_T C_1^2 cmd_\psi^2 \\ & +(4C_T C_1^2)thrust^2 + (8C_T C_1 C_2)thrust + 4C_T C_2^2 \end{aligned}$$

Finally, the system has been augmented with new states x_{11}, x_{12}, x_{13} and x_{14} representing the integral terms in (13). We obtain the final 14-dimensional non-linear dynamical system below:

$$\begin{aligned} \dot{z} &= -sin(\theta)u + cos(\theta)sin(\phi)v + cos(\theta)cos(\phi)w \\ \dot{u} &= rv - qw + sin(\theta)g \\ \dot{v} &= -ru + pw - cos(\theta)sin(\phi)g \\ \dot{w} &= qu - pv - cos(\theta)cos(\phi)g + \frac{F}{m} \\ \dot{\phi} &= p + cos(\phi)tan(\theta)r + tan(\theta)sin(\phi)q \\ \dot{\theta} &= cos(\phi)q - sin(\phi)r \\ \dot{\psi} &= \frac{cos(\phi)}{cos(\theta)}r + \frac{sin(\phi)}{cos(\theta)}q \\ \dot{p} &= \frac{I_y - I_z}{I_x}qr + \frac{1}{I_x}M_x \\ \dot{q} &= \frac{I_z - I_x}{I_y}pr + \frac{1}{I_y}M_y \\ \dot{r} &= \frac{I_x - I_y}{I_z}pq + \frac{1}{I_z}M_z \\ \dot{x_{11}} &= 2(z_{sp} - z) - w \\ \dot{x_{12}} &= p_{sp} - p \\ \dot{x_{13}} &= q_{sp} - q \\ \dot{x_{14}} &= r_{sp} - r \end{aligned}$$

The physical and constant parameters for the crazyflie are obtained by merging data from [12, 28], and summed up in Table (1).

I_x	$1.657171e - 5$	C_T	$1.285e - 8$
I_y	$1.6655602e - 5$	C_D	$7.645e - 11$
I_z	$2.9261652e - 5$	C_1	0.04076521
m	0.028	C_2	380.8359
g	9.81	d	$\frac{0.046}{\sqrt{2}}$

Table 1: Parameters for the model

Specifications of the experiments. We are defining a setpoint as above, so that the quadrotor should move from altitude 0 to 1 meter and so that its roll rate would go from 0 to 1 degree per second, within 5 seconds. In our equations, this corresponds to : $p_{sp} = 1.0$, $q_{sp} = 0$, $r_{sp} = 0$, $z_{sp} = 1.0$.

The initial altitude and rotation speeds of the quadrotor are considered uncertain and are as follows : $z = [-0.2, 0.2]$, $p = [-0.5, 0.5]$, $q = [-0.5, 0.5]$ and all other values are initialized to 0.

Using our prototype with a variable step size between 0.001 and 0.036 and Taylor models of order 5, the computation time to complete the outer-approximation of the reachable set over a time interval of 5 seconds was 6.3 seconds on a standard laptop PC with an i5-7300HQ 2.5GHz processor and 8 Gb RAM, running under Linux Ubuntu 16.04. This compares favorably with other methods for such high-dimensional non-linear models [8], especially with respect to the Eulerian methods of [3] which need a linearization of the dynamics, and clever decomposition methods to deal with 6-dimensional sub-models. The computation time for both inner and outer-approximations is 996 seconds.

The inner and outer approximations obtained for a selection among the components are represented Figure 2.

4 REACHABILITY AND VERIFICATION

4.1 Safety analysis

Following [31], we specify a safety problem by a tuple (φ^f, Z_0, L), where φ^f is the dynamics, Z_0 is the set of initial states, and L is the set of unsafe states.

We will say that φ^f is safe over time horizon $[0, t]$ for all possible inputs if for all $z_0 \in Z_0$, for all $u \in \mathbb{U}$, trajectories $\varphi^f([0, t]; z_0, u)$ do not intersect L. Similarly, we are interested in φ^f being safe over time horizon $[0, t]$ for some input $u \in \mathbb{U}$, or for some inputs $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ depending on other arbitrary inputs $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$.

Forward inner and outer-approximations provide semi-decision procedures for safety over a finite time horizon:

Proposition 4.1. *Any inner-approximation $\mathcal{I}_s$ (resp. outer-approximation O_s) for $s \in [0, t]$ or any flowpipe inner-approximation $\mathcal{I}$ (resp. outer-approximation O) of the robust (resp. maximal) reachable set allows to prove the following:*

- *If $O_s \cap L = \emptyset$ for all $s \in [0, t]$ (resp. $O \cap L = \emptyset$) then φ^f is safe over horizon $[0, t]$ for all possible inputs $u \in \mathbb{U}$*
- *If $\mathcal{I}_s \cap L \neq \emptyset$ for some $s \in [0, t]$ (resp. $\mathcal{I} \cap L \neq \emptyset$) then φ^f is unsafe over horizon $[0, t]$, for some possible inputs $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ (possibly depending on disturbances $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$)*

The proof relies on Proposition 3 of [31].

