Scalable Computation of Robust Control Invariant Sets of Nonlinear Systems

Lukas Schäfer, Felix Gruber, and Matthias Althoff

***Abstract*— Ensuring robust constraint satisfaction for an infinite time horizon is a challenging, yet crucial task when deploying safety-critical systems. We address this issue by synthesizing robust control invariant sets for perturbed nonlinear sampled-data systems. This task can be encoded as a nonconvex program for which we propose a tailored, computationally efficient successive convexification algorithm. Based on the zonotopic representation of invariant sets, we obtain an updated candidate for the invariant set and the safety-preserving controller by solving a single convex program. To obtain a possibly large region of safe operation, our algorithm is designed so that the sequence of candidate invariant sets has monotonically increasing volume. We demonstrate the efficacy and scalability of our approach by applying it to a broad range of nonlinear control systems from the literature with up to 20 dimensions.**

***Index Terms*— Invariant sets, nonlinear control systems, scalability, robust control, cyber-physical systems, safety.**

I. Introduction

AUTONOMOUS systems, such as vehicles, robots, and drones, have recently attracted a lot of interest both in academia and industry. However, when deploying such systems in safety-critical applications, it is crucial to guarantee safety for an infinite time horizon. This task can be accomplished by computing robust control invariant (RCI) sets: once the system state has entered an RCI set, the associated safety-preserving controller takes over to keep the state inside this RCI set and, thereby, satisfaction of state and input constraints at any future point in time is guaranteed. Among the many applications in robust control synthesis, RCI sets are commonly used as terminal constraints in robust model predictive control to ensure recursive feasibility and stability [1]–[3]. Similarly, RCI sets can be employed as terminal constraints in online safety-verification frameworks [4]. They have also been applied as part of supervisory safety filters for learning-based control [5], [6]. These filters monitor whether a desired input compromises safety and, if so, overrides this desired input using a safety-preserving controller.

Even though the computation of RCI sets has been an active research area for decades [7], most work has been devoted to linear systems [8]–[10]. Since we compute RCI sets for nonlinear system, we focus on this system class in our subsequent literature survey. Besides RCI sets, we also review work on corresponding safety-preserving controllers.

Manuscript received Month Date, Year; revised Month Date, Year. This work was supported by the European Commission Project justIT-SELF under Grant 817629.

The authors are with the Department of Informatics, Technical University of Munich, D-85748 Garching, Germany (e-mail: lukas.schaefer@tum.de, felix.gruber@tum.de, althoff@tum.de)

A. Related Work

The evolution of uncertain discrete-time nonlinear systems can be enclosed by a convex set, which leads to the framework of convex difference inclusion systems [11], [12]. Examples include polytopic linear difference inclusion [13] or difference-of-convex systems [11], [14], which have been used to compute polytopic (robust control) invariant sets in [11], [12], [15]. Computing polytopic (robust control) invariant sets in this framework boils down to solving linear programs for each vertex and, if applicable, a vertex-associated safety-preserving control input. Since even the number of vertices of a box grows exponentially with the dimension of the state space, the applicability of these approaches is restricted to low-dimensional systems.

Another line of research for the computation of polytopic (robust control) invariant sets focuses on systems with polynomial dynamics [16]–[18] and is based on convex relaxations for polynomial optimization problems over cones [19], [20]. The basic idea is to synthesize a controller that renders every half-space representing the polytope invariant, which can be encoded as a polynomial optimization problem. Due to the specific structure, lifting the problem to a higher-dimensional space admits a linear programming relaxation. To depend less on a suitable choice of the normal vectors, the approach is extended to optimize over the normal vectors and the offsets of the half-spaces in [18]. However, it is unclear how the lifting step can be automated and the scalability of the approach to higher-dimensional systems has not yet been demonstrated.

In contrast to the previously considered polytopic sets, ellipsodial sets scale better to higher-dimensional systems at the cost of more conservative results. In [21], [22], nonlinear systems are approximated by linear difference inclusions whose reachable sets are represented using polytopes in vertex representation and a robust control invariant ellipsoid is obtained by solving a set of linear matrix inequalities. However, the representation of the difference inclusion compromises the scalability of the approach. A control invariant ellipsoid and an associated safety-preserving linear feedback for the linearized system are computed in [23]. Control invariance for the original discrete-time nonlinear system is verified by solving a sequence of non-convex programs. To reduce the conservatism, higher-order approximations for both the

feedback and the sub-level set inducing a control invariant ellipsoid are used in [24]. By restricting the class of considered systems to polynomial dynamics, the problem of computing a control invariant set can be formulated as a sum-of-squares program. For a fixed degree of the polynomials, a sum-of-squares program can be converted into a semi-definite program. However, the authors only consider nominal systems in [23], [24]. Ellipsoidal sets have also been applied to compute invariant tubes in robust model predictive control [25], [26].

Yet another possibility for computing invariant sets are methods using Hamilton-Jacobi equations, which have also been applied to reachability analysis [27] and for finding robust regions of attraction [28]. However, solving the associated partial differential equations scales exponentially with respect to the number of state variables [27]. More recently, convex programming relaxations have been proposed for the computation of the region of attraction and robust invariant sets for perturbed polynomial systems subject to state constraints [29]–[31]. The basic idea is to relax the Hamilton-Jacobi equations into systems of inequalities that admit the formulation of a semi-definite program. However, a candidate safety-preserving controller has to be designed a-priori.

In contrast to the Hamilton-Jacobi framework, relying on the notion of occupation measures yields an infinite-dimensional linear program when synthesizing (control) invariant sets of discrete-time and continuous-time polynomial systems. This optimization problem admits a finite-dimensional relaxation that translates into a semi-definite program [32]. In [32], [33] over-approximations of the maximal control invariant set and the region of attraction are computed. Under-approximations of the maximal positive invariant set are considered in [34], where an extension to bounded disturbances is introduced. This line of research yields promising results including invariant sets for six-dimensional under-actuated systems [32]. However, the complexity of this approach is exponential in the degree of the approximating polynomial [32] and none of these approaches considers perturbed and controlled nonlinear systems.

Another line of research for safety-preserving controller synthesis of nonlinear systems are control barrier functions (CBF), which attracted a lot of interest recently [35]–[41]. Research has mostly focused on control-affine systems [35]–[37] or uncertain control-affine systems [38]–[41]. There exist several approaches to obtain the CBF, whose sub-level set represents an invariant set [35]: the CBF has to a) be guessed based on the application, which makes it difficult to guarantee feasibility of the online control problem, b) synthesized from trajectories, which can be computationally expensive, or c) computed by conversion into a set of sum-of-squares constraints, which suffers from poor scalability [42].

B. Contribution and Outline

In this paper, we propose a novel approach for the computation of RCI sets of perturbed nonlinear sampled-data systems. Compared to existing approaches, our algorithm scales favorably with the dimension of the state space. In particular, we

- use zonotopes as an efficient set representation of RCI sets of nonlinear systems;
- propose a parameterized representation of reachable sets that enables to jointly synthesize an RCI set and a corresponding safety-preserving set-based controller in a single convex program; and
- derive a successive convexification algorithm, where the sequence of convex programming solutions is recursively feasible and the sequence of candidate RCI sets has monotonically increasing volume.

The remainder of this work is structured as follows: In Sec. II, we introduce zonotopes and polytopes as efficient set representations and conditions for zonotope containment. In addition, we provide our problem statement. Subsequently, we present our solution concept in Sec. III. In Sec. IV, we review and modify the reachability analysis algorithm in [43] as an essential building block of our approach for computing RCI sets. The convex program for synthesizing an RCI set and a corresponding safety-preserving controller is proposed in Sec. V. This section also covers the analysis of the sequence of convex programming solutions and the properties of our algorithm including its computational complexity. In Sec. VI, we demonstrate the efficacy of our approach using a multitude of examples from the literature. Finally, conclusions are drawn in Sec. VII.

II. Preliminaries

In this section, we first introduce our notation. Afterwards, we introduce zonotopes and polytopes as efficient set representations and recall two encodings of zonotope containment problems. This section closes with a statement of our control problem.

A. Notation

The set of real, nonnegative real, and positive real numbers is denoted by $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{R}_{>0}$, respectively; the set of natural numbers with and without zero is denoted by $\mathbb{N}_0$ and $\mathbb{N}$, respectively. We use $e_j,\ j \in \{1,\dots,n\}$, to denote the standard unit vectors of the Cartesian coordinate system in $\mathbb{R}^n$. The set $\{r, r+1, \dots, q\} \subset \mathbb{N}_0,\ 0 \leq r \leq q$, is denoted by $\mathbb{N}_{[r:q]}$. The vector full of ones and zeros of appropriate dimension is denoted by $\mathbf{1}$ and $\mathbf{0}$, respectively. Given a real matrix A, $\det(A)$ refers to the determinant of A. We use $A_{(\cdot,j)}$ to denote the $j-$th column of A and $A_{(\cdot,\mathcal{J})}$, where $\mathcal{J} \subset \mathbb{N}$, to denote the corresponding submatrix of A. The absolute value $|A|$ as well as equalities and inequalities between vectors and matrices are applied elementwise. For $a \in \mathbb{R}^n$, the operator $\operatorname{diag}(a)$ returns a diagonal matrix with the elements of a on the main diagonal. Given two sets $\mathcal{A}, \mathcal{B} \subset \mathbb{R}^n$, $\mathcal{A} \oplus \mathcal{B} = \{a+b : a \in \mathcal{A}, b \in \mathcal{B}\}$ denotes their Minkowski addition, $\mathcal{A} \times \mathcal{B} = \{\left[a^T, b^T\right]^T : a \in \mathcal{A}, b \in \mathcal{B}\}$ denotes their Cartesian product, and $\textsc{conv}(\mathcal{A}, \mathcal{B})$ denotes their convex hull. The linear map of $\mathcal{A}$ with a matrix $M \in \mathbb{R}^{m \times n}$ is defined as $M\mathcal{A} = \{Ma : a \in \mathcal{A}\}$ and the operator $\textsc{volume}(\mathcal{A})$ returns the volume of $\mathcal{A}$. Given an interval $\mathcal{C} = \{c : \underline{c} \leq c \leq \overline{c}\} \subset \mathbb{R}$, the operators $\textsc{center}(\mathcal{C}) = \underline{c}+\overline{c}/2$ and $\textsc{radius}(\mathcal{C}) = \overline{c}-\underline{c}/2$ return the center and radius of $\mathcal{C}$, respectively. In case of an interval matrix $\mathcal{M} \subset \mathbb{R}^{m \times n}$, both operators are applied elementwise.

B. Set Representations

Zonotopes are a popular set representation for reachability analysis and controller synthesis of linear systems [44].

Definition 1 (Zonotope): A zonotope $\mathcal{Z} \subset \mathbb{R}^{n_z}$ in generator representation is defined by

$$\mathcal{Z} = \{z \in \mathbb{R}^{n_z} : z = c + G\lambda, |\lambda| \leq \mathbf{1}\}$$

where $c \in \mathbb{R}^{n_z}$ is the center and $G \in \mathbb{R}^{n_z \times \eta(\mathcal{Z})}$ is the generator matrix with $\eta(\mathcal{Z}) \in \mathbb{N}_0$ denoting the number of generators of $\mathcal{Z}$. We use $\mathcal{Z} = \langle c, G \rangle_{\mathcal{Z}}$ as a more compact notation.

According to [45], the Minkowski addition $\mathcal{Z}_1 \oplus \mathcal{Z}_2$ of two zonotopes $\mathcal{Z}_1 = \langle c_1, G_1 \rangle_{\mathcal{Z}} \subset \mathbb{R}^{n_z}$, $\mathcal{Z}_2 = \langle c_2, G_2 \rangle_{\mathcal{Z}} \subset \mathbb{R}^{n_z}$ and the linear map $M\mathcal{Z}_1$ of a zonotope $\mathcal{Z}_1$ are

$$\mathcal{Z}_1 \oplus \mathcal{Z}_2 = \langle c_1 + c_2, [G_1, G_2] \rangle_{\mathcal{Z}}, \tag{1a}$$

$$M\mathcal{Z}_1 = \langle Mc_1, MG_1 \rangle_{\mathcal{Z}}. \tag{1b}$$

As proposed in [46, Theorem 3.3], we tightly over-approximate the set-based multiplication $\mathcal{M}\mathcal{Z}_1$, where $\mathcal{M}$ is an interval matrix, by

$$\mathcal{M} \otimes \mathcal{Z}_1 = \left\langle Cc_1, \left[CG_1, \operatorname{diag}\left(R \left| [c_1, G_1] \right| \mathbf{1}\right)\right] \right\rangle_{\mathcal{Z}}, \tag{2}$$

where $C = \text{CENTER}(\mathcal{M})$ and $R = \text{RADIUS}(\mathcal{M})$. The operator $\text{BOX}(\mathcal{Z}_1) = \langle c_1, \operatorname{diag}(|G_1|\mathbf{1}) \rangle_{\mathcal{Z}}$ returns the smallest axis-aligned box enclosure of $\mathcal{Z}_1$ [47]. Given a vector $a \in \mathbb{R}^n_{\geq 0}$, we use the same operator to compute $\text{BOX}(a) = \langle \mathbf{0}, \operatorname{diag}(a) \rangle_{\mathcal{Z}}$.

As a second set representation, we introduce polytopes.

Definition 2 (Polytope): We refer to a bounded set $\mathcal{P} \subset \mathbb{R}^{n_z}$ as a polytope, if it is defined by

$$\mathcal{P} = \{z \in \mathbb{R}^{n_z} : Hz \leq h\},$$

where $H \in \mathbb{R}^{m \times n_z}$ and $h \in \mathbb{R}^m$. We use $\mathcal{P} = \langle H, h \rangle_{\mathcal{P}}$ as a more compact notation.

