

Computing Controlled Invariant Sets of Nonlinear Control-Affine Systems

Scott Brown

Mohammad Khajenejad

Sze Zheng Yong

Sonia Martínez

Abstract—In this paper, we consider the computation of controlled invariant sets (CIS) of discrete-time nonlinear control-affine systems. We propose an iterative refinement procedure based on polytopic inclusion functions, which is able to inner-approximate the maximal controlled invariant set to within a guaranteed robustness margin. In particular, this procedure allows us to guarantee the invariance of the resulting near-maximal CIS while also computing sets of control inputs which enforce the invariance. Further, we propose an alternative version of this procedure which refines the CIS by computing backward reachable sets of individual components of set unions, rather than all at once. This reduces the total number of inclusion checking operations required for convergence, especially when compared with existing methods. Finally, we compare our methods to a sampling based approach and demonstrate the improved accuracy and faster convergence.

I. INTRODUCTION

Invariance is an important concept for ensuring robustness and safety of control systems. For a dynamical system, a set is (*forward*) *invariant* if every trajectory starting in that set remains in the set for all time. For control systems, this notion can be generalized with the determination of a control input which is able to render a set invariant, leading to the notion of a *controlled invariant set* (CIS). For systems which are subject to uncertainty or noise, the concept of a *robust controlled invariant set* (RCIS) is critical for safety, as it guarantees invariance in the presence of disturbances.

Literature Review. Controlled invariant sets have been thoroughly studied for linear systems, e.g., [1]–[4]. Many of these methods employ iterative procedures based on a one-step backward operator [1], [2] to find backward reachable sets of the system for computing the CIS with high precision. In order to improve the computation time for high-dimensional systems, other non-iterative techniques have also been proposed which rely on lifting to a higher dimensional space to compute the CIS in closed form and projecting the resulting set to the original domain, e.g., [3], [4].

On the other hand, determining controlled invariant sets of nonlinear systems remains a significant challenge. Some works employ convex or zonotopic approximations, e.g., [5], [6], in order to reduce the computational complexity. However, as the maximal controlled invariant sets are nonconvex in general, these methods can be overly conservative.

S. Brown, M. Khajenejad and S. Martínez are with the Mechanical and Aerospace Engineering Department, University of California San Diego, San Diego, CA, USA. ({sab007, mkhajenejad, soniamd}@ucsd.edu)

S. Z. Yong is with the Mechanical and Industrial Engineering Department, Northeastern University, Boston, MA, USA. (s.yong@northeastern.edu)

This work is partially supported by NSF grants 2003517,3 and CNS-2313814.

Another related work pertains to the study of invariant sets of *switched* systems, e.g., [7]–[9], where the input controls switching between a finite number of modes. In that case, the input is easily determined by considering all possible modes and selecting those which lead to invariance [8]. By sampling a continuous set of inputs, these methods can be applied to more general nonlinear systems, but the accuracy and scalability may be limited [9]. These methods result in sets that are guaranteed to be invariant, but the sampling is an additional source of computational complexity as it must be fine enough to properly capture the nonlinear behavior of the system. As a result, these methods are difficult to apply to systems with multiple inputs.

Contributions. In this paper, we propose two iterative algorithms to compute not necessarily convex inner-approximations of the maximal controlled invariant sets of control-affine systems up to a guaranteed robustness margin, *without* sampling the set of allowable inputs. These algorithms are complete, in the sense that they only return an empty set if the system does not admit a robustly controlled invariant set and always terminate in finite time. Inspired by [8], our methods use a bisection approach to under-approximate the one-step backward reachable set operator. The main idea of the approach is to compute the *forward* reachable set of the region of interest, which is described by a union of intervals. The parts of this forward set that are entirely contained in the original set are used as an under-approximation of the backward reachable set. To check the containment, we use polyhedral over-approximations of forward reachable sets, which allows us to cast the problem of determining the control input as a translation of a polyhedron. This technique allows us to determine a *continuous*, rather than sampled, set of invariance enforcing control inputs. In addition, we leverage the structure of set unions in an alternative algorithm, which has the potential to significantly reduce the total number of inclusion checking operations required, when compared with existing methods.

A. Notation

Let $\mathbb{Z}_{\geq 0}$ be the set of nonnegative integers, while \mathbb{R}^n and $\mathbb{R}^{n \times p}$ are the n -dimensional Euclidean space and the set of $n \times p$ matrices, respectively. By means of \mathcal{B}_r , we denote the ∞ -norm hyperball of radius r . We make use of $\mathbb{I}\mathbb{R}^n$ to denote the collection of (multidimensional) intervals of \mathbb{R}^n , and denote its elements as $[x] \triangleq [\underline{x}, \bar{x}] \in \mathbb{I}\mathbb{R}^n$ with lower and upper bounds \underline{x} and \bar{x} . The function $w([x])$ measures interval width (i.e., $w([x]) = \|\bar{x} - \underline{x}\|$ with any vector norm $\|\cdot\|$), $\text{mid}([x])$ selects the midpoint of $[x]$ (i.e., $\text{mid}([x]) = \frac{1}{2}(\bar{x} + \underline{x})$), and a function in brackets $[f]([x])$ represents an

interval inclusion function (cf. Definition 1). The operator \oplus denotes the Minkowski sum of two sets, i.e., $A \oplus B \triangleq \{a + b : a \in A, b \in B\}$, and \ominus denotes the Pontryagin difference, i.e., $A \ominus B \triangleq \{a : \{a\} \oplus B \subseteq A\}$. The usual set difference is denoted as $A \setminus B \triangleq \{a \in A : a \notin B\}$. For a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ and a set $S \subset \mathbb{R}^n$, $f(S)$ denotes the image of S under f . For a bounded polyhedron (polytope) \mathcal{P} , we use $H_{\mathcal{P}}$ and $b_{\mathcal{P}}$ to denote the components defining the halfspace representation $\mathcal{P} = \{x : H_{\mathcal{P}}x \leq b_{\mathcal{P}}\}$. The symbol $V_{\mathcal{P}}$ denotes the vertices of \mathcal{P} . Finally, $\text{conv } \mathcal{X}$ denotes the convex hull of the set \mathcal{X} .

