



Characterization, verification and computation of robust controlled invariants for monotone dynamical systems

Adnane Saoud^{1,2} · Murat Arcak³

Received: 15 May 2022 / Accepted: 21 August 2023

© The Author(s), under exclusive licence to Springer-Verlag London Ltd., part of Springer Nature 2023

Abstract

In this paper, we consider the problem of computing robust controlled invariants for discrete-time monotone dynamical systems. We consider different classes of monotone systems depending on whether the sets of states, control inputs and disturbances respect a given partial order. Then, we present set-based and trajectory-based characterizations of robust controlled invariants for the considered class of systems. Based on these characterizations, we propose algorithmic approaches for the verification and computation of robust controlled invariants. Finally, illustrative examples are provided showing the merits of the proposed approach.

Keywords Controlled invariance · Monotone systems · Safety

1 Introduction

The concept of controlled invariance plays an important role in control theory [1, 2], as it reflects the ability to control the system so that all trajectories initialized in a set remain there for all future time. This concept is crucial in safety-critical applications such as vehicle platoons [3–5], air traffic management [6], robotics [7, 8] and power networks [9] where formal proofs are required to show the ability to maintain the state in the safe region.

✉ Adnane Saoud
adnane.saoud@centralesupelec.fr

Murat Arcak
arcak@berkeley.edu

¹ Laboratoire des Signaux et Systèmes, CentraleSupélec, Université Paris Saclay, Gif-sur-Yvette, France

² College of Computing, Mohammed VI Polytechnical University, Benguerir, Morocco

³ Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA

Different approaches have been proposed in the literature to compute controlled invariants for different classes of discrete-time systems. In [1], controlled invariants are obtained as level sets of Lyapunov-like functions. Iterative algorithms are used to compute controlled invariants in [10] for piecewise affine systems and more recently in [11] for linear systems. Controlled invariants for polynomial systems have been explored using linear programming in [12] and semidefinite programming in [13]. For general nonlinear systems, interval controlled invariants have been investigated recently in [14]. Other approaches have been proposed recently using symbolic control techniques [15, 16].

In this paper, we study robust controlled invariants for discrete-time monotone dynamical systems. We consider different classes of monotone systems depending on whether the sets of states, control inputs and disturbance inputs respect a given partial order. Moreover, we focus on lower closed constraints. For the considered classes of systems and constraints, we present characterizations of the structure of the robust controlled invariants. Then, we present an algorithmic procedure allowing to compute robust controlled invariants using an appropriately defined concept of feasibility. Finally, we illustrate the theoretical results on an adaptive cruise control problem.

Related work The computation of controlled invariants for monotone systems has been explored for continuous time systems for the particular class of sets given by intervals. The approach in [17] deals with monotone autonomous multi-affine systems and in [18] the authors present an approach to the computation of robust controlled invariants for monotone systems with inputs. In [19], the authors use formal methods and symbolic control techniques to compute robust controlled invariants for discrete time monotone dynamical systems. The closest work to the current paper in the literature is [20] where the authors introduce a notion of s-sequence to characterize a controlled invariant for disturbance state monotone systems. Our approach generalizes the one in [20] by allowing to deal with different classes of monotone systems, by providing new characterizations of the structure of the robust controlled invariants and by using a new algorithmic procedure to compute robust controlled invariants based on tools from multi-dimensional binary search algorithms used in multi-objective optimization [21].

A preliminary version of this work is currently under review in the IEEE Conference on Decision and Control (CDC) 2022 [22]. In the current paper we are providing proofs for different results, which has not been done in the conference version. Moreover, while in [22], we are only dealing with the computation of the controlled invariants, we are also presenting here another algorithm for the verification of controlled invariants together with a new numerical example.

The remainder of this paper is organized as follows. In Sect. 3, we introduce the class of systems we consider. Section 4 introduces the concept of robust controlled invariants. In Sects. 5 and 6, we present different characterizations of robust controlled invariants. Section 7 presents algorithms to verify and compute controlled invariants. Finally, Sect. 5 presents numerical results validating the merits of the proposed approach. To improve the readability of the paper, all the proofs are given in the appendix.

Notation

The symbols \mathbb{N} , $\mathbb{N}_{>0}$, \mathbb{R} and $\mathbb{R}_{>0}$ denote the set of positive integers, non-negative integers, real and non-negative real numbers, respectively. Given $N \in \mathbb{N}_{>0}$ and a set $Y \subseteq \mathbb{R}^n$, Y^w denotes the set of infinite sequences of elements of Y . For a map $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$, $\text{dom } f := \{x \in \mathbb{R}^n : f(x) \text{ is well defined}\}$. Given a non-empty set K , $\text{Int}(K)$ denotes its interior, $\text{cl}(K)$ denotes its closure, ∂K denotes its boundary and \overline{K} its complement. For a set K , the operator $\text{Single}(K)$ randomly selects a unique element from the set K . The Euclidean norm is denoted by $\|\cdot\|$. For $x \in \mathbb{R}^n$ and for $\varepsilon > 0$, $\mathcal{B}_\varepsilon(x) = \{z \in \mathbb{R}^n \mid \|z - x\| \leq \varepsilon\}$ and for a set $K \subseteq \mathbb{R}^n$, $\mathcal{B}_\varepsilon(K) = \cup_{x \in K} \mathcal{B}_\varepsilon(x)$.