C. Zonotope Containment

Since the synthesis of an RCI set is usually formulated using set containment problems [8], [9], [48], we recall two approaches to verify the containment of a zonotope in a polytope and in another zonotope. Given a zonotope $\mathcal{Z}_1 = \langle c_1, G_1 \rangle_{\mathcal{Z}} \subseteq \mathbb{R}^{n_z}$ and a polytope $\mathcal{P} = \langle H, h \rangle_{\mathcal{P}} \subseteq \mathbb{R}^{n_z}$, $\mathcal{P}$ contains $\mathcal{Z}_1$, i.e., $\mathcal{Z}_1 \subseteq \mathcal{P}$, if and only if [49]

$$Hc_1 + |HG_1|\,\mathbf{1} \leq h. \tag{3}$$

Consider the zonotope $\mathcal{Z}_2 = \langle c_2, G_2 \operatorname{diag}(\alpha) \rangle_{\mathcal{Z}} \subseteq \mathbb{R}^{n_z}$ where $\alpha \in \mathbb{R}^{\eta(\mathcal{Z}_2)}_{>0}$. To check whether $\mathcal{Z}_1 \subseteq \mathcal{Z}_2$ using (3), the circumbody $\mathcal{Z}_2$ has to be converted into half-space representation [50]. However, the number of half-spaces can grow exponentially with respect to $\eta(\mathcal{Z}_2)$ [51]. Using a slight modification of the approach from [52, Lemma 2], $\mathcal{Z}_1 \subseteq \mathcal{Z}_2$ if there exist $\Gamma \in \mathbb{R}^{\eta(\mathcal{Z}_2) \times \eta(\mathcal{Z}_1)}$, $\gamma \in \mathbb{R}^{\eta(\mathcal{Z}_2)}$ such that

$$G_1 = G_2\Gamma, \tag{4a}$$

$$c_2 - c_1 = G_2\gamma, \tag{4b}$$

$$|[\Gamma, \gamma]|\,\mathbf{1} \leq \alpha. \tag{4c}$$

Note that in contrast to (3), the conditions in (4) only constitute a sufficient criterion for $\mathcal{Z}_1 \subseteq \mathcal{Z}_2$; it is shown in [51] that the zonotope containment problem is co-NP-complete.

D. Problem Statement

We consider perturbed continuous-time nonlinear systems that evolve according to

$$\dot{x}(t) = f(x(t), u(t), w(t)), \tag{5}$$

where $x(t) \in \mathbb{R}^{n_x}$ denotes the state of the system, $u(t) \in \mathbb{R}^{n_u}$ denotes the control input, and $w(t) \in \mathbb{R}^{n_w}$ denotes the unknown disturbance at time $t \in \mathbb{R}_{\geq 0}$. The function f is assumed to be twice continuously differentiable and the input as well as disturbance trajectories $u(\cdot)$ and $w(\cdot)$, respectively, are assumed to be piecewise continuous. We make no assumption about the statistical nature of the disturbance, only that the set of admissible disturbances $\mathcal{W}$ contains the origin and is given in generator representation. We use $w(\cdot) \in \mathcal{W}$ as a more compact notation for $w(t) \in \mathcal{W}$ at all times. The same shorthand is used for state and input trajectories throughout this paper. Given an initial state $x(0) = x_0$, an input trajectory $u(\cdot)$, and a disturbance trajectory $w(\cdot)$, the solution of (5) at time $t \in \mathbb{R}_{\geq 0}$ is denoted by $\chi(x_0, u(\cdot), w(\cdot), t)$.

In controller synthesis for cyber-physical systems, one usually encounters the setting of sampled-data systems: a physical plant that evolves in continuous time is controlled by a digital controller [5]. The sensors sample at discrete points in time $t_k = k\Delta t$ with $\Delta t \in \mathbb{R}_{>0}$, $k \in \mathbb{N}_0$ and the actuators provide a piecewise constant control input

$$u(t) = u_{\text{ctrl}}(x(t_k)), \quad \forall t \in [t_k, t_{k+1}[, \tag{6}$$

where u_{ctrl} denotes a given sampled-data control law. Next, we define the reachable set of the perturbed nonlinear system in (5) under the sampled-data control law u_{ctrl}.

Definition 3 (One-step Reachable Set): For the system in (5), a set of initial states $\mathcal{X}_0 \subset \mathbb{R}^{n_x}$, a sampled-data controller u_{ctrl}, and a set of disturbances $\mathcal{W}$, the reachable set $\mathcal{R}_e(\Delta t, \mathcal{X}_0, u_{\text{ctrl}})$ after one time step is the set of trajectories starting in $\mathcal{X}_0$ evaluated at time Δt:

$$\begin{aligned}\mathcal{R}_e(\Delta t, \mathcal{X}_0, u_{\text{ctrl}}) = \{&\chi(x(0), u_{\text{ctrl}}(x(0)), w(\cdot), \Delta t) : \\ &\exists x(0) \in \mathcal{X}_0, \exists w(\cdot) \in \mathcal{W}\}.\end{aligned} \tag{7}$$

The reachable set over the time interval $[0, \Delta t]$ is defined as the union of reachable sets $\mathcal{R}_e(t, \mathcal{X}_0, u_{\text{ctrl}})$, $\forall t \in [0, \Delta t]$, i.e.,

$$\mathcal{R}_e([0, \Delta t], \mathcal{X}_0, u_{\text{ctrl}}) = \bigcup_{t \in [0, \Delta t]} \mathcal{R}_e(t, \mathcal{X}_0, u_{\text{ctrl}}). \tag{8}$$

Since the computation of the exact reachable sets in (7) and (8) is not possible for general nonlinear systems [53], we compute over-approximations to ensure safety [54], i.e., $\mathcal{R}_o(t, \mathcal{X}_0, u_{\text{ctrl}}) \supseteq \mathcal{R}_e(t, \mathcal{X}_0, u_{\text{ctrl}})$, $\forall t \in [0, \Delta t]$.

The state and the control input are constrained by

$$x(\cdot) \in \mathcal{X} = \langle H_{\mathcal{X}}, h_{\mathcal{X}} \rangle_{\mathcal{P}}, \tag{9a}$$

$$u(\cdot) \in \mathcal{U} = \langle H_{\mathcal{U}}, h_{\mathcal{U}} \rangle_{\mathcal{P}}. \tag{9b}$$

In this paper, the control goal is to find an RCI set with maximum volume around a steady state (x_{eq}, u_{eq}) so that we

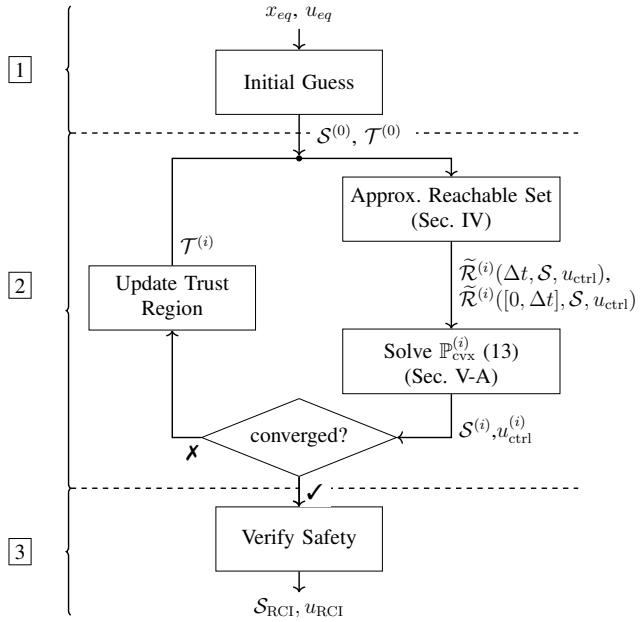


Fig. 1: Overview of our successive convexification approach for the computation of RCI sets of nonlinear sampled-data systems.

ensure satisfaction of the constraints in (9) despite unknown disturbances for a possibly large region of operation.

III. Solution Concept

We obtain a possibly large RCI set by solving the following non-convex program

$$\mathbb{P}_{\text{RCI}}:$$

$$\left(\hat{\mathcal{S}}_{\text{RCI}}, \hat{u}_{\text{RCI}}\right) = \underset{\mathcal{S}, u_{\text{ctrl}}}{\text{argmax}} \quad \text{VOLUME}\left(\mathcal{S}\right) \tag{10a}$$

$$\text{such that}$$

$$\mathcal{R}_o(\Delta t, \mathcal{S}, u_{\text{ctrl}}) \subseteq \mathcal{S}, \tag{10b}$$

$$\mathcal{R}_o([0, \Delta t], \mathcal{S}, u_{\text{ctrl}}) \subseteq \mathcal{X}, \tag{10c}$$

$$\forall x_0 \in \mathcal{S}, u_{\text{ctrl}}\left(x_0\right) \in \mathcal{U}, \tag{10d}$$

where the constraints are based on the definition of RCI sets of sampled-data systems [55]. The condition in (10b) ensures invariance of $\hat{\mathcal{S}}_{\text{RCI}}$; moreover, satisfaction of the state and input constraints in between sampling times is enforced by the constraints in (10c) and (10d), respectively. Thus, robust satisfaction of (9a) and (9b) for every $x(0) \in \hat{\mathcal{S}}_{\text{RCI}}$ follows by induction. Since we consider nonlinear systems, $\mathbb{P}_{\text{RCI}}$ is non-convex in general and, thus, computationally expensive to solve. Moreover, a suitable initial guess is required to prevent convergence to an infeasible stationary point.

Inspired by [56], [57], we propose a successive convexification scheme to derive a computationally efficient approach for the computation of a possibly large RCI set $\mathcal{S}_{\text{RCI}}$ with the corresponding controller u_{RCI}. To achieve scalability, $\mathcal{S}_{\text{RCI}}$ is represented as a zonotope. Our algorithm consists of the following three main steps (see Fig. 1):

1 **Initial Guess:** First, an initial guess $\mathcal{S}^{(0)} = \left\langle x_{eq}, G^{(0)} \right\rangle_{\mathcal{Z}}$ for the RCI set $\mathcal{S}_{\text{RCI}}$ is computed. As we will discuss subsequently, we set $\eta\left(\mathcal{S}_{\text{RCI}}\right) = \eta\left(\mathcal{S}^{(0)}\right)$; thus, $\eta\left(\mathcal{S}^{(0)}\right)$ is a user-defined parameter that allows to balance flexibility with computational effort. For instance, $\mathcal{S}^{(0)}$ can be obtained using the approach for the computation of zonotopic safe sets of linear systems [8].

2 **Successive Convexification:** As already mentioned, we successively solve a convex approximation of the non-convex program $\mathbb{P}_{\text{RCI}}$. To this end, we adopt the generator scaling approach introduced in [58]: given an initial guess $\mathcal{S}^{(0)}$, we keep the orientation of the generators fixed and introduce a vector of scaling factors $s \in \mathbb{R}^{\eta(\mathcal{S}_{\text{RCI}})}_{>0}$ as optimization variables. Thus, the generator matrices of the candidate sets $\mathcal{S}^{(i)} = \left\langle x_{eq}, G^{(i)} \right\rangle_{\mathcal{Z}}$, where the superscript $i \in \mathbb{N}$ refers to the solution of the $i-$th iteration, are defined recursively

$$G^{(i)} = G^{(i-1)}\text{diag}\left(s^{(i)}\right),$$

with the initial step $G^{(1)} = G^{(0)}\text{diag}\left(s^{(1)}\right)$.
We use the zonotope $\mathcal{S}^{(i)}_{\text{ctrl}} = \left\langle u_{eq}, G^{(i)}_{\text{ctrl}} \right\rangle_{\mathcal{Z}}$, where $G^{(i)}_{\text{ctrl}} \in \mathbb{R}^{n_u \times \eta(\mathcal{S}_{\text{RCI}})}$, to represent the candidate safety-preserving controller $u^{(i)}_{\text{ctrl}}$, which is associated with the candidate RCI set $\mathcal{S}^{(i)}$. Given a state $x \in \mathcal{S}^{(i)}$, we obtain a safety-preserving control input as

$$u^{(i)}_{\text{ctrl}}\left(x\right) = u_{eq} + G^{(i)}_{\text{ctrl}}\lambda(x), \quad |\lambda(x)| \leq \mathbf{1}, \tag{11}$$

where $\lambda(x)$ parameterizes x in $\mathcal{S}^{(i)}$, i.e., $x = x_{eq} + G^{(i)}\lambda(x)$.
The key ingredient of our approach are approximations of the exact reachable sets

$$\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}^{(i)}, u^{(i)}_{\text{ctrl}}) \approx \mathcal{R}_e(\Delta t, \mathcal{S}^{(i)}, u^{(i)}_{\text{ctrl}}), \tag{12a}$$

$$\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}^{(i)}, u^{(i)}_{\text{ctrl}}) \approx \mathcal{R}_e([0, \Delta t], \mathcal{S}^{(i)}, u^{(i)}_{\text{ctrl}}), \tag{12b}$$

which admit the computation of the candidate set $\mathcal{S}^{(i)}$ and controller $u^{(i)}_{\text{ctrl}}$ by solving a single convex program (Sec. IV). More precisely, the approximations of the reachable sets in (12) are designed in a way to arrive at a convex encoding of the constraints in (10b) and (10c). Based on (12), we solve the following conic convex programming approximation of $\mathbb{P}_{\text{RCI}}$ (Sec. V-A)

$$\mathbb{P}^{(i)}_{\text{cvx}}:$$

$$\left(s^{(i)}, u^{(i)}_{\text{ctrl}}\right) = \underset{s, u_{\text{ctrl}}}{\text{argmax}} \quad J^{(i)}_{\text{cvx}}\left(\mathcal{S}\right) \tag{13a}$$

$$\text{such that}$$

$$\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}, u_{\text{ctrl}}) \subseteq \mathcal{S}, \tag{13b}$$

$$\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}, u_{\text{ctrl}}) \subseteq \mathcal{X}, \tag{13c}$$

$$\mathcal{S}_{\text{ctrl}} \subseteq \mathcal{U}, \tag{13d}$$

$$\mathcal{S} \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}, \tag{13e}$$

$$\mathcal{S} = \left\langle x_{eq}, G^{(i-1)}\text{diag}\left(s\right) \right\rangle_{\mathcal{Z}}, \tag{13f}$$

where the cost function $J^{(i)}_{\text{cvx}}\left(\mathcal{S}\right)$ denotes a suitable concave approximation of (10a) (see Sec. V-A). Since the control inputs can only be chosen within $\mathcal{S}_{\text{ctrl}}$ due to

(11), the constraint in (13d) automatically ensures the input constraint in (10d). For simplicity, we refer to $\mathcal{S}^{(i)}$ and $u_{\text{ctrl}}^{(i)}$ as the solution of $\mathbb{P}_{\text{cvx}}^{(i)}$.

In addition to the constraints originating from $\mathbb{P}_{\text{RCI}}$, we introduce the trust-region-like constraint in (13e), which confines $\mathcal{S}$ to a neighborhood of $\mathcal{S}^{(i-1)}$, please refer to [59, Ch. 4] for an introduction to trust-region methods. Throughout this paper, we assume that $\mathcal{T}^{(i-1)}$ is chosen as an axis-aligned box that is centered at the origin. This constraint enables the formulation of the approximations in (16) so that $\text{VOLUME}\left(\mathcal{S}^{(i)}\right)$ is monotonically growing (Sec. V-B).