II. PRELIMINARIES

This section introduces preliminary notions that will be used throughout the paper. We begin by defining inclusion functions, which are critical for tractably approximating the images of sets under nonlinear functions.

Definition 1. Given a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$, an inclusion function is an interval function $[f] : \mathbb{R}^n \rightarrow \mathbb{R}^m$ that satisfies

$$[f]([x]) \supseteq f([x]), \quad \forall [x] \in \mathbb{R}^n,$$

where $f([x])$ denotes the exact image of $[x]$ under f .

The reader is referred to [10, Section 2.4] and [11] for a thorough discussion of different types of inclusion functions, such as natural, centered, etc., as well as mixed-monotone decomposition-based inclusion functions. The results of this paper are not specific to any one type of inclusion function, but different choices will affect the precision of the result.

A. Translating Polytopes

This section defines two different operations on polytopes: translating one into another, and translating one so it intersects another. These will be used in our algorithm to determine safe control inputs.

Definition 2. Given two sets \mathcal{P} and \mathcal{Q} , the set of translations of \mathcal{P} that insert \mathcal{P} into \mathcal{Q} is denoted by

$$\mathcal{I}(\mathcal{P}, \mathcal{Q}) \triangleq \{r \in \mathbb{R}^n : \mathcal{P} \oplus \{r\} \subseteq \mathcal{Q}\} = \mathcal{Q} \ominus \mathcal{P}.$$

Similarly, the set of translations of \mathcal{P} that overlap \mathcal{P} with \mathcal{Q} is defined as

$$\mathcal{O}(\mathcal{P}, \mathcal{Q}) \triangleq \{s \in \mathbb{R}^n : \mathcal{P} \oplus \{s\} \cap \mathcal{Q} \neq \emptyset\}.$$

From the definition it is clear that for a set $\mathcal{Q} = \bigcup_{i=1}^N \mathcal{Q}_i$, $\mathcal{O}(\mathcal{P}, \mathcal{Q}) = \bigcup_{i=1}^N \mathcal{O}(\mathcal{P}, \mathcal{Q}_i)$. We now describe how to compute these operations when \mathcal{P} and \mathcal{Q} are polytopes.

Proposition 1 ([12, Theorem 2.3]). For polytopes \mathcal{P} and \mathcal{Q} ,

$$\mathcal{I}(\mathcal{P}, \mathcal{Q}) = \{r \in \mathbb{R}^n : H_{\mathcal{Q}}r \leq b_{\mathcal{Q}} - \beta\},$$

where $\beta_i = \max_{v \in V_{\mathcal{P}}} (H_{\mathcal{Q}})_i v$. If \mathcal{P} cannot be embedded into \mathcal{Q} , then this results in $\mathcal{I}(\mathcal{P}, \mathcal{Q}) = \emptyset$.

Proposition 2. Given two polytopes \mathcal{P} and \mathcal{Q} ,

$$\mathcal{O}(\mathcal{P}, \mathcal{Q}) = \left\{ s \in \mathbb{R}^n : \begin{bmatrix} H_{\mathcal{Q}} \\ -H_{\mathcal{P}} \end{bmatrix} s \leq \begin{bmatrix} b_{\mathcal{Q}} - \alpha \\ b_{\mathcal{P}} - \gamma \end{bmatrix} \right\},$$

where $\alpha_i = \min_{v \in V_{\mathcal{P}}} (H_{\mathcal{Q}})_i v$ and $\gamma_i = \min_{v \in V_{\mathcal{Q}}} (H_{\mathcal{P}})_i v$.

Proof. See Appendix A. ■

III. INVARIANCE CONTROL PROBLEM

Here we introduce the class of systems under consideration and define the concept of controlled invariance. Specifically, we consider nonlinear control affine systems of the form

$$x_{k+1} = f(x_k, u_k) \triangleq f_0(x_k) + \sum_{i=1}^m g_i(x_k) u_{i,k}, \quad (1)$$

where $x \in \mathbb{R}^n$ is the state and $u \in \mathcal{U} \subset \mathbb{R}^m$ is the input. We assume that \mathcal{U} is a compact interval, and we will restrict our attention to a region of interest, $\Omega \subset \mathbb{R}^n$, which we assume to be given as a finite union of compact intervals.

Assumption 1. The functions f_0 , and g_1, \dots, g_m are Lipschitz continuous, i.e., for every $x, y \in \Omega$,

$$\begin{aligned} \forall i \in \{1, \dots, m\}, \quad \exists L_i \text{ s.t. } \|g_i(x) - g_i(y)\| &\leq L_i \|x - y\|, \\ \text{and } L_0 \text{ s.t. } \|f_0(x) - f_0(y)\| &\leq L_0 \|x - y\|. \end{aligned}$$

Next we define the precise notions of invariance which we will consider in this work.

Definition 3 (Controlled Invariant). A set $\mathcal{X} \subset \mathbb{R}^n$ is controlled invariant with respect to the dynamics (1) if for every $x_0 \in \mathcal{X}$, there exists an input u such that $f(x_0, u) \in \mathcal{X}$.

There are many computational challenges associated with computing controlled invariant sets, many of which arise due to the infinite precision required to adequately handle regions near the boundary of the set. As such, it is convenient to modify the definition to incorporate a robustness margin r .

Definition 4 (Robustly Controlled Invariant). A set $\mathcal{X} \subset \mathbb{R}^n$ is r -robustly controlled invariant for system (1) if for every $x_0 \in \mathcal{X}$, there exists a non-empty corresponding set of control inputs $\mathcal{U}_I(x_0)$ such that for any input $u \in \mathcal{U}_I(x_0)$, $f(x_0, u) \in \mathcal{X} \ominus \mathcal{B}_r$.

Intuitively, in order to be robustly invariant, every point must be mapped into the interior of the set, at some distance r from the boundary. See [8] for more details.

We are ready to formally state the problem which we aim to address in this paper.

Problem 1. For a system (1) that satisfies Assumption 1 and a region of interest $\Omega \subset \mathbb{R}^n$, given by a union of compact intervals, compute the maximal controlled invariant set contained in Ω up to a guaranteed robustness margin. Additionally, compute the corresponding set of control inputs that enforces this invariance.