Example 4.2. The example of Section 3.4.1 gives an application to Proposition 4.1 : take L to be $x \geq 1$. The maximal outer flowpipe does not intersect L, which proves safety whatever the parameters values. Now, take L to be $x \geq 0.95$ and $t \leq 4$, it intersects the inner-approximation of the maximal reachable set, proving it is unsafe, i.e. there exist some parameters values such that the car gets as close as 0.05 to its objective in less than 4 seconds. This is true also robustly, with respect to K_d (Figure 1 (a)): whatever K_d, there exist an initial condition and a value of K_p such that the unsafe region is reached. But this is not true robustly with respect to K_p (Figure 1 (b)): the robust inner-approximation does not intersect $x \geq 0.95$: we cannot prove that whatever K_p, there exist an initial condition and a value of K_d such that the unsafe region is reached. Finally, the minimal outer flowpipe does not intersect $x \geq 0.95$, which proves that there exist values of K_d and K_p for which the system is safe, whatever the initial condition.

Example 4.3. Consider the quadrotor example of Section 3.4.2. We can for example prove using Proposition 4.1 and the outer-approximation represented on Figure 2(a) that the roll rate p will not go above 1.4 degree per second over the first 5 seconds of operation, whatever initial roll rate, altitude, and state.

4.2 Forward reach-avoid and sweep-avoid

A useful generalization of safety properties is the so-called reach-avoid properties. In general, they are defined as backward properties, see e.g. [11]: given a target set K and a set L to be avoided, we are looking for the set of initial states such that there exists a control going from these initial states to K, while avoiding L.

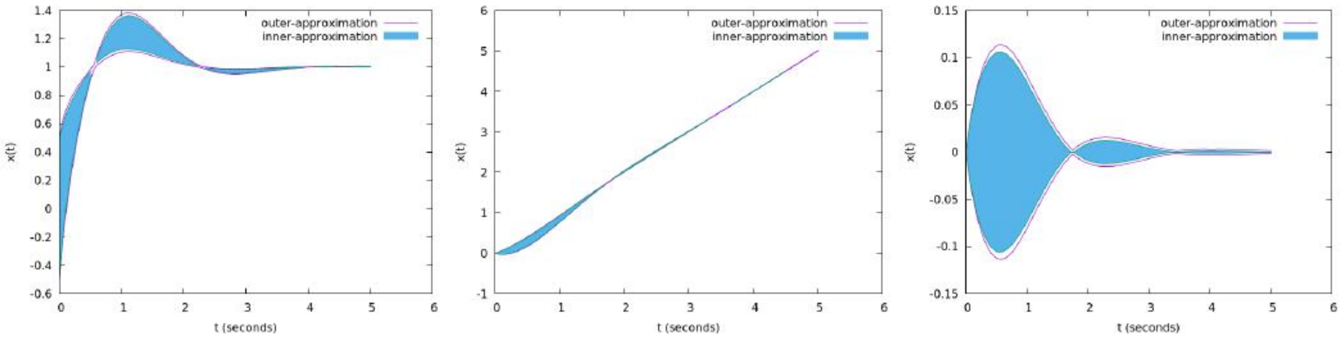
Still, a forward analogue, the *forward robust reach-avoid set*, is useful for checking that from a given set of initial states, for a given set of controls, even in the presence of disturbances, trajectories given by φ^f reach a target set while avoiding another one:

$$\begin{aligned} FRA^f_{\mathcal{AE}}(K, L, [0, t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \{z \in K \mid \forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \\ \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists z_0 \in Z_0 (\exists s \in [0, t],\ z = \varphi^f(s; z_0, u) \\ \wedge (\forall s' \in [0, t], \nexists z' \in L,\ z' = \varphi^f(s'; z_0, u()))\} \quad (14) \end{aligned}$$

Note that the definition given here is slightly stronger than that in [11], as we require here that the unsafe states are avoided until time t instead of until the time s where the target is reached. This formulation simplifies in particular the verification conditions, but could be adapted to match the original definition. Note also that some previous work [29, 35] has also been considering robust reach avoid properties, but generally the quantifiers on controls $u_{\mathcal{A}}$ and $u_{\mathcal{E}}$ are reversed with respect to our definition. This can be desirable for example when disturbances are not observable.

In the case we can reach K while avoiding L, $FRA^f_{\mathcal{AE}}(K, L, [0, t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ is the subset of K that is effectively reached in K while avoiding L. In case it is non empty, we have proved the existence of solutions to the *reach-avoid* problem for (K, L). In case it is equal to K, we say that we have solved the *sweep-avoid* problem for (K, L). We mean that we can cover all of K while avoiding L. This is naturally useful in path-planning problems.

Classically, the existence of solutions to the reach-avoid problem is proved if we can find an outer-approximation O at some time instant fully included in the target set, and if the intersection of the outer-approximation tube with the unsafe set L is empty. However, this is a strong condition, which we can weaken using the computation of an inner-approximating tube: indeed, if we can find a (robust) inner-approximation $\mathcal{I}$ with non empty intersection with the target set K, then the existence of solutions to the (robust) reach-avoid problem is proved. If moreover, $K \subseteq \mathcal{I}$, then we proved that the whole target set K is covered, we solved the (robust) sweep-avoid problem.



(a) Roll rate p **(b) Roll ϕ** **(c) Pitch θ**

Figure 2: Inner and outer approximations for the quadrotor model.