We iteratively solve $\mathbb{P}_{\text{cvx}}^{(i)}$ until the sequence of candidate sets $\mathcal{S}^{(i)}$ and controllers $u_{\text{ctrl}}^{(i)}$ converges, where convergence is measured in terms of the relative increase of the volume of $\mathcal{S}^{(i)}$

$$\frac{\text{VOLUME}\left(\mathcal{S}^{(i)}\right) - \text{VOLUME}\left(\mathcal{S}^{(i-1)}\right)}{\text{VOLUME}\left(\mathcal{S}^{(i-1)}\right)} \leq \epsilon$$

and $\epsilon \in \mathbb{R}_{>0}$ is a user-defined parameter.

3 **Verification of Safety:** Since we have only used approximations of the reachable sets in 2, satisfaction of the constraints in (10b) and (10c) is not guaranteed. To verify safety, we compute over-approximations $\mathcal{R}_o(\Delta t, \mathcal{S}^{(i)}, u_{\text{ctrl}}^{(i)})$ and $\mathcal{R}_o([0, \Delta t], \mathcal{S}^{(i)}, u_{\text{ctrl}}^{(i)})$ of the reachable sets starting from the converged set $\mathcal{S}^{(i)}$ using the adaptive algorithm presented in [60]. If the conditions in (10b) and (10c) are satisfied, our algorithm returns the RCI set $\mathcal{S}_{\text{RCI}} = \mathcal{S}^{(i)}$ and the corresponding safety-preserving controller $u_{\text{RCI}} = u_{\text{ctrl}}^{(i)}$; (10d) is satisfied by construction, as previously explained.

Otherwise, we adopt the approach for over-approximating reachable sets of nonlinear-systems [60] to obtain a feasible solution: we enlarge $\widetilde{\mathcal{R}}^{(i+1)}(\Delta t, \mathcal{S}, u_{\text{ctrl}})$ and $\widetilde{\mathcal{R}}^{(i+1)}([0, \Delta t], \mathcal{S}, u_{\text{ctrl}})$ before solving $\mathbb{P}_{\text{cvx}}^{(i+1)}$ and rechecking for satisfaction of (10b) and (10c). This procedure is repeated until the conditions in (10b) and (10c) are satisfied.

In the next section, we derive the approximations of the reachable sets in (12).

IV. Parameterized Reachability Analysis

In this section, we briefly recall the approach for reachability analysis of nonlinear systems introduced in [43], [60]. Afterwards, we present an approximation of the reachable sets in (12) tailored to our successive convexification approach. These approximations are designed so that our approach avoids the execution of the reachability analysis algorithm while solving the optimization problem $\mathbb{P}_{\text{cvx}}^{(i)}$.

A. Reachability Analysis of Nonlinear Systems

To compute reachable sets, we first abstract the system dynamics in (5) by a first-order Taylor expansion, which yields the following differential inclusion

$$\dot{x}(t) \in f_{\text{lin}}(t) \oplus \mathcal{L}(t), \tag{14}$$

where $f_{\text{lin}}(t)$ is the linearized flow function of the system dynamics and the Lagrange remainder $\mathcal{L}(t)$ captures the linearization error. The abstraction in (14) admits the application of the superposition principle of linear systems. Thus, the computation of the over-approximated reachable sets can be split into two parts [46, Ch. 3.2-3.3], [47]:

$$\begin{aligned}\mathcal{R}_o(\Delta t, \mathcal{X}_0, u_{\text{ctrl}}) =& \mathcal{R}_{\text{lin}}(\Delta t, \mathcal{X}_0, u_{\text{ctrl}}) \\ &\oplus \mathcal{R}_p\left(\mathcal{L}([0, \Delta t])\right),\end{aligned} \tag{15a}$$

$$\begin{aligned}\mathcal{R}_o([0, \Delta t], \mathcal{X}_0, u_{\text{ctrl}}) =& \mathcal{R}_{\text{lin}}([0, \Delta t], \mathcal{X}_0, u_{\text{ctrl}}) \\ &\oplus \mathcal{R}_p\left(\mathcal{L}([0, \Delta t])\right),\end{aligned} \tag{15b}$$

where $\mathcal{R}_{\text{lin}}(\Delta t, \mathcal{X}_0, u_{\text{ctrl}})$ and $\mathcal{R}_{\text{lin}}([0, \Delta t], \mathcal{X}_0, u_{\text{ctrl}})$ are shorthands for the reachable sets of $f_{\text{lin}}(t)$. $\mathcal{R}_p\left(\mathcal{L}([0, \Delta t])\right)$ returns the reachable set due to the set of linearization errors $\mathcal{L}([0, \Delta t])$ as presented in [61].

B. Approximative Parameterized Reachability Analysis

Based on (15), we propose parameterized approximations of the reachable sets to leverage the scalable encoding of zonotope containment problems in (4). The approximations of the time-point and time-interval reachable sets are defined as

$$\begin{aligned}\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}, u_{\text{ctrl}}) =& \widetilde{\mathcal{R}}_{\text{lin}}^{(i)}(\Delta t, \mathcal{S}, u_{\text{ctrl}}) \\ &\oplus \mathcal{R}_p\left(\text{BOX}\left(\Psi^{(i)}(\mathcal{S})\right)\right),\end{aligned} \tag{16a}$$

$$\begin{aligned}\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}, u_{\text{ctrl}}) =& \widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0, \Delta t], \mathcal{S}) \\ &\oplus \mathcal{R}_p\left(\text{BOX}\left(\Psi^{(i)}(\mathcal{S})\right)\right),\end{aligned} \tag{16b}$$

where $\Psi^{(i)}(\mathcal{S}) \in \mathbb{R}_{\geq 0}^{n_x}$ denotes an approximation of the Lagrange remainder whose properties are discussed in Sec. IV-B.3. We compute the sets in (16) so that they are linear in the optimization variables s and u_{ctrl}. Due to the definition of the Minkowski addition of two zonotopes in (1a), the computation of the sets in (16) can be discussed separately: in Sec. IV-B.1 and Sec. IV-B.2, we present the parameterized reachable sets $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}(\Delta t, \mathcal{S}, u_{\text{ctrl}})$ and $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0, \Delta t], \mathcal{S})$ for points in time and time intervals, respectively, of the abstraction $f_{\text{lin}}(t)$. Afterwards, we discuss the approximation $\Psi^{(i)}(\mathcal{S})$ of the Lagrange remainder in Sec. IV-B.3.

1) Parameterized Time-Point Reachable Set: Since we aim to compute an RCI set around the steady state x_{eq}, the expansion point of the differential inclusion (14) is chosen as $(x_{eq}, u_{eq}, \mathbf{0})$. Thus, the linear flow function $f_{\text{lin}}(t)$ simplifies to

$$f_{\text{lin}}(t) = A_{\text{lin}}(x(t) - x_{eq}) + B_{\text{lin}}(u(t) - u_{eq}) + E_{\text{lin}}w(t),$$

where A_{lin}, B_{lin}, and E_{lin} are matrices of appropriate dimensions. By plugging in $\mathcal{S}$ from (13f), u_{ctrl} from (11) and using reachability algorithms for linear systems [47], we obtain

$$\begin{aligned}\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}(\Delta t, \mathcal{S}, u_{\text{ctrl}}) = [A, B]\left\langle \mathbf{0}, \begin{bmatrix} G^{(i-1)}\text{diag}(s) \\ G_{\text{ctrl}} \end{bmatrix} \right\rangle_{\mathcal{Z}} \\ \oplus \mathcal{R}_p\left(E_{\text{lin}}\mathcal{W}\right),\end{aligned} \tag{17}$$

with

$$A = e^{A_{\text{lin}}\Delta t}, \quad B = \int_0^{\Delta t} e^{A_{\text{lin}}\sigma} d\sigma B_{\text{lin}}.$$

2) Parameterized Time-Interval Reachable Set: Next, we compute the time-interval reachable set $\mathcal{R}_{\text{lin}}([0,\Delta t],\mathcal{X}_0,u_{\text{ctrl}})$ in (15b) based on [46] by

$$\begin{aligned}\mathcal{R}_{\text{lin}}([0,\Delta t],\mathcal{S},u_{\text{ctrl}}) = \\ \text{CONV}\left(\mathcal{S},\mathcal{R}_{\text{lin}}(\Delta t,\mathcal{S},u_{\text{ctrl}})\right)\oplus\mathcal{F}\otimes\mathcal{S}_{\text{aug}},\end{aligned} \tag{18}$$

where $\mathcal{F}\subset\mathbb{R}^{n_x\times(n_x+n_u)}$ is an interval matrix and

$$\begin{aligned}\mathcal{S}_{\text{aug}} &= (\mathcal{S}\oplus\{-x_{eq}\})\times(\text{BOX}\,(\mathcal{U})\oplus\{-u_{eq}\}),\\ &= \left\langle\begin{bmatrix}\mathbf{0}\\ c_{\text{BOX}(\mathcal{U})}-u_{eq}\end{bmatrix},\begin{bmatrix}G^{(i-1)}\text{diag}\,(s) & \mathbf{0}\\ \mathbf{0} & G_{\text{BOX}(\mathcal{U})}\end{bmatrix}\right\rangle_{\mathcal{Z}},\\ &= \langle c_{\text{aug}},G_{\text{aug}}\rangle_{\mathcal{Z}}.\end{aligned}$$

The addend $\mathcal{F}\otimes\mathcal{S}_{\text{aug}}$ accounts for the curvature of trajectories between points in time. By exploiting the constraints on the reachable sets in $\mathbb{P}_{\text{cvx}}^{(i)}$, we propose the following simplification of (18), which is linear in the generator scaling factors s.

Proposition 1: If the invariance constraint in (13b) is satisfied, the time-interval reachable set

$$\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0,\Delta t],\mathcal{S}) = \mathcal{S}\oplus\mathcal{F}\otimes\mathcal{S}_{\text{aug}}, \tag{19}$$

in (16b) is equivalent to $\mathcal{R}_{\text{lin}}([0,\Delta t],\mathcal{S},u_{\text{ctrl}})$ in (18). In addition, the center and the generator matrix of the zonotope representing $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0,\Delta t],\mathcal{S})$ are linear in the generator scaling factors s.

Proof: Equivalence of (18) and (19): By combining the invariance constraint in (13b) with (16a), we obtain that $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}(\Delta t,\mathcal{S},u_{\text{ctrl}})\subseteq\mathcal{S}$ since $\text{BOX}\left(\Psi^{(i)}(\mathcal{S})\right)$ is centered at the origin. Thus, $\mathcal{S}=\text{CONV}\left(\mathcal{S},\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}(\Delta t,\mathcal{S},u_{\text{ctrl}})\right)$ so that $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0,\Delta t],\mathcal{S})=\mathcal{R}_{\text{lin}}([0,\Delta t],\mathcal{S},u_{\text{ctrl}})$.

Linearity with respect to s: Since the centers and generator matrices of $\mathcal{S}$ and $\mathcal{S}_{\text{aug}}$ are linear in s, linearity of $\widetilde{\mathcal{R}}_{\text{lin}}^{(i)}([0,\Delta t],\mathcal{S})$ in s follows from positive homogeneity of $|\cdot|$, (2), and (1). ■

3) Parameterized Lagrange Remainder: We apply two steps to arrive at a parameterized formulation of $\mathcal{L}(t)$ that is tailored to a convex approximation of $\mathbb{P}_{\text{RCI}}$: First, we have to circumvent the mutual dependency between the time-interval reachable set $\mathcal{R}_o([0,\Delta t],\mathcal{X}_0,u_{\text{ctrl}})$ and the set of linearization errors $\mathcal{L}([0,\Delta t])$, which is evaluated over $\mathcal{R}_o([0,\Delta t],\mathcal{X}_0,u_{\text{ctrl}})$ [43]. To this end, we use $\mathcal{S}\approx\mathcal{R}_o([0,\Delta t],\mathcal{S},u_{\text{ctrl}})$ to approximate $\mathcal{L}([0,\Delta t])$. Since $\mathcal{S}=\mathcal{R}_o([0,0],\mathcal{S},u_{\text{ctrl}})$, we write $\mathcal{L}(0)\approx\mathcal{L}([0,\Delta t])$. To make the dependency on $\mathcal{S}$ clear, we use $\mathcal{L}(\mathcal{S})$ instead of $\mathcal{L}(0)$ in the remainder of this section.

Second, we introduce the approximation $\Psi_j^{(i)}(\mathcal{S})$ of $\mathcal{L}_j(\mathcal{S})$, which is interchangeable as long as several requirements ensuring convexity and recursive feasibility of $\mathbb{P}_{\text{cvx}}^{(i)}$ are met.

Definition 4: The continuous function $\Psi_j^{(i)}(\mathcal{S})\in\mathbb{R}_{\geq 0}, j\in\mathbb{N}_{[1:n_x]}$, which approximates $\mathcal{L}_j(\mathcal{S})$, is suitable for our successive convexification approach, if it satisfies the following requirements:

- C1) Recursive feasibility: $\Psi_j^{(i+1)}\left(\mathcal{S}^{(i)}\right)\leq\Psi_j^{(i)}\left(\mathcal{S}^{(i)}\right)$ holds for all $i\in\mathbb{N}$;
- C2) Over-approximativeness: $\forall\mathcal{S}$ satisfying (13e), it holds that $\mathcal{L}_j(\mathcal{S})\leq\Psi_j^{(i)}(\mathcal{S})$;
- C3) Convexity: $\Psi_j^{(i)}(\mathcal{S})$ enables a convex formulation of the constraints in (13b) and (13c) when using the encodings in (3) and (4). Moreover, every auxiliary constraint that is required for a given $\Psi_j^{(i)}(\mathcal{S})$ to satisfy the requirements in C1) - C3) is representable using (a product of) linear, second-order, exponential, power, or semidefinite cones [62].

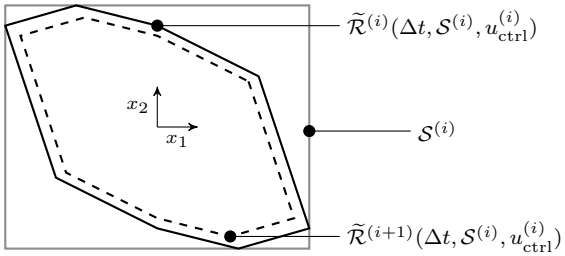


Fig. 2: If $\Psi_j^{(i)}(\mathcal{S})$ is chosen according to Def. 4, a feasible solution $\mathcal{S}^{(i)}$, $u_{\text{ctrl}}^{(i)}$ of $\mathbb{P}_{\text{cvx}}^{(i)}$ is also feasible for $\mathbb{P}_{\text{cvx}}^{(i+1)}$: both $\widetilde{\mathcal{R}}^{(i)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})$ and $\widetilde{\mathcal{R}}^{(i+1)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})$ are contained in $\mathcal{S}^{(i)}$, i.e., the invariance constraint in (13b) is satisfied for $\mathbb{P}_{\text{cvx}}^{(i)}$ and $\mathbb{P}_{\text{cvx}}^{(i+1)}$.