IV. COMPUTATION OF CONTROLLED INVARIANT SETS

This section starts by reviewing a well-known iterative procedure for computing maximal controlled invariant sets [13]. After this, we describe our main contribution, which under-approximates the operator used in each iteration.

Definition 5 (Pre-Set). *The pre-set, or the one-step backward reachable set of a set $\Omega \subset \mathbb{R}^n$ is defined as*

$$Q(\Omega) \triangleq \{x \in \mathbb{R}^n : \exists u \in \mathcal{U} \text{ s.t. } f(x, u) \in \Omega\}.$$

We further define the operator

$$I(\Omega) \triangleq Q(\Omega) \cap \Omega,$$

which will enable computation of the maximal controlled invariant set. Repeated application is denoted as $I^i(\Omega) = I(I^{i-1}(\Omega))$, $i \in \mathbb{Z}_{\geq 0}$, with $I^0(\Omega) = \Omega$. We also define $I_r(\Omega) \triangleq Q(\Omega \ominus \mathcal{B}_r) \cap \Omega$.

Lemma 1 ([13, Special Case of Proposition 4]). *If $\Omega \subset \mathbb{R}^n$ is closed, then*

$$I^\infty \triangleq \lim_{i \rightarrow \infty} I^i(\Omega)$$

is the maximal controlled invariant set contained in Ω .

This result is the basis for many iterative algorithms, e.g., [1], [2], [13]. However, there are several computational challenges when dealing with nonlinear systems. In addition to operations involving *backward* reachability, our algorithm also utilizes operations related to *forward* reachability, which we define here.

Definition 6 (Reachable Set). *The one-step forward reachable set of a set $\Omega \subset \mathbb{R}^n$ is defined as*

$$P(\Omega) \triangleq \{x \in \mathbb{R}^n : \exists x_0 \in \Omega, u \in \mathcal{U} \text{ s.t. } x = f(x_0, u)\}.$$

The following definition restricts the previous reachable set to that of a particular input, which is used later for determining a suitable controller.

Definition 7 (Fixed-Control Reachable Set). *For a given $u \in \mathcal{U}$, the fixed-control one-step forward reachable set of a set $\Omega \subset \mathbb{R}^n$ is defined as*

$$P_u(\Omega) \triangleq \{x \in \mathbb{R}^n : \exists x_0 \in \Omega \text{ s.t. } x = f(x_0, u)\}.$$

From the definitions, it is clear that $\bigcup_{u \in \mathcal{U}} P_u(\Omega) = P(\Omega)$.

A. Polyhedral Approximation of Reachable Sets

Our algorithm will employ polyhedral over-approximations of $P(\Omega)$ and $P_u(\Omega)$ to determine feasible control inputs that can lead to invariance.

To this end, we use a decomposition of the function f_0 , which we will show to satisfy certain properties. This decomposition will vary depending on the interval $[x]$ under consideration. We first compute A and ϕ such that

$$f_0(x) = Ax + \phi(x), \quad \forall x \in [x], \quad (2)$$

decomposing f_0 into a linear term plus a nonlinear remainder term. This is always possible (since we can let $A = 0$) and can be done in multiple different ways. For example, if f_0 is differentiable, this can be done via linearization about the midpoint of the interval. Another possibility is that f_0 has a bounded Jacobian matrix on $[x]$, in which case we can apply a Jacobian sign-stable decomposition [14, Proposition 2] to compute (2). The method of decomposition will affect the

accuracy of the final approximation, as we will discuss at the end of this section. Then, by using an inclusion function $[\Phi] : \mathbb{R}^n \rightarrow \mathbb{R}^n$ satisfying $[\Phi]([x]) \supseteq \phi([x])$, we can guarantee that

$$f_0([x]) \subseteq A[x] \oplus [\Phi]([x]), \quad (3)$$

where $A[x]$ denotes the exact (polytopic) image of $[x]$ under the linear map A .

We also decompose the individual input functions g_i . For an inclusion function $[g_i]$, let $s_i = \text{mid}([g_i]([x]))$ and $[\Psi_i]([x]) = [g_i]([x]) \ominus \{s_i\}$, so that

$$g_i([x]) \subseteq \{s_i\} \oplus [\Psi_i]([x]), \quad (4)$$

and $[\Psi_i]([x])$ is centered at the origin. A centered $[\Psi_i]([x])$ will result in a better approximation later on. We will use the notation $S \in \mathbb{R}^{n \times m}$ and $[\Psi] : \mathbb{R}^n \rightarrow \mathbb{R}^{n \times m}$ to denote the matrices with columns s_i and $[\Psi_i]$, respectively.

In order to guarantee the accuracy of the algorithm, we must first compute bounds on the error of these over-approximations. Assumption 1 allows us to upper bound the width of the resulting inclusion functions.

Proposition 3. *Under Assumption 1, there exist inclusion functions $[\Phi]$ and $[\Psi_i]$, $i \in \{1, \dots, m\}$, and constants $\tilde{L}_i > 0$, $i \in \{0, \dots, m\}$ so that for every interval $[x] \subseteq \Omega$,*

$$w([\Phi]([x])) \leq \tilde{L}_0 w([x]) \quad \text{and} \quad w([\Psi_i]([x])) \leq \tilde{L}_i w([x]).$$

Proof. We can, for example, use inclusion functions based on mixed-monotone decompositions (cf. [15, Lemma 1]) or the mean-value form (cf. [10] and [8, Eq. (3)]) that can be shown to satisfy these bounds. ■

With these decompositions in mind, we can define our approximations of the forward reachable sets. Let

$$\bar{P}([x]) \triangleq A[x] \oplus [\Phi]([x]) \oplus S\mathcal{U} \oplus [\Psi]([x])\mathcal{U}$$

be the polyhedral over-approximation of the one-step forward reachable set, and let

$$\bar{P}_u([x]) \triangleq A[x] \oplus [\Phi]([x]) \oplus Su \oplus [\Psi]([x])\mathcal{U} \quad (5)$$

be the polyhedral over-approximation of the fixed-control reachable set. The expression $S\mathcal{U}$ denotes the polytopic image of \mathcal{U} under the linear transformation S , and $[\Psi]([x])\mathcal{U}$ denotes the interval-valued product that can be computed using interval arithmetic. The over-approximation $[\Psi]([x])\mathcal{U}$ is used rather than $[\Psi]([x])u$ so that u appears linearly in (5) with a constant coefficient S . This introduces some conservatism, as seen in the following lemma.