Example 4.4. A cannon shoots bullets, that should be able to reach targets T_1 and T_2, and should avoid a vertical wall, described by the avoid set L, before which the canon is hiding. The ballistics of the bullets is given by the trajectory (x, y), the velocity v and the angle γ of the velocity with respect to the x axis. We use a simple approximation of an Euler model without wind [21], in which there is a drag effect due to the air, and we use a small angles approximation:

$$\dot{v} = -g\gamma - \frac{\rho v^2}{2m} a C_d \qquad \dot{x} = v(1-\gamma^2/2)$$
$$\dot{\gamma} = -\frac{g(1-\gamma^2/2)}{v} \qquad \dot{y} = v\gamma$$

The gravity g is taken to be 9.81 m/s^2, $\rho = 1204.4$ is the air density, $a = 0.000126677$ is the cross section of the bullet, $C_d = 0.45$ is the drag coefficient. The mass m of the bullet is uncertain bounded in [11,15], and considered as a disturbance. Initial velocity $v(0)$ is taken to be in [181,185], and initial angle $\gamma(0)$ is in [2.5,3.5]. The initial coordinates are $x(0) \in [0, 0.01]$ and $y(0) \in [0, 0.01]$.

We plot in Figure 3, the computed reachable sets, for $y(t)$, the unsafe region L and target regions T_1 and T_2 described hereafter.

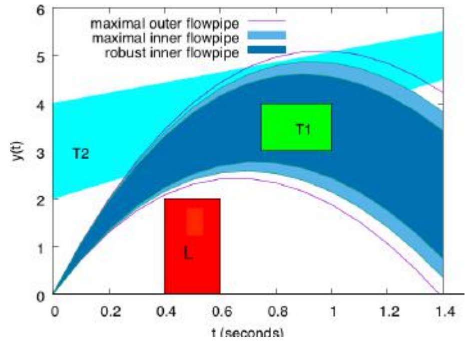


Figure 3: Height $y(t)$ in Example4.4

The unsafe region L is a wall, defined by $y(t) \leq 2,\ \forall t \in [0.4, 0.6]$. Safety is proved here, as the intersection between L and the outer-approximated flowpipe is empty.

The target region T_1 is defined by $3 \leq y(t) \leq 4,\ \forall t \in [0.75, 1]$. We want to prove that every state of this region is reachable for some admissible initial condition of the system, or said differently that the whole region is covered or swept, and this whatever the mass of the bullet. This property is proved here by the fact that region T_1 is fully included in the robust inner-approximated flowpipe.

The target region T_2 is a moving target, defined by some lower and upper surfaces $l(t)$ and $u(t)$, by $l(t) \leq y(t) \leq u(t)$. We want to prove that some point of this target is reachable, whatever the mass of the bullet. This property is proved by the fact that the intersection between region T_2 and the robust inner-approximation is non-empty. Also, we can localize time instants at which the region is sure to be reached: the intersection of the robust flowpipe with the moving target is non-empty only for $0.3 \leq t \leq 1.2$ (the outer-approximation would also give an over-approximation $0.3 \leq t \leq 1.35$ of time instants at which the region can possibly be reached).

Note that our abstraction being parameterized by the time of the system, we could consider some temporal properties, such as bounds on the minimal or maximal time between crossing over an obstacle L and reaching a target T_1.

Example 4.5. Let us now come back to the quadrotor example. Using the combination of inner and outer-approximations in Figure 2, we can prove that there exist some input states such that the quadrotor will reach a roll angle of 5 degrees in less than 5 seconds, while not getting above 0.15 degrees of pitch angle, showing the good behavior of the attitude controller.

4.3 Backward reachable sets

Backward reachability is known [31] to allow for proving a larger set of properties. Backward minimal and maximal reachable sets [24] can be generalized to robust reachable sets, as in the forward case. We will define here only the backward reachable *tubes* (also called victory domain , [4] or capture basin [2]):

$$B^f_{\mathcal{AE}}(K, [0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \{z_0 \in Z_0 \mid \forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}},$$
$$\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists s \in [0,t], \exists z \in K,\ z = \varphi^f(s; z_0, u)\}$$

We note that

$$B^f_{\mathcal{AE}}(K, [0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = R^{-f}_{\mathcal{AE}}([0,t]; K, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \cap Z_0 \quad (15)$$

Therefore, we can also inner and outer-approximate the backward reachable sets. This allows for supplementing the semi-decision procedures for e.g. safety analyses sketched in Section 4.1:

Proposition 4.6. *Let L be a set of unsafe states, $\mathcal{I}_{\mathcal{A}\mathcal{E}}$ an inner-approximation of the robust reachable set $R^{-f}_{\mathcal{A}\mathcal{E}}([0,t]; L, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, and $O_{\mathcal{E}}$ a maximal outer-approximation, we have:*

- *If $O_{\mathcal{E}} \cap Z_0 = \emptyset$ then $\forall u \in \mathbb{U}$, φ^f is safe over time $[0,t]$*
- *If $\mathcal{I}_{\mathcal{A}\mathcal{E}} \cap Z_0 \neq \emptyset$ then $\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ which makes φ^f unsafe*

4.4 Backward reach-avoid properties

Some authors [29] study stronger backward robust properties than considered up to now in this work, such as the following backward reach-avoid set:

$$\begin{aligned} &BRA^f_{\mathcal{E}\mathcal{A}}(K, L, [0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) \\ &\quad = \{z_0 \in Z_0 \mid \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, (\exists s \in [0,t], \exists z \in K, \\ &\qquad\quad z = \varphi^f(t; z_0, u) \wedge \forall s' \in [0,t], \nexists z \in L,\ z = \varphi^f(t; z_0, u)\} \end{aligned}$$

This definition uses a different alternation of quantifiers (exists, for all) from the one (for all, exists) our framework of Section 3 can deal with - note the notation $BRA^f_{\mathcal{E}\mathcal{A}}$ reflecting this point. In $BRA^f_{\mathcal{E}A}$, controls do not depend on perturbations, which make it a stronger property. We can still compute approximations of this set by noting that it can be decomposed as

$$\bigcup_{u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}} \left(B^f_{\mathcal{A}\mathcal{E}}(K, [0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, \emptyset) \cap B^f_{\mathcal{A}\mathcal{E}}(L, [0,t]; Z_0, \mathbb{U}, \emptyset, I_{\mathcal{A}})^c \right)$$

where $(.)^c$ denotes the set complement.