We have introduced $\Psi_j^{(i)}(\mathcal{S})$ so that higher-order derivatives only have to be evaluated prior to solving $\mathbb{P}_{\text{cvx}}^{(i)}$; otherwise, $\mathbb{P}_{\text{cvx}}^{(i)}$ would usually be non-convex. Let us now discuss the properties of $\Psi_j^{(i)}(\mathcal{S})$ in Def. 4:

C1) Recursive feasibility: The effect of choosing $\Psi_j^{(i)}(\mathcal{S})$ according to C1) in Def. 4 is illustrated in Fig. 2: Consider the solution $\mathcal{S}^{(i)}$, $u_{\text{ctrl}}^{(i)}$ of $\mathbb{P}_{\text{cvx}}^{(i)}$, which satisfies the invariance constraint in (13b), i.e., $\widetilde{\mathcal{R}}^{(i)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})\subseteq\mathcal{S}^{(i)}$. According to C1), $\Psi^{(i+1)}\left(\mathcal{S}^{(i)}\right)\leq\Psi^{(i)}\left(\mathcal{S}^{(i)}\right)$ and, thus, we obtain $\widetilde{\mathcal{R}}^{(i+1)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})\subseteq\widetilde{\mathcal{R}}^{(i)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})$, see Theorem 1 in Sec. V-B. Therefore, the solution of $\mathbb{P}_{\text{cvx}}^{(i)}$ also satisfies the invariance constraint in $\mathbb{P}_{\text{cvx}}^{(i+1)}$: $\widetilde{\mathcal{R}}^{(i+1)}(\Delta t,\mathcal{S}^{(i)},u_{\text{ctrl}}^{(i)})\subseteq\mathcal{S}^{(i)}$.

C2) Over-approximativeness: Ideally, we would like to ensure $\Psi_j^{(i)}(\mathcal{S})=\mathcal{L}_j(\mathcal{S})$ while satisfying all conditions in Def. 4, which is usually not possible since we consider general nonlinear systems. Since $\mathcal{S}\subseteq\mathcal{R}_o([0,\Delta t],\mathcal{S},u_{\text{ctrl}})$, our heuristic $\mathcal{L}_j(\mathcal{S})$ under-approximates $\mathcal{L}([0,\Delta t])$ and, therefore, we choose $\mathcal{L}_j(\mathcal{S})$ as a lower bound of $\Psi_j^{(i)}(\mathcal{S})$. As a side effect, this lower bound prevents $\Psi_j^{(i)}(\mathcal{S})\ll\mathcal{L}_j(\mathcal{S})$ with increasing i as a consequence of C1).

C3) Convexity: We use $\Psi_j^{(i)}(\mathcal{S})$ to compute the approximations of the reachable sets in (16). Therefore, $\Psi_j^{(i)}(\mathcal{S})$ has to admit a convex formulation of the invariance and state constraint in (13b) and (13c), respectively.

Subsequently, we propose a set of suitable functions $\Psi_j^{(i)}(\mathcal{S}), j\in\mathbb{N}_{[1:n_x]}$, to demonstrate that the conditions in Def. 4 are not overly restrictive as we assumed the flow function in (5) to be twice continuously differentiable. To this end, we parameterize the edgelengths of $\text{BOX}(\mathcal{S})=\langle x_{eq},\text{diag}\,(\Delta\bar{x})\rangle_{\mathcal{Z}}$ by the generator scaling factors s:

$$\Delta\bar{x}_l(s)=\sum_{m=1}^{\eta(\mathcal{S}_{\text{RCI}})}\left|e_l^T G_{(\cdot,m)}^{(i-1)}\right|s_m,\ l\in\mathbb{N}_{[1:n_x]}. \tag{20}$$

The formulation of $\Psi_j^{(i)}(\mathcal{S})$ is based on the over-approximation of the Lagrange remainder proposed in [43,

Proposition 1]: For $z \in \text{BOX}(\mathcal{S}) \times \text{BOX}(\mathcal{U} \times \mathcal{W}) = \langle [x_{eq}^T, u_{eq}^T, \mathbf{0}]^T, \text{diag}(\Delta\bar{z}) \rangle_{\mathcal{Z}}$

$$\mathcal{L}_j(\mathcal{S}) \leq \mathcal{L}_j(\text{BOX}(\mathcal{S})) = \frac{1}{2} \Delta\bar{z}^T \max_z \left| H^{(j)}(z) \right| \Delta\bar{z}, \quad (21)$$

where $H^{(j)}(\cdot)$ denotes the Hessian of the $j-$th component of the differential equation in (5) and the maximum operator is applied elementwise. Note that $\Delta\bar{z}_l(s) = \Delta\bar{x}_l(s)$, $l \in \mathbb{N}_{[1:n_x]}$, and the remaining components of $\Delta\bar{z}$ are constant.

Proposition 2 (Parameterized Lagrange Remainder): Consider the set of functions $\Psi_j^{(i)}(\mathcal{S}), j \in \mathbb{N}_{[1:n_x]}$:

$$\Psi_j^{(i)}(\mathcal{S}) = \Psi_{\text{quad},j}^{(i)}(\mathcal{S}) + \tau_0 \Delta\Psi_j^{(i)}, \quad (22)$$

with

$$\Psi_{\text{quad},j}^{(i)}(\mathcal{S}) = \sum_{l=1}^{n_z} \left| H_{(l,l)}^{(j)}\left(\zeta^{(i-1)}\right) \right| \tau_l + \sum_{l=1}^{n_z} \sum_{m=1, m\neq l}^{n_z} \left| H_{(l,m)}^{(j)}\left(\zeta^{(i-1)}\right) \right| \Delta\bar{z}_l(\mathbf{1}) \Delta\bar{z}_m(\mathbf{1}), \quad (23a)$$

$$\Delta\Psi_j^{(i)} = \mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}\right) - \Psi_{\text{quad},j}^{(i)}\left(\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}\right), \quad (23b)$$

where $\zeta^{(i-1)}$ denotes the maximizer in (21) for $\mathcal{S} = \mathcal{S}^{(i-1)}$. The auxiliary variables $\tau_0, \tau_1, \ldots, \tau_{n_z}$ are confined to the cones

$$\tau_0 \geq \max\left\{0, \left\{\frac{\Delta\bar{x}_l(s) - \Delta\bar{x}_l(\mathbf{1})}{\Delta\bar{x}_l^{(\mathcal{T})} - \Delta\bar{x}_l(\mathbf{1})}\right\}_{l \in \mathbb{N}_{[1:n_x]}}\right\}, \quad (24a)$$

$$\tau_l \geq \Delta\bar{z}_l^2(s), \; l \in \mathbb{N}_{[1:n_z]}, \quad (24b)$$

where $\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)} = \left\langle x_{eq}, \text{diag}\left(\Delta\bar{x}^{(\mathcal{T})}\right) \right\rangle_{\mathcal{Z}}$. The functions $\Psi_j^{(i)}(\mathcal{S})$, $j \in \mathbb{N}_{[1:n_x]}$, and the auxiliary constraints in (24) satisfy the conditions in Def. 4 and, thus, are a suitable approximation of the Lagrange remainder.

A proof of Proposition 2 is provided in Appendix I. We use a one-dimensional example, i.e., $\text{BOX}(\mathcal{S}) = \mathcal{S}$, in Fig. 3 to present our proposed functions $\Psi_j^{(i)}(\mathcal{S})$ for two subsequent iterations of $\mathbb{P}_{\text{cvx}}^{(i)}$, $i \in \{q, q+1\} \subset \mathbb{N}$. Moreover, we use Fig. 3 to illustrate that our $\Psi_j^{(i)}(\mathcal{S})$ satisfy C1) and C2) in Def. 4. Our proposed functions consist of a quadratic term $\Psi_{\text{quad},j}^{(i)}(\mathcal{S})$, which is motivated by the quadratic function in (21), and a piecewise linear term, which compensates the gap $\Delta\Psi_j^{(i)}$ between $\mathcal{L}_j(\text{BOX}(\mathcal{S}))$ and $\Psi_{\text{quad},j}^{(i)}(\mathcal{S})$ for $\mathcal{S} = \mathcal{S}^{(i-1)} \oplus \mathcal{T}^{(i-1)}$. As shown in Fig. 3, the combination of the two components ensures that our $\Psi_j^{(i)}(\mathcal{S})$ are over-approximative for all $\mathcal{S} \subseteq \mathcal{S}^{(i-1)} \oplus \mathcal{T}^{(i-1)}$. Satisfaction of the recursive feasibility condition C1) follows by construction since our $\Psi_j^{(i)}(\mathcal{S})$ are exact, i.e, $\Psi_j^{(i)}(\mathcal{S}) = \mathcal{L}_j(\text{BOX}(\mathcal{S}))$, for $\mathcal{S} = \mathcal{S}^{(i-1)}$; please compare $\Psi_j^{(q+1)}(\mathcal{S})$ with $\Psi_j^{(q)}(\mathcal{S})$ for $\mathcal{S} = \mathcal{S}^{(q)}$.

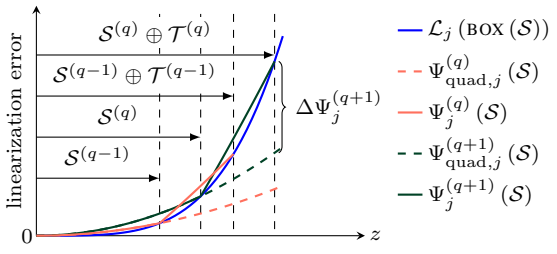


Fig. 3: Illustration of our functions $\Psi_j^{(i)}(\mathcal{S})$ from Proposition 2 for two subsequent iterations of $\mathbb{P}_{\text{cvx}}^{(i)}$, $i \in \{q, q+1\} \subset \mathbb{N}$, using a one-dimensional example: Our $\Psi_j^{(i)}(\mathcal{S})$ over-approximate $\mathcal{L}_j(\text{BOX}(\mathcal{S}))$ for every feasible $\mathcal{S}$ and are exact for $\mathcal{S} = \mathcal{S}^{(i-1)}$.

V. Successive Convexification

In the first part of this section, we discuss the choice of the cost function in (13a) and characterize the optimization problem $\mathbb{P}_{\text{cvx}}^{(i)}$. Afterwards, we discuss the properties of the sequence of solutions obtained by iteratively solving $\mathbb{P}_{\text{cvx}}^{(i)}$. Finally, we analyze the computational complexity of our algorithm.

A. Convex Programming Approximation

As previously mentioned, we aim at maximizing the volume of RCI sets: According to [63], the volume of the candidate RCI set $\mathcal{S}$ can be computed as

$$\text{VOLUME}(\mathcal{S}) = 2^{n_x} \sum_{j=1}^{n_{\text{comb}}} \underbrace{\left| \det\left(G_{(\cdot,\mathcal{J}(j))}^{(i-1)} \right) \right|}_{=w_j^{(i)}} \underbrace{\prod_{l \in \mathcal{J}(j)} s_l}_{=m_j^{(i)}}, \quad (25)$$

where $\mathcal{J}(j)$ denotes one of the n_{comb} possible n_x-membered subsets of $\mathbb{N}_{[1:\eta(\mathcal{S}_{\text{RCI}})]}$. To cast (25) as a concave cost function, we use

$$J_{\text{cvx}}^{(i)}(\mathcal{S}) = 2^{n_x} \sum_{j=1}^{n_{\text{comb}}} w_j^{(i)} \sqrt[n_x]{m_j^{(i)}}, \quad (26)$$

where concavity follows from concavity of the geometric mean [64, Sec. 3.1]. Note that $\text{VOLUME}\left(\mathcal{S}^{(i-1)}\right) = J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i-1)}\right)$ since $J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i-1)}\right)$ corresponds to setting $s = \mathbf{1}$, i.e., $m_j^{(i)} = 1$, $j \in \mathbb{N}_{[1:n_{\text{comb}}]}$. To derive a meaningful sequence of convex programming approximations $\mathbb{P}_{\text{cvx}}^{(i)}$, we require that the volume of $\mathcal{S}^{(i)}$ is monotonically increasing:

Lemma 1: For $i \in \mathbb{N}$, let $\mathcal{S}^{(i-1)}$, $\mathcal{S}^{(i)}$ denote the solution of $\mathbb{P}_{\text{cvx}}^{(i-1)}$, $\mathbb{P}_{\text{cvx}}^{(i)}$, respectively. If $J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i-1)}\right) \leq J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i)}\right)$, it holds that $\text{VOLUME}\left(\mathcal{S}^{(i-1)}\right) \leq \text{VOLUME}\left(\mathcal{S}^{(i)}\right)$.

Proof: By assumption, $J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i)}\right) - J_{\text{cvx}}^{(i)}\left(\mathcal{S}^{(i-1)}\right) \geq 0$, which can be rearranged as

$$\sum_{j \in \mathcal{J}_-} w_j^{(i)} \left| \sqrt[n_x]{m_j^{(i)}} - 1 \right| \leq \sum_{j \in \mathcal{J}_+} w_j^{(i)} \left| \sqrt[n_x]{m_j^{(i)}} - 1 \right|, \quad (27)$$

where we assign the index $j \in \mathbb{N}_{[1:n_{\text{comb}}]}$ to the set $\mathcal{J}_-$ if $\sqrt[n_x]{m_j^{(i)}} - 1 < 0$ and to $\mathcal{J}_+$ otherwise.

We use (27) to derive a similar result for $\text{VOLUME}\left(\mathcal{S}^{(i)}\right) - \text{VOLUME}\left(\mathcal{S}^{(i-1)}\right)$: Due to strict monotonicity of the addends

with respect to $m_j^{(i)}$ in both (25) and (26), we obtain the same index sets $\mathcal{J}_-$, $\mathcal{J}_+$ when applying the above approach to $\text{VOLUME}\left(\mathcal{S}^{(i)}\right) - \text{VOLUME}\left(\mathcal{S}^{(i-1)}\right)$. Hence, it remains to be shown that

$$\sum_{j\in\mathcal{J}_-} w_j^{(i)} \left|m_j^{(i)} - 1\right| \leq \sum_{j\in\mathcal{J}_+} w_j^{(i)} \left|m_j^{(i)} - 1\right|,$$

which follows from concavity of the geometric mean and a first-order Taylor expansion of both sides in (27). ∎

Next, we characterize the convex program $\mathbb{P}_{\text{cvx}}^{(i)}$.