Lemma 2. *Let $\rho \triangleq \tilde{L}_0 + \max_{1 \leq i \leq m} \tilde{L}_i w(\mathcal{U}_i)$. Then for all intervals $[x] \subset \Omega$, the following inclusions hold:*

$$P_u([x]) \subseteq \bar{P}_u([x]) \subseteq P_u([x]) \oplus \mathcal{B}_{\rho w([x])},$$

$$P([x]) \subseteq \bar{P}([x]) \subseteq P([x]) \oplus \mathcal{B}_{\rho w([x])}.$$

Proof. The inclusion $P_u([x]) \subseteq \bar{P}_u([x])$ is guaranteed by construction, since

$$P_u([x]) = A[x] \oplus \phi([x]) \oplus Su \oplus \sum_{i=1}^m \hat{g}_i([x])u_i,$$

$\phi([x]) \subseteq [\Phi]([x])$, and $\hat{g}_i([x]) \subseteq [\Psi_i]([x])$ where $\hat{g}_i \triangleq g_i - s_i$. The inclusion $P_u([x]) \subseteq P_u([x]) \oplus \mathcal{B}_{\rho w}([x])$ follows from Proposition 3 and the definition of the Minkowski sum. The second statement is proved in the same way. ■

B. Interval Approximation of Pre-Sets

We describe our main contribution next, which is a novel algorithm for approximating the operator I for systems of the form (1). Given a union of compact intervals Ω , we propose an iterative refinement procedure that approximates $I(\Omega)$ by another union of compact intervals. Algorithm 1 summarizes the main steps of this process, described in detail next.

Algorithm 1 $I(\Omega)$

Require: Ω, ε

```

1:  $q \leftarrow \{\Omega\}, \mathcal{N} \leftarrow \emptyset, \underline{I} \leftarrow \emptyset, \mathcal{E} \leftarrow \emptyset, \mathcal{U}_I \leftarrow \emptyset$ 
2: while  $q \neq \emptyset$  do
3:    $[x] \leftarrow \text{pop\_front}(q)$ 
4:   Compute  $A, \Phi, s_i$ , and  $\Psi_i$  on  $[x]$ 
5:   if  $\bar{P}([x]) \cap \Omega = \emptyset$  then
6:      $\mathcal{N} \leftarrow \mathcal{N} \cup [x]$ 
7:   else if  $\exists u \in \mathcal{U}$  s.t.  $\bar{P}_u([x]) \subseteq \Omega$  then
8:      $\underline{I} \leftarrow \underline{I} \cup [x]$ 
9:      $\mathcal{U}_I \leftarrow \mathcal{U}_I \cup ([x], S^\dagger(SU([x])))$  ▷ See Lemma 3
10:  else if  $w([x]) \leq \varepsilon$  then
11:     $\mathcal{E} \leftarrow \mathcal{E} \cup [x]$ 
12:  else
13:     $(l, r) \leftarrow \text{bisect}([x])$ 
14:     $\text{push\_back}(q, l), \text{push\_back}(q, r)$ 
15:  end if
16: end while
17: return  $\underline{I}, \mathcal{U}_I$ 

```

The algorithm is a loop that operates on a queue (q) of intervals. An element of the queue is retrieved (and removed) from the front of the queue using the `pop_front` operation, while an element is added to the back of the queue using the `push_back` operation. The following steps are implemented until the queue is empty. We perform an inclusion check on every interval $[x]$, to see whether it may be included as part of the pre-set of Ω . Two tests are performed:

- 1) Is the forward reachable set from $[x]$ disjoint with Ω ? If so, $[x]$ is disjoint from $I(\Omega)$.
- 2) Can an input u be found so that the reachable set from $[x]$, restricted to the input u , lies entirely within Ω ? If so, $[x] \subset I(\Omega)$.

If either condition is satisfied, then the set $[x]$ is saved in lists labeled \mathcal{N} (the collection of intervals disjoint with $I(\Omega)$) and \mathcal{S} (the collection of intervals contained in $I(\Omega)$).

If neither condition is satisfied and the $[x]$ is wider than the specified tolerance, it is bisected along its largest dimension and both resulting intervals are added to the back of the queue using the `push_back` operation. Otherwise, $[x]$ is added to \mathcal{E} , which is a collection of the “indeterminate” sets, which are neither disjoint from nor subsets of $I(\Omega)$.

Line 7 of Algorithm 1 requires checking the condition

$$\exists u \in \mathcal{U} \text{ s.t. } \bar{P}_u([x]) \subseteq \Omega, \quad (6)$$

which is a nonconvex feasibility problem, due to the non-convexity of Ω . Luckily, we can exploit the structure of both $\bar{P}_u([x])$ and Ω in order to efficiently and precisely compute the set of u that satisfy (6). Notice that, in the definition of \bar{P}_u , the term $A[x] \oplus [\Phi]([x]) \oplus [\Psi]([x])\mathcal{U}$ is a convex polyhedron, and the additive term Su serves only to *translate* the resulting polyhedron. On the other hand, Ω is a union of intervals, and also more generally a union of polyhedra. Therefore, we can reduce the feasibility problem in (6) to a problem of translating a polyhedron into a union of polyhedra. We describe here an equivalence which helps solve this problem, inspired by [16].

Lemma 3. Let $\mathcal{P} = \text{conv}(\Omega \cap \bar{P}([x]))$ and $\mathcal{Q} = \mathcal{P} \setminus (\Omega \cap \bar{P}([x]))$. Then, the following statements are equivalent:

- 1) $\exists u \in \mathcal{U}$ such that $\bar{P}_u([x]) \subseteq \Omega$;
- 2) $SU([x]) \triangleq \mathcal{I}(\bar{P}_0([x]), \mathcal{P}) \setminus \mathcal{O}(\bar{P}_0([x]), \mathcal{Q}) \neq \emptyset$.

where $\bar{P}_0([x])$ is $\bar{P}_u([x])$ with $u = 0$.