We can thus find inner-approximations (respectively outer-approximations) of BRA^f_{EA} by inner-approximating (respectively outer-approximating) $B^f_{AE}(K, [0,t]; Z_0, \mathbb{U}, I_{\mathcal{A}}, \emptyset)$ and outer-approximating (respectively inner-approximating) $B^f_{AE}(\ L, [0,t]; Z_0, \mathbb{U}, \emptyset, I_{\mathcal{A}})$. As we need to take a union on all $u_{\mathcal{E}}$, this method is only convenient when instantiating $u_{\mathcal{E}}$ on a finite set.

5 CONCLUSION AND FUTURE WORK

We discussed the use of inner and outer approximated reachable sets for property verification, and demonstrated it on simple examples. The Taylor-based flowpipes that we compute for the matrix of sensitivity of trajectories with respect to initial conditions and parameters or inputs, can also be used for backward analysis yielding inputs and parameter synthesis, using a parametric Hansen-Sengupta operator [15]. The inner-approximation we propose here relying purely on outer-approximation, we believe it can also be extended quite naturally to the case of hybrid system. Finally, this work is intended to be a component of future work towards abstract model-checking algorithms for STL-like properties, and actual control synthesis in the line of e.g. TuLiP [10, 36].

REFERENCES

[1] M. Althoff. 2013. Reachability Analysis of Nonlinear Systems Using Conservative Polynomialization and Non-convex Sets. In *HSCC*. ACM publishers, 173–182.

[2] J.-P. Aubin. 2001. Viability Kernels and Capture Basins of Sets Under Differential Inclusions. *SIAM Journal on Control and Optimization* (2001).

[3] S. Bansal, M. Chen, S. L. Herbert, and C. J. Tomlin. 2017. Hamilton-Jacobi reachability: A brief overview and recent advances. In *CDC*.

[4] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre. 1999. *Set-Valued Numerical Analysis for Optimal Control and Differential Games.* Birkhäuser.

[5] X. Chen, E. Ábrahám, and S. Sankaranarayanan. 2012. Taylor Model Flowpipe Construction for Non-linear Hybrid Systems. In *RTSS*.

[6] X. Chen, S. Sankaranarayanan, and E. Abraham. 2014. Under-approximate Flowpipes for Non-linear Continuous Systems. In *FMCAD*.

[7] J. Comba and J. Stolfi. 1993. Affine arithmetic and its applications to computer graphics. *In SIBGRAPI* (1993).

[8] A. E. C. Da Cunha. 2015. Benchmark: Quadrotor Attitude Control. In *ARCH'14-15*, Vol. 34. EasyChair, 57–72.

[9] T. Dang, O. Maler, and R. Testylier. 2010. Accurate hybridization of nonlinear systems. In *HSCC*.

[10] I. Filippidis, S. Dathathri, S. C. Livingston, N. Ozay, and R. M. Murray. 2016. Control design for hybrid systems with TuLiP: The Temporal Logic Planning toolbox. In *CCA*. IEEE, 1030–1041.

[11] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry. 2015. Reach-avoid problems with time-varying dynamics, targets and constraints. In *HSCC*.

[12] J. Förster. 2015. System Identification of the Crazyflie 2.0 Nano Quadrocopter. Bachelor Thesis.

[13] A. Girard. 2005. Reachability of uncertain linear systems using zonotopes. In *HSCC'05*. Springer.

[14] A. Girard, C. Le Guernic, and O. Maler. 2006. Efficient Computation of Reachable Sets of Linear Time-Invariant Systems with Inputs. In *HSCC*.

[15] A. Goldsztejn. 2006. A Branch and Prune Algorithm for the Approximation of Non-linear AE-solution Sets. In *ACM SAC*.

[16] Alexandre Goldsztejn. 2012. Modal Intervals Revisited, Part 1: A Generalized Interval Natural Extension. *Reliable Computing* 16 (2012), 130–183.

[17] Alexandre Goldsztejn. 2012. Modal Intervals Revisited, Part 2: A Generalized Interval Mean Value Extension. *Reliable Computing* 16 (2012), 184–209.

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

[19] E. Goubault and S. Putot. 2017. Forward Inner-Approximated Reachability of Non-Linear Continuous Systems. In *HSCC*. ACM.

[20] E. Goubault, S. Putot, and L. Sahlman. 2018. Inner and Outer Approximating Flowpipes for Delay Differential Equations. In *CAV*.

[21] R. Scitovski J. Cumin, B. Grizelj. 2009. Numerical Solving of Ballistic Flight Equations for Big Bore Air Rifle. *Technical Gazette* 16 (2009).

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

[23] S. Kaynama, J. Maidens, M. Oishi, I. M. Mitchell, and G. A. Dumont. 2012. Computing the Viability Kernel Using Maximal Reachable Sets. In *HSCC*. ACM.