Lemma 2: Let $\Psi^{(i)}(\mathcal{S})$ be chosen according to Def. 4. Then the optimization problem $\mathbb{P}_{\text{cvx}}^{(i)}$ can be cast as a conic program, i.e., $\mathbb{P}_{\text{cvx}}^{(i)}$ is a convex approximation of (10).

Proof: First, we recall the standard form of a conic program:

$$\min_{y} \quad c^T y \tag{28a}$$
$$\text{such that} \quad Cy = b, \tag{28b}$$
$$y \in \mathcal{K} \tag{28c}$$

where $\mathcal{K}$ is a product of lower-dimensional convex cones [62].

Cost function: The cost function $J_{\text{cvx}}^{(i)}(\mathcal{S})$ in (26) is a conical combination of geometric means and, thus, $J_{\text{cvx}}^{(i)}(\mathcal{S})$ is concave. Following the approach for the maximization of the geometric mean of non-negative affine functions in [65, Sec. 2.3 e)], we cast the maximization of (26) as the minimization of a linear cost function constrained by a product of second-order and linear cones.

Invariance constraint: By combining (17) and Def. 4 with the definition of the Minkowski addition of zonotopes, see (1a), we obtain that the zonotope representing $\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}^{(i)}, u_{\text{ctrl}}^{(i)})$ in (16a) is linear in the optimization variables. Hence by using (4), the approximation of the invariance constraint in (13b) is represented as a linear equality constraint and a product of linear cones.

State, input, and trust-region-like constraint: By combining Proposition 1 and Def. 4 with (1a), we obtain that the zonotope representing $\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}^{(i)}, u_{\text{ctrl}}^{(i)})$ in (16b) is linear in the optimization variables. The zonotope $\mathcal{S}_{\text{ctrl}}^{(i)}$ representing the controller $u_{\text{ctrl}}^{(i)}$ is linear in the optimization variables by definition. Since both $\mathcal{X}$ and $\mathcal{U}$ are assumed to be represented using polytopes, see (9), encoding the constraints in (13c) and (13d) using the criterion in (3) yields a product of linear cones. The same result applies for the trust-region-like constraint in (13e) since $\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}$ can be represented using a polytope defined by $2n_x$ half-spaces.

Auxiliary constraints: The constraint in (13f), which defines the center and generator matrix of $\mathcal{S}$, is a linear equality constraint and, thus, can be rearranged in the form of (28b). Finally, C3) in Def. 4 ensures that any required auxiliary constraints for the formulation of $\Psi^{(i)}(\mathcal{S})$ according to Def. 4 can be rewritten as a product of convex cones. ∎

Remark 1: By combining Lemma 2 and Proposition 2, the approximation of the Lagrange remainder used in our experiments yields a second-order cone program $\mathbb{P}_{\text{cvx}}^{(i)}$. The proof follows from the fact that the auxiliary variables in (24) are confined to a product of linear and second-order cones.

B. Successive Convexification Loop

Before discussing the properties of the sequence of solutions of $\mathbb{P}_{\text{cvx}}^{(i)}$, we briefly consider the initial trust-region $\mathcal{T}^{(0)}$ and the update mechanism, see Fig. 1. To ensure recursive feasibility of the sequence of solutions of $\mathbb{P}_{\text{cvx}}^{(i)}$, we require that $\mathcal{T}^{(i-1)}$ contains the origin in its interior. This prevents the trust-region-like constraint in (13e) from obstructing convergence to a possibly large RCI set. We introduce a suitable choice of $\mathcal{T}^{(0)}$ and a simple update strategy that is tailored to Proposition 2 in Appendix II.

The formulation of the approximations of the reachable sets in (16a) and (16b) realizes two appealing properties of the sequence of solutions of $\mathbb{P}_{\text{cvx}}^{(i)}$.

Theorem 1: Let $\mathbb{P}_{\text{cvx}}^{(m)}, m \in \mathbb{N}$, admit a feasible solution $\mathcal{S}^{(m)}$ and $u_{\text{ctrl}}^{(m)}$. For every $i > m, i \in \mathbb{N}$, it holds that

1) $\hat{\mathcal{S}}^{(i)} = \mathcal{S}^{(i-1)}$, and $\hat{u}_{\text{ctrl}}^{(i)} = u_{\text{ctrl}}^{(i-1)}$ are a feasible solution of $\mathbb{P}_{\text{cvx}}^{(i)}$, and,
2) the volume of the set $\mathcal{S}^{(i)}$ is monotonically increasing, i.e., $\text{VOLUME}\left(\mathcal{S}^{(i-1)}\right) \leq \text{VOLUME}\left(\mathcal{S}^{(i)}\right)$.

Proof:

1) The constraint in (13f) satisfies $\mathcal{S} = \hat{\mathcal{S}}^{(i)}$ for $s = \mathbf{1}$. From (17) and (19), it follows that

$$\begin{aligned}\widetilde{\mathcal{R}}_{\text{lin}}^{(m+1)}(\Delta t, \hat{\mathcal{S}}^{(m+1)}, \hat{u}_{\text{ctrl}}^{(m+1)}) &= \widetilde{\mathcal{R}}_{\text{lin}}^{(m)}(\Delta t, \mathcal{S}^{(m)}, u_{\text{ctrl}}^{(m)}),\\ \widetilde{\mathcal{R}}_{\text{lin}}^{(m+1)}([0, \Delta t], \hat{\mathcal{S}}^{(m+1)}) &= \widetilde{\mathcal{R}}_{\text{lin}}^{(m)}([0, \Delta t], \mathcal{S}^{(m)}).\end{aligned} \tag{29}$$

Moreover, since $\Psi^{(m+1)}\left(\hat{\mathcal{S}}^{(m+1)}\right) \leq \Psi^{(m)}\left(\mathcal{S}^{(m)}\right)$, see Def. 4, C1), we obtain that

$$\begin{aligned}&\mathcal{R}_p\left(\text{BOX}\left(\Psi^{(m+1)}\left(\hat{\mathcal{S}}^{(m+1)}\right)\right)\right)\\ &\quad\subseteq \mathcal{R}_p\left(\text{BOX}\left(\Psi^{(m)}\left(\mathcal{S}^{(m)}\right)\right)\right).\end{aligned} \tag{30}$$

By combining (29) and (30), it follows that

$$\begin{aligned}\widetilde{\mathcal{R}}^{(m+1)}(\Delta t, \hat{\mathcal{S}}^{(m+1)}, \hat{u}_{\text{ctrl}}^{(m+1)}) &\subseteq \hat{\mathcal{S}}^{(m+1)},\\ \widetilde{\mathcal{R}}^{(m+1)}([0, \Delta t], \hat{\mathcal{S}}^{(m+1)}, \hat{u}_{\text{ctrl}}^{(m+1)}) &\subseteq \mathcal{X},\end{aligned}$$

i.e., the constraints in (13b) and (13c) in $\mathbb{P}_{\text{cvx}}^{(m+1)}$ are satisfied. Since $\hat{u}_{\text{ctrl}}^{(m+1)} = u_{\text{ctrl}}^{(m)}$, satisfaction of the input constraint in (13d) follows trivially. The trust-region-like constraint in (13e) is satisfied since $\{\mathbf{0}\} \in \mathcal{T}^{(m)}$.

2) From feasibility of $\mathcal{S}^{(m)}$ for $\mathbb{P}_{\text{cvx}}^{(m+1)}$, it follows that $J_{\text{cvx}}^{(m+1)}\left(\mathcal{S}^{(m)}\right) = J_{\text{cvx}}^{(m+1)}\left(\hat{\mathcal{S}}^{(m+1)}\right)$ is a lower bound of $J_{\text{cvx}}^{(m+1)}\left(\mathcal{S}^{(m+1)}\right)$ and Lemma 2 ensures growing cost in (13a) if there exists a minimizer such that $J_{\text{cvx}}^{(m+1)}\left(\mathcal{S}^{(m)}\right) < J_{\text{cvx}}^{(m+1)}\left(\mathcal{S}^{(m+1)}\right)$. The claim follows from Lemma 1.

It follows by induction that the assertions hold for all $i > m$. ∎

Remark 2: Since n_{comb} can become prohibitively large for high-dimensional systems, we propose to maximize the volume of a zonotope $\mathcal{S}_{\text{red}}$ with $\eta(\mathcal{S}_{\text{red}}) \leq \eta(\mathcal{S}_{\text{RCI}})$ under the constraint that $\mathcal{S}_{\text{red}} \subseteq \mathcal{S}$. Using Lemma 1, it follows that we obtain a lower bound of $\text{VOLUME}\left(\mathcal{S}^{(i)}\right)$ whose value is monotonically increasing. Extending the results in Lemma 2

and Theorem 1 is straightforward and, therefore, omitted due to space restrictions.

Remark 3: So far, we have assumed that $\mathcal{S}^{(0)}$, $\mathcal{T}^{(0)}$ and $\Psi^{(1)}(\mathcal{S})$ are chosen so that there exists a feasible solution of $\mathbb{P}_{\text{cvx}}^{(1)}$. In the case that this assumption does not hold, we reformulate the constraints in (13b), (13c) as soft constraints, i.e., we add a slack variable to the constraints in (4c)

$$|[\Gamma, \gamma]|\,\mathbf{1} \leq s + \kappa_1,$$

and (3)

$$Hc_1 + |HG_1|\,\mathbf{1} \leq h + \kappa_2,$$

where κ_1, κ_2 are non-negative vectors of appropriate dimension. To recover a solution of the original convex program $\mathbb{P}_{\text{cvx}}^{(i)}$ if one exists, an exact penalty term is added to the cost function in (13a) [66]. Since the modified constraints are linear inequality constraints and the additional cost term due to the exact penalty is linear, the results in Lemma 2 and Theorem 1 are not affected by this modification.

C. Computational Complexity

Since the computation of the initial guess $\mathcal{S}^{(0)}$ is not a part of the proposed algorithm, we only consider the successive convexification loop and the verification of the converged solution.

The computation of the parameterized approximations of the reachable sets in (12) is based on the reachability analysis algorithm in [43], which has complexity $\mathcal{O}\left((n_x + n_u)^3\right)$ [67]. However, we cannot provide a general bound on the complexity of this step since the computation of $\Psi^{(i)}(\mathcal{S})$ is an interchangeable module. As we have shown in Lemma 2, $\mathbb{P}_{\text{cvx}}^{(i)}$ is a conic program, which subsumes optimization over the (nonsymmetric) exponential and power cone. Recently, it has been shown that there exist algorithms for nonsymmetric conic programming, which compute solutions in polynomial time [68], [69]. Since updating the trust-region $\mathcal{T}^{(i)}$ after solving $\mathbb{P}_{\text{cvx}}^{(i)}$ is optional, we do not consider this step. Let $\mathcal{O}_{\text{conic}}$ denote the complexity of solving $\mathbb{P}_{\text{cvx}}^{(i)}$, which can be polynomial in n_x, n_u, depending on the choice of $\Psi^{(i)}(\mathcal{S})$. The overall complexity of the successive convexification step then follows as $\mathcal{O}\left(N_{\text{cvx}}\left((n_x + n_u)^3 + \mathcal{O}_{\text{conic}}\right)\right)$, where N_{cvx} denotes the number of iterations of $\mathbb{P}_{\text{cvx}}^{(i)}$. Please note that we cannot provide an upper bound on N_{cvx}.

The computational effort for verifying the converged candidate RCI set is dominated by solving $\mathbb{P}_{\text{cvx}}^{(i)}$ and the computation of reachable sets which has polynomial complexity. Since we cannot guarantee that the verification eventually succeeds, we limit the number of iterations by N_{ver}. The overall complexity of our algorithm therefore follows as $\mathcal{O}\left((N_{\text{cvx}} + N_{\text{ver}})\left(\mathcal{O}_{\text{conic}} + (n_x + n_u)^3\right)\right)$.

VI. Numerical Experiments

In this section, we apply our robust control approach to a set of control systems proposed in the literature. We start by demonstrating the broad applicability and scalability of our approach in Sec. VI-A. In the subsections thereafter, we take a closer look at some selected results: First, we compare our algorithm with two approaches from the literature in Sec. VI-B. Afterwards, we consider a cartpole to demonstrate that our approach successfully handles underactuated systems in Sec. VI-C.

Our implementation and the benchmark systems alongside all parameters will be made publicly available with the next release of the AROC[1] toolbox [71]. For reachability analysis, we use our open-source toolbox CORA [72]. The convex programs $\mathbb{P}_{\text{cvx}}^{(i)}$ are modeled using CVX, a package for specifying and solving convex programs [73], [74] and solved using MOSEK [75]. All computations were conducted on a laptop equipped with an Intel Core i7-11370H and 64 GB of memory.

For the computation of the initial guess $\mathcal{S}^{(0)}$, we use a modified version of the algorithm for the computation of safe terminal sets of linear systems proposed in [8]. Throughout this section, the number of generators of the zonotope representing $\mathcal{S}_{\text{RCI}}$ is chosen as $\eta(\mathcal{S}_{\text{RCI}}) = 5n_x$. For the examples in Sec. VI-B and Sec. VI-C, the origin is chosen as the equilibrium for the computation of $\mathcal{S}_{\text{RCI}}$.

A. Computation Times

To demonstrate the broad applicability and scalability of our approach, we applied it to a variety of control systems where the dimension of the state space n_x ranges from two to 20. In case of the examples with $n_x = 2$, we maximized the concave approximation in (26) of the volume of $\mathcal{S}$; in case of the examples with $n_x \geq 4$, we maximized the volume of an inscribed zonotope $\mathcal{S}_{\text{red}} \subseteq \mathcal{S}$ whose order was chosen so that the number of addends in (26) does not exceed 1500, see Remark 2.

The results are summarized in Table I, where the fifth and sixth columns contain the number of convex programming iterations, i.e., the number of $\mathbb{P}_{\text{cvx}}^{(i)}$ that are solved, as well as the average solver time per $\mathbb{P}_{\text{cvx}}^{(i)}$, respectively. The seventh column shows the number of convex programming iterations required for verifying safety and the penultimate column indicates the success of the verification procedure. The computation time for the execution of our algorithm is shown in the last column. Note that the last column does not include the time for converting $\mathbb{P}_{\text{cvx}}^{(i)}$ into standard form since this step is not a part of our approach.

There are two main conclusions that can be drawn from the results in Table I: first, we successfully applied our approach to a variety of nonlinear control systems ranging from applications such as chemical reactors to under-actuated systems, see Sec. VI-C, despite only relying on linearization. In case of the pendubot example, the sequence of solutions of $\mathbb{P}_{\text{cvx}}^{(i)}$ converges to a feasible solution that cannot be verified as safe. Second, the total computation times indicate that the approach scales favorably with the dimension of the state space.