Proof. From $\bar{P}_0([x]) = A[x] \oplus [\Phi]([x]) \oplus [\Psi]([x])\mathcal{U}$, we obtain that for any u , $\bar{P}_u([x]) = \bar{P}_0([x]) \oplus \{Su\}$. Furthermore, $\bar{P}([x]) = \bar{P}_0([x]) \oplus SU$. This gives rise to the equivalence

$$\begin{aligned} \exists u \in \mathcal{U} \text{ s.t. } \bar{P}_u([x]) \subseteq \Omega \\ \iff \exists r \in \mathbb{R}^n \text{ s.t. } \bar{P}_0([x]) \oplus \{r\} \subseteq \Omega \cap \bar{P}([x]), \end{aligned}$$

where it must be true that $r = Su$. We see that by intersecting Ω with $\bar{P}([x])$ on the right hand side, we can identify a translation by a vector r , which is automatically restricted to the range of S . To find the r in the latter expression, we first find the translations into the *convex hull* of $\Omega \cap \bar{P}([x])$ (i.e., $\mathcal{I}(\bar{P}_0([x]), \mathcal{P})$), then remove the translations that cause overlap with parts of the convex hull that are not in the original set (i.e., $\mathcal{O}(\bar{P}_0([x]), \mathcal{Q})$). This gives the set of translations r that result in containment in $\Omega \cap \bar{P}([x])$, therefore yielding the expression for $SU([x])$. ■

Since \mathcal{Q} is the difference between a polytope and a union of polytopes, its closure can be expressed as the union of a finite number of polytopes [17]. This means that the closures of $\mathcal{O}(\bar{P}_0([x]), \mathcal{Q})$ and $SU([x])$ can also be expressed as unions of a finite number of polytopes. The equivalence in Lemma 3 provides a tractable method of solving the feasibility problem in (6), using procedures to efficiently compute \mathcal{I} and \mathcal{O} . Finally, since $\forall r \in SU([x]), \exists u \in \mathcal{U}$ such that $r = Su$, we can recover the set of inputs with the Moore-Penrose pseudoinverse, $\mathcal{U}([x]) = S^\dagger(SU([x]))$, which is stored/saved in \mathcal{U}_I as pairs $([x], \mathcal{U}([x]))$.

Remark 1. The computation of the set difference between two polyhedra can be represented as a union of (not necessarily closed) polyhedra. This procedure is computationally expensive, especially when considering the difference between a polyhedron and a union of polyhedra, for which the best algorithms [17] have exponential complexity. In fact,

the computation of set differences is the largest computational burden of our method. Caching results from previous iterations can reduce the amount of computation required, but these details are omitted for the sake of brevity. •

We finish this section by proving that Algorithm 1 returns a useful approximation of $I(\Omega)$, which is within some known bound of the maximal CIS.

Lemma 4. *Let Ω be a finite union of compact intervals. Then, for any precision $\varepsilon > 0$, Algorithm 1 terminates in a finite number of iterations. Furthermore, letting $\underline{I}(\Omega)$ denote the output of Algorithm 1 and $r = \rho\varepsilon$, it holds that*

$$I(\Omega \ominus \mathcal{B}_r) \subseteq I_r(\Omega) \subseteq \underline{I}(\Omega) \subseteq I(\Omega). \quad (7)$$

Proof. The proof is similar to [8, Lemma 1], relying on the bounds provided by Lemma 2. ■

C. Near-Maximal Controlled Invariant Sets

With the ability to compute $\underline{I}(\Omega)$ using Algorithm 1, all that remains is to repeat this operation until convergence is achieved. Algorithm 2 describes this simple procedure, which is guaranteed to terminate in finite time.

Algorithm 2 Approximation of $I^\infty(\Omega)$

Require: Ω, ε

```

1:  $I_0 \leftarrow \Omega, I_1 \leftarrow \emptyset$ 
2: while  $I_0 \neq I_1$  do
3:    $I_1 \leftarrow I_0$ 
4:    $I_0 \leftarrow \underline{I}(I_0)$  ▷ via Algorithm 1
5: end while
6: return  $I_0$ 
```

Theorem 1. *For any finite union of compact intervals Ω and precision $\varepsilon > 0$, Algorithm 2 terminates in a finite number of iterations. Furthermore, denoting the output of the algorithm as $\underline{I}^\infty(\Omega)$, the following inclusions hold:*

$$I_r^\infty(\Omega) \subseteq \underline{I}^\infty(\Omega) \subseteq I^\infty(\Omega),$$

where $r = \rho\varepsilon$. Finally, $\underline{I}^\infty(\Omega)$ is controlled invariant.

Note that it is possible for the algorithm to return an empty set only if the system does not admit an r -robustly controlled invariant set, meaning $I_r^\infty = \emptyset$.

Proof. Let $\underline{I}^k(\Omega)$ denote the value of $\underline{I}(\underline{I}^{k-1}(\Omega))$ in the k -th iteration, with $\underline{I}^0(\Omega) = \Omega$. Since the algorithm terminates if $\underline{I}^{k-1}(\Omega) = \underline{I}^k(\Omega)$, we only need to consider the case when they are not equal. In this case, the structure of Algorithm 1 is such that $\underline{I}^k(\Omega) \subsetneq \underline{I}^{k-1}(\Omega)$. Since Ω is compact, $\underline{I}^k(\Omega)$ contains only a finite number of intervals which will be considered using the bisection method for a given ε . Then $\exists K \geq 0$ such that $\underline{I}^k(\Omega) = \emptyset, \forall k \geq K$, meaning the algorithm terminates in finite time.

To prove the inclusions, note that by Lemma 4, $I_r(\Omega) \subseteq \underline{I}(\Omega) \subseteq I(\Omega)$. Also, for any two sets $A \subseteq B \subseteq \mathbb{R}^n$, we know that $\underline{I}(A) \subseteq \underline{I}(B)$ and $I_r(A) \subseteq I_r(B)$. Therefore

by applying Lemma 4 and induction, we can determine that $I_r^k(\Omega) \subseteq \underline{I}^k(\Omega) \subseteq I^k(\Omega)$ for all $k \geq 0$.