[24] S. Kaynama, M. Oishi, I. M. Mitchell, and G. A. Dumont. 2011. The continual reachability set and its computation using maximal reachability techniques. In *IEEE CDC*.

[25] M. Korda, D. Henrion, and C. N. Jones. 2013. Inner Approximations of the Region of Attraction for Polynomial Dynamical Systems. In *NOLCOS*.

[26] A. B Kurzhanski and P. Varaiya. 2000. Ellipsoidal techniques for reachability analysis: internal approximation. *Systems & control letters* (2000).

[27] D. Liberzon. 2003. *Switching in Systems and Control.* Birkhauser.

[28] C. Luis and J. Le Ny. 2016. Design of a Trajectory Tracking Controller for a Nanoquadcopter. https://arxiv.org/abs/1608.05786v1.

[29] K. Margellos and J. Lygeros. 2011. Hamilton-Jacobi Formulation for Reach-Avoid Differential Games. *IEEE Trans. Automat. Contr.* 56, 8 (2011), 1849–1861.

[30] T. Le Mézo, L. Jaulin, and B. Zerr. 2017. Bracketing the solutions of an ordinary differential equation with uncertain initial conditions. *Appl. Math. Comput.* (2017).

[31] I. M. Mitchell. 2007. Comparing Forward and Backward Reachability as Tools for Safety Analysis. In *HSCC*.

[32] Ramon E. Moore. 1966. *Interval analysis.*

[33] N. S. Nedialkov, K. Jackson, and G. Corliss. 1999. Validated Solutions of Initial Value Problems for Ordinary Differential Equations. *Appl. Math. Comp.* (1999).

[34] M. Amin Ben Sassi, R. Testylier, T. Dang, and A. Girard. 2012. Reachability Analysis of Polynomial Systems Using Linear Programming Relaxations. In *ATVA*.

[35] C. J. Tomlin, J. Lygeros, and S. Shankar Sastry. 2000. A game theoretic approach to controller design for hybrid systems. *Proc. IEEE* 88, 7 (2000), 949–970.

[36] T. Wongpiromsarn, U. Topcu, N. Ozay, H. Xu, and R. M. Murray. 2011. TuLiP: a software toolbox for receding horizon temporal logic planning.. In *HSCC*. ACM.

[37] B. Xue, M. Fränzle, and N. Zhan. 2018. Under-Approximating Reach Sets for Polynomial Continuous Systems. In *Proceedings of HSCC '18*. ACM, 51–60.

[38] B. Xue, P. Nazier Mosaad, M. Fränzle, M. Chen, Y. Li, and N. Zhan. 2017. Safe Over- and Under-Approximation of Reachable Sets for Delay Differential Equations. In *FORMATS (LNCS)*, Vol. 10419. Springer, 281–299.

[39] Bai Xue, Zhikun She, and Arvind Easwaran. 2016. Under-Approximating Backward Reachable Sets by Polytopes. In *CAV*.

[40] Z. Zhou, J. Ding, H. Huang, R. Takei, and C. Tomlin. 2018. Efficient path planning algorithms in reach-avoid problems. *Automatica* 89 (2018).

A PROOFS

Proof of Theorem 3.3. The proof can be found in [17]. □

Proof of Lemma 3.5. Let a set $\mathcal{I}_{\mathcal{AE}}$ such that $\forall z \in \mathcal{I}_{\mathcal{AE}}$, $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists z_0 \in Z_0, \varphi^f(t; z_0, u) = z$. Then any such $z \in \mathcal{I}_{\mathcal{AE}}$ obviously belongs to $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$. In other words, whatever the disturbances $u_{\mathcal{A}}$, any point of $\mathcal{I}_{\mathcal{AE}}$ is proved to be the solution at time t of system (1), for some value of $z_0 \in Z_0$ and some control $u_{\mathcal{E}}$. Thus $\mathcal{I}_{\mathcal{AE}}$ is an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

Now, we prove that the set of robust inner-approximations of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ admits a supremum. For every set of inner-approximations $(\mathcal{I}_i)$ of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, their union $\mathcal{I} = \bigcup_i \mathcal{I}_i$ is an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$: for all $z \in \mathcal{I}$, there is an index i with $z \in \mathcal{I}_i$. As $\mathcal{I}_i$ is an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, we thus know that $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists z_0 \in Z_0, \varphi^f(t; z_0, u) = z$. Overall, the supremum $\mathcal{I}$ is thus an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

We then show that $\mathcal{I}$ is equal to $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$. Take $z \in R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ and consider the supremum $\mathcal{I}$ of all sets inner-approximating $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$. We prove that $\mathcal{I} \cup \{z\}$ is an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ as well: for all $\tilde{z} \in \mathcal{I} \cup \{z\}$, either $\tilde{z} = z$ and as $z \in R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, we have that $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}, \exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}, \exists z_0 \in Z_0, z = \varphi^f(t; z_0, u)$, or $\tilde{z} \in \mathcal{I}$ and we have the same property. Overall this means that $\mathcal{I} \cup \{z\}$ is an inner-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$. But as $\mathcal{I}$ is the supremum of all such sets and $\mathcal{I} \subseteq \mathcal{I} \cup \{z\}$, $\mathcal{I} \cup \{z\} = \mathcal{I}$ and $z \in \mathcal{I}$. □