To obtain a better impression of the scalability of our approach, we consider a chain of n_{mass} nonlinear mass-spring-damper systems, where we increased n_{mass} from one ($n_x = 2$) to ten ($n_x = 20$). The dynamics of the $j-$th mass are governed

[1] https://tumcps.github.io/AROC/

TABLE I: Computational Effort

Example	n_x	n_u	n_w	$\mathbb{P}_{\text{cvx}}^{(i)}$		Verification		total time
				# iter.	∅ solver time	# iter.	feas.	
Artifical System [22] (Sec. VI-B.1)	2	2	2	9	0.18 s	3	✓	7.5 s
Jet Engine [16] (Sec. VI-B.2)	2	1	1	14	0.14 s	0	✓	3.2 s
Cart [71]	2	1	2	15	0.13 s	0	✓	3.9 s
Mass-Spring-Damper System [25]	2	1	2	16	0.15 s	0	✓	4.5 s
Cartpole (dynamics of the pendulum) [76]	2	1	1	18	0.15 s	0	✓	5.5 s
Cartpole [77] (Sec. VI-C)	4	1	1	16	0.93 s	0	✓	63.2 s
Pendubot [78]	4	1	1	11	1.29 s	max.	✗	-
Chemical Reactor [79], [80]	4	2	2	22	1.32 s	0	✓	71.1 s
Robot Arm [71]	4	2	4	13	0.81 s	1	✓	82.5 s
Longitudinal Quadrotor [5]	6	2	2	10	0.95 s	0	✓	46.7 s
Multi-Tank	8	8	3	10	4.73 s	0	✓	96.5 s
Coupled Van-der-Pol - based on [81] [82, Sec. 5.2]	10	5	5	14	4.04 s	0	✓	92.1 s
Chain of Mass-Spring-Damper-Systems ($n_{\text{mass}} = 10$, Sec. VI-A)	20	10	20	15	7.36 s	0	✓	124.2 s

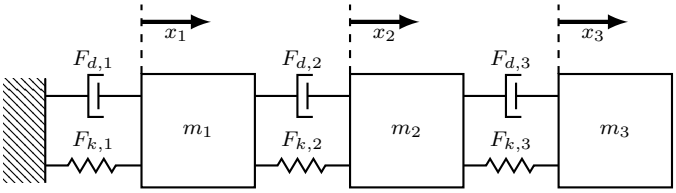


Fig. 4: Chain of Mass-Spring-Damper Systems ($n_{\text{mass}} = 3$).

by the set of differential equations (based on the cart system from [71])

$$\begin{bmatrix}\dot{x}_{j,1}\\ \dot{x}_{j,2}\end{bmatrix} = \begin{bmatrix} x_{j,2} + w_{j,1} \\ -F_{k,j}(x) - F_{d,j}(x) + u_j + w_{j,2}\end{bmatrix},$$
$$F_{k,j}(x) = 0.8\left((x_{j,1} - x_{j-1,1})^3 - (x_{j+1,1} - x_{j,1})^3\right),$$
$$F_{d,j}(x) = 1/3\left((x_{j,2} - x_{j-1,2})^2 - (x_{j+1,2} - x_{j,2})^2\right),$$

where $x_{j,1}, x_{j,2}$ denote the deviation from the equilibrium position and velocity, respectively. The resulting system for $n_{\text{mass}} = 3$ is depicted in 4. The constraint sets are chosen as $\mathcal{X}_j = [-6\,\text{m}, 6\,\text{m}] \times [-6\,{}^m/_s, 6\,{}^m/_s]$, $\mathcal{U}_j = [-14\,{}^m/_{s^2}, 14\,{}^m/_{s^2}]$, and the disturbance is confined to the set $\mathcal{W}_j = [-0.1\,{}^m/_s, 0.1\,{}^m/_s] \times [-0.1\,{}^m/_{s^2}, 0.1\,{}^m/_{s^2}]$. Measurements are taken with a sampling time of $\Delta t = 0.1\,\text{s}$.

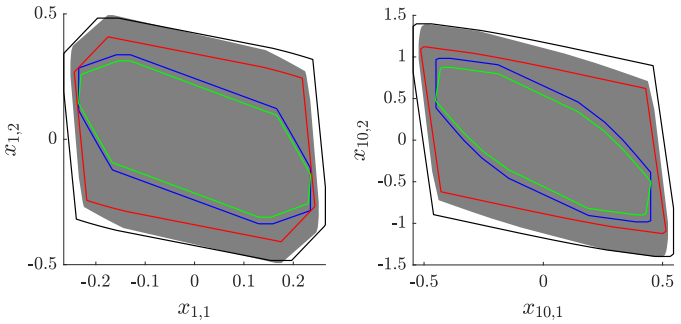
The results for $n_{\text{mass}} \in \mathbb{N}_{[1:10]}$ are summarized in Table II. As already indicated by the results in Table I, the computational effort of our approach only scales moderately with the dimension of state space. This result can be observed best by comparing the average solver time for $\mathbb{P}_{\text{cvx}}^{(i)}$ in the third column of Table II. Note that for all $n_{\text{mass}} \in \mathbb{N}_{[1:10]}$, the converged solution of the sequence of $\mathbb{P}_{\text{cvx}}^{(i)}$ was verified as safe without enlarging the approximations of the reachable sets in (16). The projections of $\mathcal{S}_{\text{RCI}}$ for $n_{\text{mass}} = 10$ onto the $x_{1,1} - x_{1,2}-$plane and onto the $x_{10,1} - x_{10,2}-$plane are shown in Fig. 5a and Fig. 5b respectively.

B. Comparison with Approaches From the Literature

In this section, we compare our approach to the results in [16], [22]. In [22], an ellipsoidal RCI set with a linear feedback controller is computed for the linearized system, which is computed using the approach in [21]. The approach in [16] computes a polytopic RCI set and a corresponding polynomial safety-preserving controller for polynomial systems.

TABLE II: Scalability: Chain of n_{mass} Mass-Spring-Damper Systems

n_{mass}	$\mathbb{P}_{\text{cvx}}^{(i)}$		Verification		total time
	# iter.	∅ solver time	# iter.	feas.	
1 ($n_x = 2$)	21	0.15 s	0	✓	8.0 s
2 ($n_x = 4$)	20	0.62 s	0	✓	43.4 s
3 ($n_x = 6$)	12	0.98 s	0	✓	34.3 s
4 ($n_x = 8$)	6	1.83 s	0	✓	48.3 s
5 ($n_x = 10$)	13	2.55 s	0	✓	61.44 s
6 ($n_x = 12$)	12	2.37 s	0	✓	43.4 s
7 ($n_x = 14$)	13	4.0 s	0	✓	73.7 s
8 ($n_x = 16$)	11	6.1 s	0	✓	98.6 s
9 ($n_x = 18$)	16	11.28 s	0	✓	229.4 s
10 ($n_x = 20$)	15	7.36 s	0	✓	124.2 s



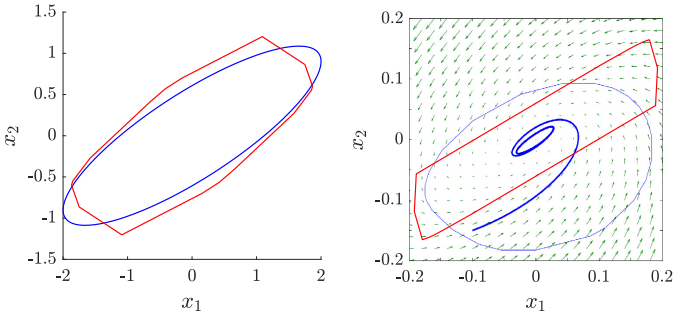
(a) $\mathcal{S}_{\text{RCI}}$ of m_1 (b) $\mathcal{S}_{\text{RCI}}$ of m_{10}

Fig. 5: Projections of the RCI set $\mathcal{S}_{\text{RCI}}$ for a chain of $n_{\text{mass}} = 10$ mass-spring-damper systems. Shown are: over-approximation of time-point $\mathcal{R}_o(\Delta t, \mathcal{S}_{\text{RCI}}, u_{\text{RCI}})$ (green) and time-interval $\mathcal{R}_o([0, \Delta t], \mathcal{S}_{\text{RCI}}, u_{\text{RCI}})$ (gray) reachable set, corresponding approximations of the converged $\mathbb{P}_{\text{cvx}}^{(i)}$ iteration $\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}_{\text{RCI}}, u_{\text{RCI}})$ (blue) and $\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}_{\text{RCI}}, u_{\text{RCI}})$ (black), respectively, $\mathcal{S}_{\text{RCI}}$ (red).

1) Robust Control Invariant Ellipsoid: The dynamics of the artificial, open-loop unstable system from [22] are governed by the set of differential equations

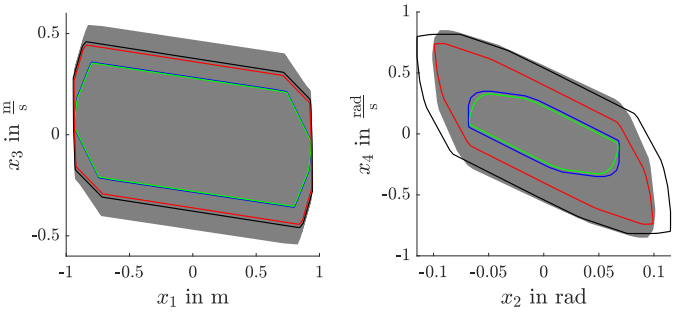
$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\end{bmatrix} = \begin{bmatrix} -x_1 + 2x_2 + 0.5u \\ -3x_1 + 4x_2 - 0.25x_2^3 - 2u + w\end{bmatrix}.$$

The constraint sets are chosen as $\mathcal{X} = [-6, 6] \times [-6, 6]$, $\mathcal{U} = [-2, 2]$, and the disturbance is confined to the set $\mathcal{W} = [-0.1, 0.1]$. Measurements are taken with a sampling time of $\Delta t = 0.1$ time units.



(a) Artificial System (b) Jet Engine, taken from [16]

Fig. 6: Comparison of our approach for the computation of RCI sets with the approaches from [22] (a) and [16] (b). The solution $\mathcal{S}_{\mathrm{RCI}}$ of our approach is depicted in red, the corresponding results from [16], [22] are depicted in blue.



(a) Position - velocity (b) Deflection - angular velocity

Fig. 7: Projections of the RCI set $\mathcal{S}_{\mathrm{RCI}}$ for the cartpole system. Shown are: over-approximation of time-point $\mathcal{R}_o(\Delta t, \mathcal{S}_{\mathrm{RCI}}, u_{\mathrm{RCI}})$ (green) and time-interval $\mathcal{R}_o([0, \Delta t], \mathcal{S}_{\mathrm{RCI}}, u_{\mathrm{RCI}})$ (gray) reachable set, corresponding approximations of the converged $\mathbb{P}^{(i)}_{\mathrm{cvx}}$ iteration $\widetilde{\mathcal{R}}^{(i)}(\Delta t, \mathcal{S}_{\mathrm{RCI}}, u_{\mathrm{RCI}})$ (blue) and $\widetilde{\mathcal{R}}^{(i)}([0, \Delta t], \mathcal{S}_{\mathrm{RCI}}, u_{\mathrm{RCI}})$ (black), respectively, $\mathcal{S}_{\mathrm{RCI}}$ (red).

The approach in [21] abstracts the nonlinear system to a linear differential inclusion. The RCI ellipsoid and the corresponding linear feedback are obtained by maximizing the volume of the ellipsoid subject to LMI conditions. However, the required linear differential inclusion has to be represented in vertex representation which compromises the scalability of their approach.

For comparison, we depict $\mathcal{S}_{\mathrm{RCI}}$ and the RCI ellipsoid for the artificial system in Fig. 6a. Due to the increased flexibility when using zonotopes to represent $\mathcal{S}_{\mathrm{RCI}}$, the volume of the RCI set is increased by 14% compared to [22].

2) Robust Control Invariant Polytope: In the second comparison, we consider the Moore-Greitzer model of a jet engine whose dynamics are governed by the set of differential equations [83]

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\end{bmatrix} = \begin{bmatrix}-x_2 - \frac{3}{2}x_1^2 - \frac{1}{2}x_1^3 + w\\ u\end{bmatrix}.$$

The constraint sets are chosen as $\mathcal{X} = [-0.2, 2] \times [-0.2, 0.2]$, $\mathcal{U} = [-0.35, 0.35]$, and the disturbance is confined to the set $\mathcal{W} = [-0.025, 0.025]$. Measurements are taken with a sampling time of $\Delta t = 0.1$ time units.

The approach in [16] tackles the task of computing an RCI set and the corresponding controller by solving a sequence of linear programs iterating between synthesizing a polynomial controller and adapting the RCI set. However, the linear programming relaxation of their polynomial optimization problem is obtained by lifting the problem to a higher-dimensional space and vertex enumeration in the lifted space. Furthermore, it is not clear, whether and how the lifting procedure can be automated.

The authors of [16] provide the results for a polytopic RCI set with 24 facets and a corresponding linear controller, which is shown in Fig. 6b alongside $\mathcal{S}_{\mathrm{RCI}}$. They obtain a larger RCI set since their approach can exploit beneficial higher-order effects in the dynamics. In addition, polytopes provide more flexibility in the design of the RCI set compared to zonotopes.