Finally, to prove invariance of $\underline{I}^\infty(\Omega)$, note that by Lemma 4, $\underline{I}^\infty(\Omega) = \underline{I}(\underline{I}^\infty(\Omega)) \subseteq \underline{I}(\underline{I}^\infty(\Omega))$. ■

Remark 2 (An Outside-In Approach). The method described in this paper is commonly known as an *outside-in* method, since we start with a region of interest Ω and search for the largest invariant set $\mathcal{X} = I^\infty(\Omega)$ which it contains. It is also possible to use an *inside-out* approach, which starts with a known invariant set, and iteratively grows that set [9]. Our method can be easily adapted for this case, as well. •

To conclude this section, we state a result that has the potential to reduce the number of inclusion checking operations required by Algorithm 2. Let $\{\Omega_i\}_{i=1}^N$ be any ordered collection of sets such that $\Omega = \bigcup_{i=1}^N \Omega_i$. Define the operator

$$I_i(\Omega) \triangleq \bigcup_{j \neq i} \Omega_j \cup (Q(\Omega) \cap \Omega_i),$$

and let $I_{1:N} \triangleq I_N(\dots(I_1(\Omega)))$. We let the I_i operator preserve the order of the constituent subsets by defining

$$(I_i(\Omega))_i = Q(\Omega) \cap \Omega_i \quad \text{and} \quad (I_i(\Omega))_j = \Omega_j, \quad j \neq i.$$

Theorem 2. *For a closed set $\Omega \subseteq \mathbb{R}^n$, $I_{1:N}$ satisfies*

$$I_{1:N}(\Omega) \subseteq I(\Omega), \quad \text{and} \quad \lim_{k \rightarrow \infty} (I_{1:N})^k(\Omega) = \lim_{k \rightarrow \infty} I^k(\Omega) = I^\infty(\Omega). \quad (8)$$

Proof. By definition, for any $i \neq j$,

$$\begin{aligned} I_i(I_j(\Omega)) &= \bigcup_{\ell \neq i} I_j(\Omega)_\ell \cup (Q(I_j(\Omega)) \cap I_j(\Omega)_i) \\ &= \bigcup_{\ell \neq i, \ell \neq j} \Omega_\ell \cup (Q(\Omega) \cap \Omega_j) \cup (Q(I_j(\Omega)) \cap I_j(\Omega)_i) \\ &\subseteq \bigcup_{\ell \neq i, \ell \neq j} \Omega_\ell \cup (Q(\Omega) \cap (\Omega_i \cup \Omega_j)), \end{aligned}$$

since $I_j(\Omega)_i \subseteq \Omega_i$ and $Q(I_j(\Omega)) \cap I_j(\Omega)_i \subseteq Q(\Omega) \cap \Omega_i$. By applying this statement recursively, we arrive at

$$I_{1:N}(\Omega) \subseteq \bigcup_{i=1}^N \Omega_i \cap Q(\Omega) = I(\Omega). \quad (9)$$

In (8), since $I_{1:N}$ is monotonically decreasing and closed, the limit exists. We will show by induction that for all $k \geq 0$, $(I_{1:N})^k(\Omega) \supseteq I^\infty(\Omega)$. Consider a point $x \in I^\infty(\Omega)$. We know $x \in Q(I^\infty(\Omega)) \subseteq Q(\Omega)$. Therefore, by the definition of I_1 , $x \in I_1(\Omega)$, meaning $I_1(\Omega) \supseteq I^\infty(\Omega)$. By repeating this reasoning for I_2, \dots, I_N , we can see that $I_{1:N}(\Omega) \supseteq I^\infty(\Omega)$. For the step case, assume that $(I_{1:N})^{k-1}(\Omega) \supseteq I^\infty(\Omega)$. Then by the same argument as the base case, for any $x \in I^\infty(\Omega)$, $x \in Q(I^\infty(\Omega)) \subseteq Q((I_{1:N})^{k-1}(\Omega))$, implying $(I_{1:N})^k(\Omega) \supseteq I^\infty(\Omega)$. Using this fact in combination with (9), monotonicity of I and $I_{1:N}$, as well as an induction argument proves (8). ■

Theorem 2 is useful because it allows us to independently consider individual regions of the invariant set, rather than

approximating the I operator all at once. Inspired by this, we propose Algorithm 3, a modified procedure that considers only one interval at a time (as opposed to Algorithm 2, which iterates over the whole set before returning the updated approximation). In the algorithm, Ω is updated whenever an interval is determined to not be a part of the invariant set. The loop terminates if every interval in the queue has been checked since Ω was last changed, meaning every interval in the queue is contained in the invariant set. The set \mathcal{C} contains all intervals $[x]$ which have been checked against the current Ω . Whenever Ω changes, \mathcal{C} is reset to the empty set. Note that `push_front` places newly bisected intervals in the front of the queue. The following theorem formalizes the convergence of Algorithm 3 and its relationship to Algorithm 2.

Algorithm 3 Alternative Approximation of $I^\infty(\Omega)$

Require: Ω, ε

```

1:  $q \leftarrow \{\Omega\}, \mathcal{C} \leftarrow \emptyset, \mathcal{N} \leftarrow \emptyset, \underline{I} \leftarrow \emptyset, \mathcal{E} \leftarrow \emptyset, \mathcal{U}_I \leftarrow \emptyset$ 
2: while  $\mathcal{C} \neq \Omega$  do
3:    $[x] \leftarrow \text{pop\_front}(q)$ 
4:    $\mathcal{C} \leftarrow \mathcal{C} \cup [x]$ 
5:   Compute  $A, \Phi, s_i$ , and  $\Psi_i$  on  $[x]$ 
6:   if  $\bar{P}([x]) \cap \Omega = \emptyset$  then
7:      $\mathcal{N} \leftarrow \mathcal{N} \cup [x]$ 
8:      $\Omega \leftarrow \Omega \setminus [x], \mathcal{C} \leftarrow \emptyset$ 
9:   else if  $\exists u \in \mathcal{U}$  s.t.  $\bar{P}_u([x]) \subseteq \Omega$  then
10:     $\text{push\_back}(q, [x])$ 
11:     $\mathcal{U}_I \leftarrow \mathcal{U}_I \cup ([x], S^\dagger(S\mathcal{U}([x])))$ 
12:   else if  $w([x]) \leq \varepsilon$  then
13:      $\mathcal{E} \leftarrow \mathcal{E} \cup [x]$ 
14:      $\Omega \leftarrow \Omega \setminus [x], \mathcal{C} \leftarrow \emptyset$ 
15:   else
16:      $(l, r) \leftarrow \text{bisect}([x])$ 
17:      $\text{push\_front}(q, l), \text{push\_front}(q, r)$ 
18:   end if
19: end while
20:  $\underline{I}^\infty \leftarrow \bigcup_{[x] \in q} [x]$ 
21: return  $\underline{I}^\infty, \mathcal{U}_I$ 