Proof of Lemma 3.6. Let $z \in R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, we first prove that z is in a set $O_{\mathcal{AE}}$ defined by the hypotheses of Lemma 3.6. As $z \in R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$, then by definition, $\forall u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, $\exists z_0 \in Z_0$, $\exists u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ such that $z = \varphi^f(t; z_0, u)$. Then, for these $z_0 \in Z_0$ and $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$, we know there exists $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, such that $z = \varphi^f(t; z_0, u)$. Thus z is in a set $O_{\mathcal{AE}}$ defined by the hypotheses of Lemma 3.6, but z is not in all such sets (depending on the choice of $u_{\mathcal{A}}$), so that $O_{\mathcal{AE}}$ does not in general define an outer-approximation of $R^f_{\mathcal{AE}}(t; Z_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

In the case when $I_{\mathcal{A}} = \emptyset$, then $z \in R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$ is such that $\exists z_0 \in Z_0, \exists u \in \mathbb{U}$ such that $z = \varphi^f(t; z_0, u)$. Then, for these $z_0 \in Z_0$ and $u \in \mathbb{U}$, we have $z = \varphi^f(t; z_0, u)$, thus $z \in O_{\mathcal{E}}$.

Let us now note that the intersection of outer-approximations of $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$ is an outer-approximation of $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$. Consider $O = \bigcap_i O_i$ where all O_i are outer-approximations of $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$. For all i, O_i being an outer-approximation means that for all $u \in \mathbb{U}, \forall z_0 \in Z_0, \exists z_i \in O_i, \varphi^f(t; z_0, u) = z_i$. Therefore, for such u and z_0, $z_i = \varphi^f(t; z_0, u) = z_j$, for all i and j. Therefore all z_i are equal and in all the O_i, i.e. are in O. Thus O is the infimum of all outer-approximations (for a given Z_0, and $\mathbb{U}$) and is an outer-approximation of $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$.

Suppose O is not equal to $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$, therefore, O contains $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$ strictly. Let $z \in O$ which is not in $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$. We prove that $O \backslash \{z\}$ is an outer-approximation. For all $u \in \mathbb{U}$, for all $z_0 \in Z_0$, we wish to find $\tilde{z} \in O \backslash \{z\}$ such that $\tilde{z} = \varphi^f(t; z_0, u)$; for now we have a $\tilde{z} \in O$ with $\tilde{z} = \varphi^f(t; z_0, u)$, we have to prove that $\tilde{z}$ cannot be equal to z. As $z \notin R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$, for all $u \in \mathbb{U}$, for all $z_0 \in Z_0$, $z \neq \varphi^f(t; z_0, u)$. Because of this we are sure that $\tilde{z} \neq z$. Therefore $O \backslash \{z\}$ is an outer-approximation, and as O is the infimum of such sets, $z \notin O$. Therefore O is equal to $R^f_{\mathcal{E}}(t; Z_0, \mathbb{U})$. □

Proof of Proposition 3.7. Let $\tilde{f}_{\mathcal{A}E}(a, e) = \boldsymbol{c} + \Delta_{\mathcal{A}} a + \Delta_{\mathcal{E}} e$ be an affine interval-valued function from $\mathbb{R}^n$ to $\mathbb{IR}$ ($\boldsymbol{c} \in \mathbb{IR}^n$, $\Delta_{\mathcal{A}} \in \mathbb{IR}^p$, $a \in \mathbb{R}^p$, $\Delta_{\mathcal{E}} \in \mathbb{IR}^q$, $e \in \mathbb{R}^q$, , $p + q = n$) and let $f_{\mathcal{A}E}$ be any affine real-valued function in $\tilde{f}_{\mathcal{A}E}$, i.e.

$$f_{\mathcal{A}E}(a, e) = c + \delta_{\mathcal{A}} a + \delta_{\mathcal{E}} e$$

for some $c \in \boldsymbol{c}$, $\delta_{\mathcal{A}} \in \Delta_{\mathcal{A}}$ and $\delta_{\mathcal{E}} \in \Delta_{\mathcal{E}}$. Write $\boldsymbol{c} = [c^-, c^+]$, and components $(\Delta_{\mathcal{A}})_i = [(\delta^-_{\mathcal{A}})_i, (\delta^+_{\mathcal{A}})_i]$ $(i = 1, \ldots, p)$, $(\Delta_{\mathcal{E}})_j = [(\delta^-_{\mathcal{E}})_j, (\delta^+_{\mathcal{E}})_j]$ $(j = 1, \ldots, q)$, and components of a : a_i for $i = 1, \ldots, p$, and of e : e_j for $j = 1, \ldots, q$.

Components $(\Delta_{\mathcal{A}})_i$ and $(\Delta_{\mathcal{E}})_j$ can be of three types : either entirely positive, containing 0, or entirely negative. We divide the indices of components $\Delta_{\mathcal{A}}$ as I the set of indices such that for all i in I, $(\delta^-_{\mathcal{A}})_i > 0$, J the set of indices such that for all j in J, $0 \in (\Delta_{\mathcal{A}})_j$, and the set of indices K such that for all k in K, $(\delta^+_{\mathcal{A}})_k < 0$.