C. Cartpole Example

To demonstrate the ability of our approach to deal with underactuated systems, a cartpole is considered next. The dynamics are governed by the set of differential equations

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix} = \begin{bmatrix}x_3\\ x_4\\ f_3(x_2, x_4)\\ f_4(x_2, x_4)\end{bmatrix} + \begin{bmatrix}0\\ 0\\ \frac{1}{m_1+m_2-m_2\cos^2(x_2)}\\ \frac{\cos(x_2)}{m_1 l+m_2 l-m_2 l\cos^2(x_2)}\end{bmatrix}(u+w),$$

$$f_3(x_2, x_4) = \frac{m_2 g\cos(x_2)\sin(x_2) - m_2 l x_4^2\sin(x_2)}{m_1 + m_2 - m_2\cos^2(x_2)},$$

$$f_4(x_2, x_4) = \frac{(m_1+m_2)g\sin(x_2) - m_2 l x_4^2\sin(x_2)\cos(x_2)}{m_1 l + m_2 l - m_2 l\cos^2(x_2)},$$

where the states represent the distance x_1 of the cart from the origin, the deflection x_2 of the pole from the upright position, the velocity x_3 of the cart, and the angular velocity x_4 of the pole, respectively. The input u is the horizontal force acting on the cart and w denotes an unknown exogenous force, that is acting on the cart in the same direction. The parameters of the model $m_1 = 2.5\,\mathrm{kg}$, $m_2 = 1.0\,\mathrm{kg}$, $l = 0.5\,\mathrm{m}$, and $g = 9.81\,\frac{\mathrm{m}}{\mathrm{s}^2}$ are taken from [77]. The constraint sets are chosen as $\mathcal{X} = [-1\,\mathrm{m}, 1\,\mathrm{m}] \times [-\frac{3}{4}\pi\,\mathrm{rad}, \frac{3}{4}\pi\,\mathrm{rad}] \times [-2\,\frac{\mathrm{m}}{\mathrm{s}}, 2\,\frac{\mathrm{m}}{\mathrm{s}}] \times [-\frac{3}{2}\pi\,\frac{\mathrm{rad}}{\mathrm{s}}, \frac{3}{2}\pi\,\frac{\mathrm{rad}}{\mathrm{s}}]$, $\mathcal{U} = [-10\,\mathrm{N}, 10\,\mathrm{N}]$, and the disturbance is confined to the set $\mathcal{W} = [-0.5\,\mathrm{N}, 0.5\,\mathrm{N}]$. Measurements are taken with a sampling time of $\Delta t = 0.1\,\mathrm{s}$. To improve the control performance, we subdivide Δt into time steps of length $\Delta t_c = 0.025\,\mathrm{s}$ for sampling the control input as in [84]. The corresponding time-point reachable set of the abstraction $f_{\mathrm{lin}}(t)$ is computed as in [49, Sec. IV.A]; the other parts of our approach remain unaffected.

Note that the initial guess does not admit a feasible solution of $\mathbb{P}^{(1)}_{\mathrm{cvx}}$. We resolved this issue as described in Remark 3. The projections of $\mathcal{S}_{\mathrm{RCI}}$ onto the $x_1 - x_3-$plane and onto the $x_2 - x_4-$plane are shown in Fig. 7a and Fig. 7b respectively.

VII. Conclusions

We have presented a scalable algorithm for the computation of RCI sets of nonlinear sampled-data systems. To this end, we designed a successive convexification procedure, which computes a sequence of candidate RCI sets with monotonically increasing volume. The core of our approach is a tailored approximation of reachable sets that enables to jointly synthesize an RCI set and a corresponding safety-preserving

controller in a single convex program. While approaches in the literature have only been applied to low-dimensional systems, we show results for a broad range of control systems with up to 20 dimensions. Moreover, the computational effort of our approach only scales moderately with the dimension of state space due to the combination of scalable reachability analysis and convex optimization.

APPENDIX I
PROOF OF PROPOSITION 2

a) C2): We show that $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}\right)\right) \leq \Psi_j^{(i)}\left(\mathcal{S}\right)$ for $\mathcal{S} \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}$, which is sufficient for C2) to hold, see (21). We split the proof into three parts and set $\tau_l = \Delta\bar{z}_l^2\left(s\right),\ l \in \mathbb{N}_{[1:n_z]}$, see (24b). In addition, we use ζ to denote the maximizer in (21) and $\zeta^{(\mathcal{T})}$ to denote the maximizer in (21) for $\mathcal{S} = \mathcal{S}^{(i-1)} \oplus \mathcal{T}^{(i-1)}$.

Case $\mathcal{S} \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$: From (24a), we obtain $\tau_0 = 0$. Since $\mathcal{S} \subseteq \text{BOX}\left(\mathcal{S}^{(i)}\right) \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$, it holds that $\left|H^{(j)}\left(\zeta\right)\right| \leq \left|H^{(j)}\left(\zeta^{(i-1)}\right)\right|$ and, therefore, $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}\right)\right) \leq \Psi_{\text{quad},j}^{(i)}\left(\mathcal{S}\right) = \Psi_j^{(i)}\left(\mathcal{S}\right)$.

Case $\text{BOX}\left(\mathcal{S}\right) \supseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$: First, note that for $\text{BOX}\left(\mathcal{S}\right) = \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$, i.e., $\tau_0 = 0$, and $\text{BOX}\left(\mathcal{S}\right) = \text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}$, i.e., $\tau_0 = 1$, it holds that $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}\right)\right) = \Psi_j^{(i)}\left(\mathcal{S}\right)$, see (22), (23). Due to the formulation of (22), we essentially consider the set $\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \tau_0\mathcal{T}^{(i-1)} \supseteq \text{BOX}\left(\mathcal{S}\right)$ for the computation of $\Psi_j^{(i)}\left(\mathcal{S}\right)$.

We consider each addend of $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}\right)\right)$ separately and, thus, have to show that

$$\begin{aligned}
&\left|H_{(l,l)}^{(j)}\left(\zeta\right)\right|\Delta\bar{z}_l^2\left(s\right) \leq \left|H_{(l,l)}^{(j)}\left(\zeta^{(i-1)}\right)\right|\Delta\bar{z}_l^2\left(s\right)\\
&\quad + \tau_0\left(\left|H_{(l,l)}^{(j)}\left(\zeta^{(\mathcal{T})}\right)\right| - \left|H_{(l,l)}^{(j)}\left(\zeta^{(i-1)}\right)\right|\right)\left(\Delta\bar{z}_l^{(\mathcal{T})}\right)^2,\\
\iff &\left(\left|H_{(l,l)}^{(j)}\left(\zeta\right)\right| - \left|H_{(l,l)}^{(j)}\left(\zeta^{(i-1)}\right)\right|\right)\Delta\bar{z}_l^2\left(s\right)\\
&\quad \leq \tau_0\left(\left|H_{(l,l)}^{(j)}\left(\zeta^{(\mathcal{T})}\right)\right| - \left|H_{(l,l)}^{(j)}\left(\zeta^{(i-1)}\right)\right|\right)\left(\Delta\bar{z}_l^{(\mathcal{T})}\right)^2,
\end{aligned} \tag{31}$$

holds in case of the main diagonal elements of $H^{(j)}\left(\cdot\right)$ and

$$\begin{aligned}
&\left|H_{(l,m)}^{(j)}\left(\zeta\right)\right|\Delta\bar{z}_l\left(s\right)\Delta\bar{z}_m\left(s\right)\\
&\quad \leq \tau_0\left(\left|H_{(l,m)}^{(j)}\left(\zeta^{(\mathcal{T})}\right)\right|\Delta\bar{z}_l^{(\mathcal{T})}\Delta\bar{z}_m^{(\mathcal{T})}\right)\\
&\qquad + \left(1-\tau_0\right)\left|H_{(l,m)}^{(j)}\left(\zeta^{(i-1)}\right)\right|\Delta\bar{z}_l\left(\mathbf{1}\right)\Delta\bar{z}_m\left(\mathbf{1}\right),
\end{aligned} \tag{32}$$

holds in case of the off-diagonal elements of $H^{(j)}\left(\cdot\right)$.

For $\tau_0 = 0$ and $\tau_0 = 1$, it holds that both sides in (31) and (32) are equivalent. By resolving (24a) with respect to $\Delta\bar{z}_l\left(s\right)$, the left-hand side in both (31) and (32) can be re-written as a quadratic function in τ_0 with non-negative coefficients, which is convex. The claim follows since the right-hand side in both (31) and (32) is affine in τ_0.

Case $\text{BOX}\left(\mathcal{S}\right) \not\supseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right) \wedge \mathcal{S} \not\subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$: This case follows by combining the proof of the previous two cases.

b) C1): As we have already shown, it holds that $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}^{(i)}\right)\right) = \Psi_j^{(i+1)}\left(\mathcal{S}^{(i)}\right)$ and $\mathcal{L}_j\left(\text{BOX}\left(\mathcal{S}\right)\right) \leq \Psi_j^{(i)}\left(\mathcal{S}\right)$, see the proof of C2). Hence, the proposed functions $\Psi_j^{(i)}\left(\mathcal{S}\right), j \in \mathbb{N}_{[1:n_x]}$, satisfy C1).

c) C3): Since the functions $\Psi_j^{(i)}\left(\mathcal{S}\right), j \in \mathbb{N}_{[1:n_x]}$, are linear in $\tau_0, \tau_1, \ldots, \tau_{n_z}$, see (22) and (23), it follows that the center and generator matrix of $\mathcal{R}_p\left(\text{BOX}\left(\Psi^{(i)}\left(\mathcal{S}\right)\right)\right)$ are constant and linear in $\tau_0, \tau_1, \ldots, \tau_{n_z}$, respectively, see the definition of $\text{BOX}\left(\cdot\right)$ and [61]. Thus, C3) is satisfied.

Using $\Delta\bar{z}_l\left(s\right)$, see (20), the constraint in (24a) is equivalent to a set of n_x+1 linear inequalities, and, hence, representable using a product of linear cones. From (20), it follows that the inequality constraints in (24b) can be rewritten as a second-order cone constraint as described in [62, Sec. 3.2.3]. Hence, the constraints due to the auxiliary variables in Proposition 2 comply with the requirements in C3), which concludes the proof.

APPENDIX II
TRUST REGION UPDATE

We introduce a suitable choice of $\mathcal{T}^{(0)}$ and a simple update strategy that is tailored to the approximation $\Psi^{(i)}\left(\mathcal{S}\right)$ of the Lagrange remainder proposed in Proposition 2. $\mathcal{T}^{(0)}$ is chosen as a box with non-empty interior that is centered at the origin. We compute the updated trust-region $\mathcal{T}^{(i)}, i \in \mathbb{N}$, according to the following rules:

- $\mathcal{S}^{(i)} \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$: It follows that $\text{BOX}\left(\mathcal{S}^{(i)}\right) \subseteq \text{BOX}\left(\mathcal{S}^{(i-1)}\right)$, i.e., $\Delta\bar{z}_l\left(\mathbf{1}\right) \geq \Delta\bar{z}_l\left(s\right),\ l \in \mathbb{N}_{[1:n_x]}$, and, thus, we obtain that $\tau_0 = 0$ from (24a). Hence, the trust-region does not affect the approximation error and we set $\mathcal{T}^{(i-1)} = \mathcal{T}^{(i)}$;
- $\mathcal{S}^{(i)}$ intersects with the boundary of $\text{BOX}\left(\mathcal{S}^{(i-1)}\right) \oplus \mathcal{T}^{(i-1)}$: There exists at least one $l \in \mathbb{N}_{[1:n_x]}$ so that the trust-region prevents the optimizer from enlarging $\mathcal{S}^{(i)}$ even further in the direction of e_l. To accelerate convergence, we uniformly enlarge the trust-region by a factor $\overline{\sigma} > 1$.
- otherwise: We consider $\mathcal{S}_{\mathcal{T}}^{(i-1)}(\tau_0) = \mathcal{S}^{(i-1)} \oplus \tau_0\mathcal{T}^{(i-1)}$, for which we compute $\Psi_j^{(i)}\left(s\right)$ in Proposition 2, and, inspired by [57], we evaluate the following relative error criterion

$$\varrho_j = \frac{\Psi_j^{(i)}\left(\mathcal{S}_{\mathcal{T}}^{(i-1)}(\tau_0)\right) - \mathcal{L}_j\left(\mathcal{S}_{\mathcal{T}}^{(i-1)}(\tau_0)\right)}{\mathcal{L}_j\left(\mathcal{S}^{(i)}\right)}.$$

If the maximum relative error $\max_{j\in\mathbb{N}_{[1:n_x]}}\varrho_j$ exceeds the strictly positive upper bound $\overline{\varrho}$, we uniformly contract the trust-region by a factor $1/\underline{\sigma}$ where $\underline{\sigma} > 1$; otherwise we set $\mathcal{T}^{(i-1)} = \mathcal{T}^{(i)}$.

Based on the assumption that the flow function of the dynamical system in (5) is twice continuously differentiable, it can be verified that the above procedure ensures that the origin lies within the interior of $\mathcal{T}^{(i)}, i \in \mathbb{N}_0$.

REFERENCES

[1] D. Mayne, "Robust and stochastic MPC: Are we going in the right direction?" *IFAC-PapersOnLine*, vol. 48, no. 23, pp. 1–8, 2015, 5th IFAC Conference on Nonlinear Model Predictive Control 2015.

[2] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[3] B. Schürmann, N. Kochdumper, and M. Althoff, "Reachset model predictive control for disturbed nonlinear systems," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 3463–3470.

[4] C. Pek, S. Manzinger, M. Koschi, and M. Althoff, "Using online verification to prevent autonomous vehicles from causing accidents," *Nature Machine Intelligence*, vol. 2, no. 9, pp. 518–528, 2020.

[5] I. M. Mitchell, J. Yeh, F. J. Laine, and C. J. Tomlin, "Ensuring safety for sampled data systems: An efficient algorithm for filtering potentially unsafe input signals," in *2016 IEEE Conference on Decision and Control (CDC)*, 2016, pp. 7431–7438.

[6] K. P. Wabersich and M. N. Zeilinger, "Linear model predictive safety certification for learning-based control," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 7130–7135.

[7] D. Bertsekas, "Infinite time reachability of state-space regions by using feedback control," *IEEE Transactions on Automatic Control*, vol. 17, no. 5, pp. 604–613, 1972.

[8] F. Gruber and M. Althoff, "Computing safe sets of linear sampled-data systems," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 385–390, 2021.

[9] M. Rungger and P. Tabuada, "Computing robust controlled invariant sets of linear systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3665–3670, 2017.

[10] S. V. Rakovic and M. Baric, "Parameterized robust control invariant sets for linear systems: Theoretical advances and computational remarks," *IEEE Transactions on Automatic Control*, vol. 55, no. 7, pp. 1599–1614, 2010.

[11] M. Fiacchini, T. Alamo, and E. Camacho, "On the computation of convex robust control invariant sets for nonlinear systems," *Automatica*, vol. 46, no. 8, pp. 1334–1338, 2010.

[12] ——, "Invariant sets computation for convex difference inclusions systems," *Systems & Control Letters*, vol. 61, no. 8, pp. 819–826, 2012.

[13] R. Robles, A. Sala, and M. Bernal, "Performance-oriented quasi-lpv modeling of nonlinear systems," *International Journal of Robust and Nonlinear Control*, vol. 29, no. 5, pp. 1230–1248, 2019.

[14] M. Fiacchini, "Convex difference inclusions for systems analysis and design," Ph.D. dissertation, Universidad de Sevilla. Departamento de Ingeniería de Sistemas y Automática, 2010.