```

Theorem 3. For any finite union of compact intervals Ω and precision $\varepsilon > 0$, Algorithm 3 terminates in a finite number of iterations and returns the same result as Algorithm 2.

Proof. Similar to the proof of Theorem 1. ■

By comparing the steps of each algorithm, one can see that the number of inclusion checks required by Algorithm 3 should be less than or equal to that of Algorithms 1 and 2. This is because Algorithm 3 updates Ω every time an interval $[x]$ is identified as not belonging to the invariant set. On the other hand, Algorithm 2 checks every $[x]$ against a fixed Ω , which is only updated in the outer loop of Algorithm 1. A formal comparison is the topic of future work.

V. EXAMPLE AND COMPARISON

In this section, we demonstrate the effectiveness of our approach on a numerical example, namely, an inverted pen-

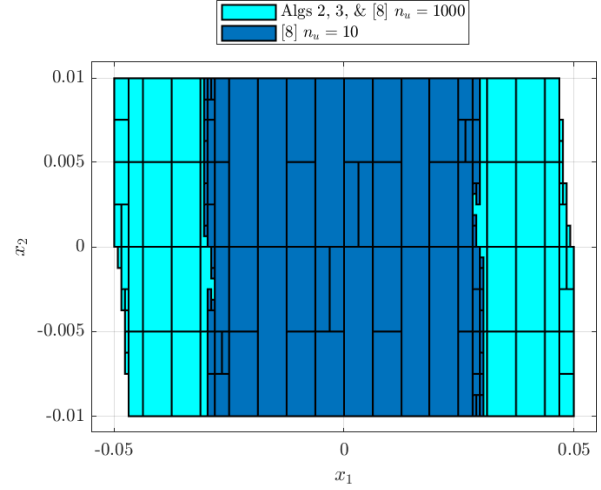


Fig. 1: Controlled invariant sets of the inverted pendulum system.

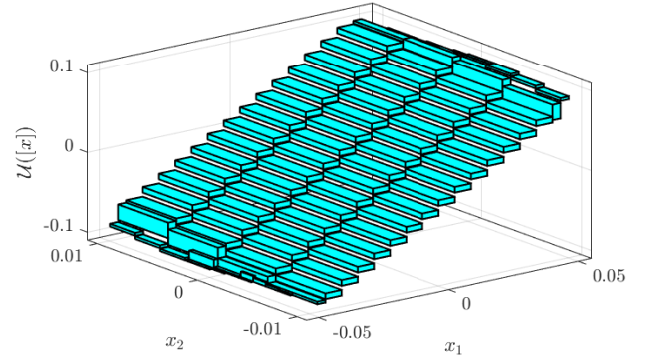


Fig. 2: Invariance-enforcing inputs $\mathcal{U}([x])$ identified by Lemma 3.

dulum on a cart. We also compare our approach to the method for switched systems in [8], where the input space is sampled and considered as controlled modes.

As in [8], we consider an inverted pendulum on a cart, discretized using forward Euler with a sampling time of 0.01s. The dynamics are

$$\dot{x}_1 = x_2, \quad \dot{x}_2 = \frac{mgl}{J} \sin(x_1) - \frac{b}{J} x_2 + \frac{l}{J} \cos(x_1) u,$$

with parameters $m = 0.2$ kg, $g = 9.8$ m/s², $l = 0.3$ m, $J = 0.006$ kg · m², and $b = 0.1$ N/m/s. This system and its discretization are control-affine. We consider a region of interest $\Omega = [-0.05, -0.05] \times [-0.01, 0.01]$ and an input set $\mathcal{U} = [-0.1, 0.1]$. The natural inclusion function is used.

Figure 1 shows the identified controlled invariant sets for our approaches, i.e., using Algorithms 2 and 3, and that of [8], with $n_u = 10$ and $n_u = 1000$ sampled inputs. All methods were run with a precision $\varepsilon = 0.001$. On the other hand, Figure 2 shows the union of all invariance-enforcing control inputs $\mathcal{U}([x])$ identified by Algorithms 2 and 3. Finally, Table I shows a comparison of computation times with different parameters. By “iterations”, we mean the number of times an interval is popped from the queue, which is equivalent to the number of inclusion checks.

Method	ε	Iterations	Total Time (s)	Volume
Algorithm 2	10^{-3}	703	0.54	97.9%
Algorithm 3	10^{-3}	618	0.63	97.9%
[8] ($n_u = 10$)	10^{-3}	10729	0.12	59.8%
[8] ($n_u = 1000$)	10^{-3}	485	0.59	97.9%

TABLE I: Computational comparison between Algorithm 2, Algorithm 3, and [8]. n_u denotes the number of input samples taken uniformly across \mathcal{U} . The volume is given in % of the original Ω .

Evidently, our method is able to identify a larger CIS in fewer iterations than the sampling and interval arithmetic based approach in [8], when the number of samples is small. This is presumably due to the higher accuracy of our polytopic approximations, and the fact that we consider the entire continuous range of control inputs. Increasing the number of sampled inputs results in a better approximation of the CIS, at the cost of some additional computation time. Finally, we see that although Algorithm 3 results in fewer iterations, it takes the longest. This is likely due to the cost of updating Ω more frequently.