Consider now z such that $\forall a \in [-1, 1]^p, \exists e \in [-1, 1]^q, z = f_{\mathcal{A}E}(a, e)$. Choose a to have as components, $a_i = 1$ (for $i \in I$), $a_j = 0$ (for $j \in J$) and $a_k = -1$ (for $k \in K$). Then necessarily $z \geq c_- + \sum_{i \in I} (\delta^-_{\mathcal{A}})_i - \sum_{k \in K} (\delta^+_{\mathcal{A}})_k - \sum_l \inf((\delta^-_{\mathcal{E}})_l, (\delta^+_{\mathcal{E}})_l)$. Similarly, choose a to have as components, $a_i = -1$ (for $i \in I$), $a_j = 0$ (for $j \in J$) and $a_k = 1$ (for $k \in K$). Then necessarily, $z \leq c_+ - \sum_{i \in I} (\delta^-_{\mathcal{A}})_i + \sum_{k \in K} (\delta^+_{\mathcal{A}})_k + \sum_l \sup((\delta^-_{\mathcal{E}})_l, (\delta^+_{\mathcal{E}})_l)$. We recognize the Kaucher arithmetic interpretation of $\tilde{f}_{\mathcal{A}E}([1, -1]^p, [-1, 1]^q)$ (see e.g. [18, 22]).

Now, consider a general function $f : \mathbb{R}^m \to \mathbb{R}$, differentiable and $\boldsymbol{x} \in \mathbb{R}^m$, which we can decompose in $\boldsymbol{x}_{\mathcal{A}} \in \mathbb{R}^p$ and $\boldsymbol{x}_{\mathcal{E}} \in \mathbb{R}^q$ with $p + q = m$. Let, for each $i \in \{1, \ldots, m\}$, $\boldsymbol{\Delta}_i \in \mathbb{IR}$ such that $\left\{ \frac{\partial f}{\partial x_i}(x),\ x \in \boldsymbol{x} \right\} \subseteq \boldsymbol{\Delta}_i$. And construct for any $\tilde{x} \in \boldsymbol{x}$,

$$\tilde{f}_{\mathcal{A}E}(a, e) = f(\tilde{x}) + \boldsymbol{\Delta}_{\mathcal{A}} a + \boldsymbol{\Delta}_{\mathcal{E}} e$$

By the mean-value theorem, for all $x_{\mathcal{A}}$ and $x_{\mathcal{E}}$ there exists some $f_{\mathcal{A}E}$ in $\tilde{f}_{\mathcal{A}E}$ such that $f_{\mathcal{A}E}(x_{\mathcal{A}} - \tilde{x}_{\mathcal{A}}, x_{\mathcal{E}} - \tilde{x}_{\mathcal{E}})$ is equal to $f(x_{\mathcal{A}}, x_{\mathcal{E}})$ (i.e. equal to z). Up to translation and rescaling, we can suppose that $x_{\mathcal{A}} - \tilde{x}_{\mathcal{A}} \in [-1, 1]$ and $x_{\mathcal{E}} - \tilde{x}_{\mathcal{E}} \in [-1, 1]$. Consider the set $R = \{z \mid \forall x_{\mathcal{A}} \in \boldsymbol{x}_{\mathcal{A}}, \exists x_{\mathcal{E}} \in \boldsymbol{x}_{\mathcal{E}}, z = f(x)\}$. For z an element of R, and for all $x_{\mathcal{A}}$ and a choice of $x_{\mathcal{E}}$ witnessing the fact that z belongs to R, we have a function $f_{\mathcal{A}E}$ as shown above, such that $f_{\mathcal{A}E}(x_{\mathcal{A}} - \tilde{x}_{\mathcal{A}}, x_{\mathcal{E}} - \tilde{x}_{\mathcal{E}})$ is equal to $f(x_{\mathcal{A}}, x_{\mathcal{E}})$. By what we proved above, $z \in \tilde{f}_{\mathcal{A}E}([1, -1]^p, [-1, 1]^q)$, i.e. $z \in O^f_{\mathcal{AE}}(\boldsymbol{x}, \tilde{x})$. Hence $O^f_{\mathcal{AE}}(\boldsymbol{x}, \tilde{x})$ is an outer-approximation of R. □

Proof of Proposition 3.9. Let $\tilde{O}_{\mathcal{E}}^{f}(t)$ a maximal outer-approximation of the solution of the system, $O_{\mathcal{E}}^{F^{\beta}}(t)$ a maximal outer-approximation of the components of J corresponding to the partial derivatives with respect to the parameters β involved in the initial condition z_0, where F^{β} is the second member of (8), $O_{\mathcal{E}}^{F^{u}_{\mathcal{A}}}(t)$ and $O_{\mathcal{E}}^{F^{u}_{\mathcal{E}}}(t)$ maximal outer-approximations of the components of J corresponding to the partial derivatives with respect to inputs $u_{\mathcal{A}}$ and $u_{\mathcal{E}}$ respectively, where F^{u} is the second member of (9). Suppose now that for each component z_i of vector z:

$$\begin{aligned}\mathcal{I}_{\mathcal{A}\mathcal{E}}^{f}(t; \boldsymbol{Z}_0, \boldsymbol{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \tilde{O}_{\mathcal{E}}^{f}(t) + O_{\mathcal{E}}^{F^{\beta}}(t)(\text{dual}\,\boldsymbol{\beta} - \tilde{\beta}) + \\ O_{\mathcal{E}}^{F^{u}_{\mathcal{A}}}(t)(\boldsymbol{u}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}}) + O_{\mathcal{E}}^{F^{u}_{\mathcal{E}}}(t)(\text{dual}\,\boldsymbol{u}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}})\end{aligned}$$

is an improper interval. Then by Theorem 3.3, as $O_{\mathcal{E}}^{F^{\beta}}(t)$, $O_{\mathcal{E}}^{F^{\beta}}(t)$ and $O_{\mathcal{E}}^{F^{u}_{\mathcal{E}}}(t)$ are outer-approximations of the Jacobian of the solutions of our differential system, with respect to z_0, $u_{\mathcal{A}}$ and $u_{\mathcal{E}}$, and as $\tilde{O}_{\mathcal{E}}^{f}(t)$ is an outer-approximation of a "central" solution of our system, $\mathcal{I}_{\mathcal{A}\mathcal{E}}^{f}(t; \boldsymbol{Z}_0, \boldsymbol{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$ yields an inner-approximation of the set $R_{\mathcal{A}\mathcal{E}}^{f}(t; \boldsymbol{Z}_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$.