[15] A. Sala, C. Ariño, and R. Robles, "Gain-scheduled control via convex nonlinear parameter varying models," *IFAC-PapersOnLine*, vol. 52, no. 28, pp. 70–75, 2019, 3rd IFAC Workshop on Linear Parameter Varying Systems LPVS 2019.

[16] M. A. Ben Sassi and A. Girard, "Controller synthesis for robust invariance of polynomial dynamical systems using linear programming," *Systems & Control Letters*, vol. 61, no. 4, pp. 506–512, 2012.

[17] ——, "Computation of polytopic invariants for polynomial dynamical systems using linear programming," *Automatica*, vol. 48, no. 12, pp. 3114–3121, 2012.

[18] M. A. Ben Sassi, A. Girard, and S. Sankaranarayanan, "Iterative computation of polyhedral invariants sets for polynomial dynamical systems," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 6348–6353.

[19] M. Kojima, S. Kim, and H. Waki, "A general framework for convex relaxation of polynomial optimization problems over cones," *Journal of the Operations Research Society of Japan*, vol. 2, 2003.

[20] J.-B. Lasserre, "Global optimization with polynomials and the problem of moments," *SIAM Journal on Optimization*, vol. 11, 2004.

[21] W.-H. Chen, J. O'Reilly, and D. Ballance, "On the terminal region of model predictive control for non-linear systems with input/state constraints," *International Journal of Adaptive Control and Signal Processing*, vol. 17, pp. 195–207, 2003.

[22] S. Yu, C. Maier, H. Chen, and F. Allgöwer, "Tube MPC scheme based on robust control invariant set with application to Lipschitz nonlinear systems," *Systems & Control Letters*, vol. 62, no. 2, pp. 194–200, 2013.

[23] M. Lazar and M. Tetteroo, "Computation of terminal costs and sets for discrete–time nonlinear MPC," *IFAC-PapersOnLine*, vol. 51, no. 20, pp. 141–146, 2018, 6th IFAC Conference on Nonlinear Model Predictive Control 2018.

[24] S. Lucia, P. Rumschinski, A. J. Krener, and R. Findeisen, "Improved design of nonlinear model predictive controllers," *IFAC-PapersOnLine*, vol. 48, no. 23, pp. 254–259, 2015, 5th IFAC Conference on Nonlinear Model Predictive Control 2015.

[25] M. E. Villanueva, J. C. Li, X. Feng, B. Chachuat, and B. Houska, "Computing ellipsoidal robust forward invariant tubes for nonlinear MPC," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7175–7180, 2017, 20th IFAC World Congress.

[26] J. Köhler, M. A. Müller, and F. Allgöwer, "A novel constraint tightening approach for nonlinear robust model predictive control," in *2018 Annual American Control Conference (ACC)*, 2018, pp. 728–734.

[27] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017, pp. 2242–2253.

[28] L. Grüne and H. Zidani, "Zubov's equation for state-constrained perturbed nonlinear systems," *Mathematical Control and Related Fields*, vol. 5, no. 1, pp. 55–71, 2015.

[29] B. Xue, Q. Wang, N. Zhan, S. Wang, and Z. She, "Synthesizing robust domains of attraction for state-constrained perturbed polynomial systems," *SIAM Journal on Control and Optimization*, vol. 59, no. 2, pp. 1083–1108, 2021.

[30] B. Xue, Q. Wang, N. Zhan, and M. Fränzle, "Robust invariant sets generation for state-constrained perturbed polynomial systems," in *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, 2019, p. 128–137.

[31] B. Xue, N. Zhan, and Y. Li, "Robust regions of attraction generation for state-constrained perturbed discrete-time polynomial systems," in *Preprints of the 21st IFAC World Congress (Virtual)*, 2020.

[32] M. Korda, D. Henrion, and C. N. Jones, "Convex computation of the maximum controlled invariant set for polynomial control systems," *SIAM Journal on Control and Optimization*, vol. 52, no. 5, pp. 2944–2969, 2014.

[33] C. Schlosser and M. Korda, "Converging outer approximations to global attractors using semidefinite programming," 2020. [Online]. Available: https://arxiv.org/abs/2005.03346

[34] A. Oustry, C. Cardozo, P. Pantiatici, and D. Henrion, "Maximal positively invariant set determination for transient stability assessment in power systems," in *2019 IEEE Conference on Decision and Control (CDC)*, 2019, pp. 6572–6577.

[35] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *2019 18th European Control Conference (ECC)*, 2019, pp. 3420–3431.

[36] M. Rauscher, M. Kimmel, and S. Hirche, "Constrained robot control using control barrier functions," in *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2016, pp. 279–285.

[37] L. Wang, A. D. Ames, and M. Egerstedt, "Safe certificate-based maneuvers for teams of quadrotors using differential flatness," in *2017 IEEE International Conference on Robotics and Automation (ICRA)*, 2017, pp. 3293–3298.

[38] S. Kolathaya, J. Reher, A. Hereid, and A. D. Ames, "Input to state stabilizing control lyapunov functions for robust bipedal robotic locomotion," in *2018 Annual American Control Conference (ACC)*, 2018, pp. 2224–2230.

[39] B. T. Lopez, J.-J. E. Slotine, and J. P. How, "Robust adaptive control barrier functions: An adaptive and data-driven approach to safety," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 1031–1036, 2021.

[40] A. J. Taylor and A. D. Ames, "Adaptive safety with control barrier functions," in *2020 American Control Conference (ACC)*, 2020, pp. 1399–1405.

[41] X. Xu, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Robustness of control barrier functions for safety critical control," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 54–61, 2015, Analysis and Design of Hybrid Systems ADHS.

[42] A. A. Ahmadi, G. Hall, A. Papachristodoulou, J. Saunderson, and Y. Zheng, "Improving efficiency and scalability of sum of squares optimization: Recent advances and limitations," in *2017 IEEE Conference on Decision and Control (CDC)*, 2017, pp. 453–462.

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

[44] M. Althoff, G. Frehse, and A. Girard, "Set propagation techniques for reachability analysis," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 4, no. 1, p. 369–395, 2021.

[45] W. Kühn, "Rigorously computed orbits of dynamical systems without the wrapping effect," *Computing*, vol. 61, pp. 47–67, 1998.

[46] M. Althoff, "Reachability analysis and its application to the safety assessment of autonomous cars," Ph.D. dissertation, Technische Universität München, 2010.

[47] M. Althoff, "Reachability analysis of large linear systems with uncertain inputs in the krylov subspace," *IEEE Transactions on Automatic Control*, vol. 65, no. 2, pp. 477–492, 2020.

[48] A. Gupta and P. Falcone, "Full-complexity characterization of control-invariant domains for systems with uncertain parameter dependence," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 19–24, 2019.

[49] B. Schürmann and M. Althoff, "Optimizing sets of solutions for controlling constrained nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 3, pp. 981–994, 2021.

[50] M. Althoff, O. Stursberg, and M. Buss, "Computing reachable sets of hybrid systems using a combination of zonotopes and polytopes," *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 233–249, 2010.

[51] A. Kulmburg and M. Althoff, "On the co-NP-completeness of the zonotope containment problem," *European Journal of Control*, vol. 62, pp. 84–91, 2021, 2021 European Control Conference Special Issue.

[52] K. Ghasemi, S. Sadraddini, and C. Belta, "Compositional synthesis via a convex parameterization of assume-guarantee contracts," in *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, 2020.

[53] A. Platzer and E. M. Clarke, "Formal verification of curved flight collision avoidance maneuvers: A case study," in *Formal Methods*, A. Cavalcanti and D. R. Dams, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 547–562.

[54] I. Mitchell, "Comparing forward and backward reachability as tools for safety analysis," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4416 LNCS, pp. 428–443, 2007.

[55] S. Raković, F. Fontes, and I. Kolmanovsky, "Reachability and invariance for linear sampled–data systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3057–3062, 2017, 20th IFAC World Congress.

[56] Y. Mao, M. Szmuk, X. Xu, and B. Acikmese, "Successive convexification: A superlinearly convergent algorithm for non-convex optimal control problems," 2019. [Online]. Available: https://arxiv.org/abs/1612.06830

[57] T. P. Reynolds and M. Mesbahi, "The crawling phenomenon in sequential convex programming," in *2020 American Control Conference (ACC)*, 2020, pp. 3613–3618.

[58] I. Mitchell, J. Budzis, and A. Bolyachevets, "Invariant, viability and discriminating kernel under-approximation via zonotope scaling: Poster abstract," in *HSCC 2019 - Proceedings of the 2019 22nd ACM International Conference on Hybrid Systems: Computation and Control*, 2019, pp. 268–269.

[59] J. Nocedal and S. Wright, *Numerical Optimization*, 2nd ed., ser. Springer Series in Operations Research and Financial Engineering. Springer, New York, NY, 2006.

[60] M. Wetzlinger, A. Kulmburg, and M. Althoff, "Adaptive parameter tuning for reachability analysis of nonlinear systems," in *HSCC 2021 - Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control (part of CPS-IoT Week)*, 2021.

[61] M. Althoff, C. Le Guernic, and B. Krogh, "Reachable set computation for uncertain time-varying linear systems," in *HSCC'11 - Proceedings of the 2011 ACM/SIGBED Hybrid Systems: Computation and Control*, 2011, pp. 93–102.

[62] Mosek ApS, *MOSEK Modeling Cookbook*, 2020. [Online]. Available: https://docs.mosek.com/modeling-cookbook/index.html

[63] E. Gover and N. Krikorian, "Determinants and the volumes of parallelotopes and zonotopes," *Linear Algebra and its Applications*, vol. 433, no. 1, pp. 28–40, 2010.

[64] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[65] F. Alizadeh and D. Goldfarb, "Second-order cone programming," *Mathematical Programming, Series B*, vol. 95, no. 1, pp. 3–51, 2003.

[66] S.-P. Han and O. Mangasarian, "Exact penalty functions in nonlinear programming," *Mathematical Programming*, vol. 17, no. 1, pp. 251–269, 1979.

[67] B. Schürmann and M. Althoff, "Guaranteeing constraints of disturbed nonlinear systems using set-based optimal control in generator space," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 11 515–11 522, 2017, 20th IFAC World Congress.

[68] S. A. Serrano, "Algorithms for unsymmetric cone optimization and an implementation for problems with the exponential cone," Ph.D. dissertation, Stanford University, 2015.

[69] R. Badenbroek and J. Dahl, "An algorithm for nonsymmetric conic optimization inspired by mosek," *Optimization Methods and Software*, vol. 0, no. 0, pp. 1–38, 2021.

[70] N. Kochdumper and M. Althoff, "Sparse polynomial zonotopes: A novel set representation for reachability analysis," *IEEE Transactions on Automatic Control*, pp. 1–1, 2020.

[71] N. Kochdumper, F. Gruber, B. Schürmann, V. Gaßmann, M. Klischat, and M. Althoff, "Aroc: A toolbox for automated reachset optimal controller synthesis," in *HSCC 2021 - Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control (part of CPS-IoT Week)*, 2021.

[72] M. Althoff, "An introduction to cora 2015," in *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*, 2015.

[73] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," *Lecture Notes in Control and Information Sciences*, vol. 371, pp. 95–110, 2008.

[74] ——, "CVX: Matlab software for disciplined convex programming, version 2.1," Mar. 2014. [Online]. Available: http://cvxr.com/cvx

[75] Mosek ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.2.47*, 2021. [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html

[76] R. Findeisen, "Nonlinear model predictive control : a sampled data feedback perspective," Ph.D. dissertation, Universität Stuttgart, 2005.

[77] J. Theis, "Sum-of-squares applications in nonlinear controller synthesis," Master's thesis, University of California, Berkeley, 2012.

[78] H. Yin, A. Packard, M. Arcak, and P. Seiler, "Finite horizon backward reachability analysis and control synthesis for uncertain nonlinear systems," in *2019 American Control Conference (ACC)*, 2019, pp. 5020–5026.

[79] K.-U. Klatt and S. Engell, "Gain-scheduling trajectory control of a continuous stirred tank reactor," *Computers & Chemical Engineering*, vol. 22, no. 4, pp. 491–502, 1998.

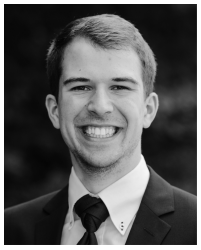
[80] S. Subramanian, S. Lucia, and S. Engell, "Handling structural plant-model mismatch via multi-stage nonlinear model predictive control," in *2015 European Control Conference (ECC)*, 2015, pp. 1602–1607.

[81] M. Dutra, A. De Pina Filho, and V. Romano, "Modeling of a bipedal locomotor using coupled nonlinear oscillators of van der pol," *Biological Cybernetics*, vol. 88, no. 4, pp. 286–292, 2003.

[82] A. Bestler and K. Graichen, "Distributed model predictive control for continuous-time nonlinear systems based on suboptimal admm," *Optimal Control Applications and Methods*, vol. 40, no. 1, pp. 1–23, 2019.

[83] M. Krstic, I. Kanellakopoulos, and P. V. Kokotovic, *Nonlinear and Adaptive Control Design*, 1st ed. Wiley-Interscience, 1995.

[84] B. Schürmann, M. Klischat, N. Kochdumper, and M. Althoff, "Formal safety net control using backward reachability analysis," *IEEE Transactions on Automatic Control*, pp. 1–1, 2021.



Lukas Schäfer joined the Cyber-Physical Systems Group at the Technical University of Munich, Germany, under Prof. Dr.-Ing. Matthias Althoff in 2021. He received the M.Sc. degree in robotics, cognition, intelligence and the B.Sc. degree in mechanical engineering both from the Technical University of Munich as well as the B.Eng. degree in Business Administration and Engineering from the Baden-Wuerttemberg Cooperative State University Stuttgart, Germany. His research is focused around robust safety-preserving controller synthesis of nonlinear systems.

Felix Gruber is a Ph.D. candidate in Computer Science at the Technical University of Munich, Germany. In 2017, he received the Master of Science degree in electrical engineering from the Technical University of Munich, Germany, and was a visiting student researcher at the University of California, Berkeley, Berkeley, CA, USA. His research interests include control theory, optimization, and reachability analysis, with applications to safety-critical systems.

Matthias Althoff is an associate professor in computer science at the Technical University of Munich, Germany. He received his diploma engineering degree in Mechanical Engineering in 2005, and his Ph.D. degree in Electrical Engineering in 2010, both from the Technical University of Munich, Germany. From 2010 to 2012 he was a postdoctoral researcher at Carnegie Mellon University, Pittsburgh, USA, and from 2012 to 2013 an assistant professor at Ilmenau University of Technology, Germany. His research interests include formal verification of continuous and hybrid systems, reachability analysis, planning algorithms, nonlinear control, automated vehicles, and power systems.