VI. CONCLUSION

We proposed two methods for approximating controlled invariant sets of nonlinear control-affine systems using an iterative refinement approach. We used techniques from computational geometry involving translations of polyhedra to allow us to efficiently compute continuous sets of feasible control inputs, rather than using a sampling approach with switched dynamics. We demonstrated the effectiveness of our method on a numerical example, which showed improved accuracy over existing methods and led to faster convergence in some cases. In the future, we will further explore the extension of our approach to continuous time, as well as the control synthesis problem, including some notions of optimality, while also investigating ways to improve the accuracy and efficiency of our algorithms. We also will test our approaches on a wide variety of nonlinear systems.

APPENDIX

A. Proof of Proposition 2

We begin by stating two intermediate results which will be used to prove the proposition. The first allows us to determine whether two polytopes intersect by examining the hyperplanes defining each polytope.

Proposition 4. *Given two polytopes \mathcal{P} and \mathcal{Q} , $\mathcal{P} \cap \mathcal{Q} \neq \emptyset$ if and only if both of the following statements are true*

- 1) \mathcal{P} intersects every halfspace defining \mathcal{Q} , i.e., $\forall i \in \{1, \dots, N_{\mathcal{Q}}\}$, $\exists p_i \in \mathcal{P}$ such that $(H_{\mathcal{Q}})_i p_i \leq (b_{\mathcal{Q}})_i$.
- 2) \mathcal{Q} intersects every halfspace defining \mathcal{P} , i.e., $\forall i \in \{1, \dots, N_{\mathcal{P}}\}$, $\exists q_i \in \mathcal{Q}$ such that $(H_{\mathcal{P}})_i q_i \leq (b_{\mathcal{P}})_i$.

Proof. Necessity is simple, since if $\mathcal{P} \cap \mathcal{Q} \neq \emptyset$, every $v \in \mathcal{P} \cap \mathcal{Q}$ will satisfy the existence conditions in 1) and 2).

To prove sufficiency, note that $\mathcal{P} \cap \mathcal{Q} = \emptyset$ if and only if there exists a separating hyperplane, defined by some $h_* \in \mathbb{R}^n$ and $b_* \in \mathbb{R}$, such that $\forall v \in \mathcal{P}$, $h_*^\top v \leq b$ and $\forall v \in \mathcal{Q}$, $h_*^\top v > b$. Conditions 1) and 2) preclude the existence of this separating hyperplane, implying $\mathcal{P} \cap \mathcal{Q} \neq \emptyset$. ■

The second intermediate result tells us how to translate a polytope so that it intersects a given halfspace.

Proposition 5. *Given a polytope \mathcal{P} and halfspace $\mathcal{H} = \{x : h^\top x \leq b\}$, the set of translations of \mathcal{P} that intersect \mathcal{H} ; i.e., $\mathcal{O}(\mathcal{P}, \mathcal{H}) \triangleq \{s \in \mathbb{R}^n : \mathcal{P} \oplus \{s\} \cap \mathcal{H} \neq \emptyset\}$, is given by*

$$\mathcal{O}(\mathcal{P}, \mathcal{H}) = \{s \in \mathbb{R}^n : h^\top s \leq b - \alpha\},$$

where $\alpha = \min_{v \in \mathcal{V}_{\mathcal{P}}} h^\top v$.

Proof. The reasoning is similar to [12, Theorem 2.3], with min replacing max because intersection, rather than containment, is required. ■

Proposition 2 follows from the combination of Proposition 4 with repeated application of Proposition 5 to every halfspace defining both \mathcal{P} and \mathcal{Q} (with $-s$ replacing s in the second part, as the translation is applied to \mathcal{P} , not \mathcal{Q}).

REFERENCES

- [1] M. Fiacchini and M. Alamir, "Computing control invariant sets in high dimension is easy," *arXiv preprint*, 2018.
- [2] 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.
- [3] T. Anevlavis and P. Tabuada, "Computing controlled invariant sets in two moves," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 6248–6254.
- [4] T. Anevlavis, Z. Liu, N. Ozay, and P. Tabuada, "Controlled invariant sets: implicit closed-form representations and applications," *arXiv preprint arXiv:2107.08566*, 2022.
- [5] 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.
- [6] L. Schäfer, F. Gruber, and M. Althoff, "Scalable computation of robust control invariant sets of nonlinear systems," *IEEE Transactions on Automatic Control*, pp. 1–15, 2023.
- [7] S. Jang, N. Ozay, and J. L. Mathieu, "An invariant set construction method, applied to safe coordination of thermostatic loads," *arXiv preprint*, 2022.
- [8] Y. Li and J. Liu, "Invariance control synthesis for switched nonlinear systems: An interval analysis approach," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2206–2211, 2018.
- [9] J. Bravo, D. Limon, T. Alamo, and E. Camacho, "On the computation of invariant sets for constrained nonlinear systems: An interval arithmetic approach," *Automatica*, vol. 41, no. 9, pp. 1583–1589, 2005.
- [10] L. Jaulin, M. Kieffer, O. Didrit, and E. Walter, "Applied interval analysis," ed: Springer, London, 2001.
- [11] M. Khajenejad and S. Z. Yong, "Tight remainder-form decomposition functions with applications to constrained reachability and guaranteed state estimation," *IEEE Transactions on Automatic Control*, pp. 1–16, 2023.
- [12] I. Kolmanovsky and E. Gilbert, "Theory and computation of disturbance invariant sets for discrete-time linear systems," *Mathematical Problems in Engineering*, vol. 4, pp. 317–367, 01 1998.
- [13] 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.
- [14] M. Khajenejad, F. Shoaib, and S. Z. Yong, "Interval observer synthesis for locally Lipschitz nonlinear dynamical systems via mixed-monotone decompositions," in *American Control Conference (ACC)*, 2022, pp. 2970–2975.
- [15] M. Khajenejad and S. Z. Yong, "Simultaneous input and state interval observers for nonlinear systems with full-rank direct feedthrough," in *IEEE Conference on Decision and Control*, 2020, pp. 5443–5448.
- [16] B. Baker, S. Fortune, and S. Mahaney, "Polygon containment under translation," *Journal of Algorithms*, vol. 7, no. 4, pp. 532–548, 1986.
- [17] M. Baotic, "Polytopic computations in constrained optimal control," *Automatika*, vol. 50, pp. 119–134, 04 2009.