Now, suppose

$$\begin{aligned}O_{\mathcal{A}\mathcal{E}}^{f}(t; \boldsymbol{Z}_0, \boldsymbol{U}, I_{\mathcal{A}}, I_{\mathcal{E}}) = \tilde{O}_{\mathcal{E}}^{f}(t) + O_{\mathcal{E}}^{F^{\beta}}(t)(\boldsymbol{\beta} - \tilde{\beta}) + \\ O_{\mathcal{E}}^{F^{u}_{\mathcal{A}}}(t)(\text{dual}\,\boldsymbol{u}_{\mathcal{A}} - \tilde{u}_{\mathcal{A}}) + O_{\mathcal{E}}^{F^{u}_{\mathcal{E}}}(t)(\boldsymbol{u}_{\mathcal{E}} - \tilde{u}_{\mathcal{E}})\end{aligned}$$

is a proper interval. Then by Proposition 3.7, as $O_{\mathcal{E}}^{F^{\beta}}(t)$, $O_{\mathcal{E}}^{F^{\beta}}(t)$ and $O_{\mathcal{E}}^{F^{u}_{\mathcal{E}}}(t)$ are outer-approximations of the Jacobian of the solutions of our differential system, with respect to z_0, $u_{\mathcal{A}}$ and $u_{\mathcal{E}}$, and as $\tilde{O}_{\mathcal{E}}^{f}(t)$ is an outer-approximation of a "central" solution of our system again, $O_{\mathcal{A}\mathcal{E}}^{f}$ is an outer-approximation of the set $R_{\mathcal{A}\mathcal{E}}^{f}(t; \boldsymbol{Z}_0, \mathbb{U}, I_{\mathcal{A}}, I_{\mathcal{E}})$. □

Proof of Proposition 4.1. The proof relies on Proposition 3 of [31], which states that the following properties are equivalent:

- φ^{f} is safe over horizon $[0, t]$ for all inputs $u \in \mathbb{U}$
- $R_{\mathcal{E}}^{f}(s; \boldsymbol{Z}_0, \mathbb{U}) \cap L = \emptyset$ for all $s \in [0, t]$
- $R_{\mathcal{E}}^{f}([0, t]; \boldsymbol{Z}_0, \mathbb{U}) \cap L = \emptyset$

Suppose that O_s is an outer-approximation of $R_{\mathcal{E}}^{f}(s; \boldsymbol{Z}_0, \mathbb{U})$ for all $s \in [0, t]$. By Lemma 3.6, we have, for all $s \in [0, t]$, $R_{\mathcal{E}}^{f}(s; \boldsymbol{Z}_0, \mathbb{U}) \subseteq O_s$. Therefore if $O_s \cap L = \emptyset$, for all $s \in [0, t]$, we have $R_{\mathcal{E}}^{f}(s; \boldsymbol{Z}_0, \mathbb{U}) \cap L \subseteq O_s \cap L = \emptyset$ for all $s \in [0, t]$ hence φ^{f} is safe over horizon $[0, t]$ for all inputs by the above equivalent properties. For inner-approximations, they are a direct translation of the definition. □

Proof of Proposition 4.6. The proof of the first statement is akin to the proof of Proposition 4 of [31]. Suppose $O \cap \boldsymbol{Z}_0 = \emptyset$, then for all $z_0 \in \boldsymbol{Z}_0$, z_0 is in the complement of O, and by Lemma 3.6 z_0 is also in the complement of the maximal reachable set for $-f$, which is the maximal backward reachable set for f by Equation (15). Negating its definition, we get $\forall u \in \mathbb{U}$, $\forall s \in [0, t]$, $\varphi^{f}(s; z_0, u) \notin L$. Conversely, suppose that $O \cap \boldsymbol{Z}_0 \neq \emptyset$. Take $z_0 \in \boldsymbol{Z}_0$, then for a control u and this initial state z_0, there exists $s \in [0, t]$ and $z \in L$ such that $\varphi^{f}(s; z_0, u) = z$, contradicting the fact that φ^{f} is safe. For the second statement, $\mathcal{I}_{\mathcal{A}\mathcal{E}} \cap \boldsymbol{Z}_0 \neq \emptyset$ exactly means that there is some initial state z_0 such that for all disturbances $u_{\mathcal{A}} \in \mathbb{U}_{\mathcal{A}}$, there exists $u_{\mathcal{E}} \in \mathbb{U}_{\mathcal{E}}$ (thus possibly depending on z_0 and $u_{\mathcal{A}}$) which makes φ^{f} unsafe over time horizon $[0, t]$. □

Acknowledgments. The authors were supported by DGA project "Validation of Autonomous Drones and Swarms of Drones" and the academic chair "Complex Systems Engineering" of Ecole Polytechnique-ENSTA-Télécom-Thalès-Dassault-Naval Group-DGA-FX-FDO-Fondation ParisTech.