2 Preliminaries

2.1 Partial orders

A partially ordered set \mathcal{L} has an associated binary relation $\leq_{\mathcal{L}}$ where for all $l_1, l_2, l_3 \in \mathcal{L}$, the binary relation satisfies: (i) $l_1 \leq_{\mathcal{L}} l_1$, (ii) if $l_1 \leq_{\mathcal{L}} l_2$ and $l_2 \leq_{\mathcal{L}} l_1$ then $l_1 =_{\mathcal{L}} l_2$ and, (iii) if $l_1 \leq_{\mathcal{L}} l_2$ and $l_2 \leq_{\mathcal{L}} l_3$ then $l_1 \leq_{\mathcal{L}} l_3$. If neither $l_1 \leq_{\mathcal{L}} l_2$ nor $l_2 \leq_{\mathcal{L}} l_1$ holds, we say that l_1 and l_2 are incomparable. The set of all incomparable couples in \mathcal{L} is denoted by $\text{Inc}_{\mathcal{L}}$. We say that $l_1 <_{\mathcal{L}} l_2$ iff $l_1 \leq_{\mathcal{L}} l_2$ and $l_1 \neq_{\mathcal{L}} l_2$. Similarly, a partial ordering $m \leq_{\mathcal{L}^w} n$ between a pair of infinite sequences $m = m_0 m_1 \dots$ and $n = n_1 n_2 \dots$ holds if and only if $m_k \leq_{\mathcal{L}} n_k$ for all $k \in \mathbb{N}_{>0}$.

For a partially ordered set \mathcal{L} , closed intervals are $[x, y]_{\mathcal{L}} := \{z \mid x \leq_{\mathcal{L}} z \leq_{\mathcal{L}} y\}$. Given a partially ordered set \mathcal{L} , for $a \in \mathcal{L}$ let $\downarrow a := \{x \in \mathcal{L} \mid x \leq_{\mathcal{L}} a\}$ and $\uparrow a := \{x \in \mathcal{L} \mid a \leq_{\mathcal{L}} x\}$. When $A \subseteq \mathcal{L}$ then its lower closure (respectively, upper closure) is $\downarrow A := \bigcup_{a \in A} \downarrow a$ (respectively, $\uparrow A := \bigcup_{a \in A} \uparrow a$). A subset $A \subseteq \mathcal{L}$ is said to be *lower-closed* (respectively, *upper-closed*) if $\downarrow A = A$ (respectively, $\uparrow A = A$). We have the following definitions relative to partially ordered sets.

Definition 1 Let \mathcal{L} be a partially ordered set and $A \subseteq \mathcal{L}$. The set A is said to be *bounded below* (in \mathcal{L}) if there exists a compact set $B \subseteq \mathcal{L}$ such that $A \subseteq \uparrow B$. Similarly, the set A is said to be *bounded above* (in \mathcal{L}) if there exists a compact set $B \subseteq \mathcal{L}$ such that $A \subseteq \downarrow B$.

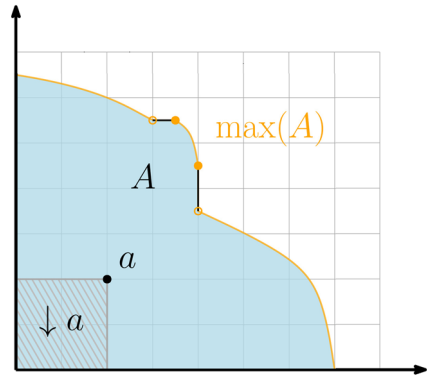
Definition 2 Let \mathcal{L} be a partially ordered set and consider a closed subset $A \subseteq \mathcal{L}$. If the set A is bounded below, then the set of *minimal elements* of A is defined as $\min(A) := \{x \in A \mid \forall x_1 \in A, x \leq_{\mathcal{L}} x_1 \text{ or } (x, x_1) \in \text{Inc}_{\mathcal{L}}\}$. Similarly, if the set A is bounded above, then the set of *maximal elements* of A is defined as $\max(A) := \{x \in A \mid \forall x_1 \in A, x \geq_{\mathcal{L}} x_1 \text{ or } (x, x_1) \in \text{Inc}_{\mathcal{L}}\}$.

An illustration of the concepts of lower-closed sets and maximal elements is provided in Fig. 1. It was shown in [23] that lower and upper-closed sets satisfy the following property.

Proposition 1 Let \mathcal{L} be a partially ordered set and consider a collection of subsets $A_i \subseteq \mathcal{L}$, $i \in \{1, 2, \dots, p\}$. The following holds:

- (i) If for all $i \in \{1, 2, \dots, p\}$, A_i is lower closed then $\cup_{i=1}^p A_i$ and $\cap_{i=1}^p A_i$ are lower closed;

Fig. 1 A lower closed set $A \subseteq \mathbb{R}_{\geq 0}^2$, with the standard ordering, in blue. The set of its maximal elements $\max(A)$ is presented in orange. The lower closure of a point $a \in A$ is presented in dashed gray



(ii) If for all $i \in \{1, 2, \dots, p\}$, A_i is upper closed then $\cup_{i=1}^p A_i$ and $\cap_{i=1}^p A_i$ are upper closed.

In the rest of the paper, we will focus on lower-closed sets; analogous results can be formulated for upper-closed sets.

2.2 Continuity of set-valued maps

In this section, we recall the following continuity notions for set-valued maps [24].

Definition 3 Consider a set-valued map $F : \mathcal{X} \rightrightarrows \mathbb{R}^n$, where $\mathcal{X} \subset \mathbb{R}^m$ and $F(x)$ is compact for all $x \in \mathcal{X}$.

- The map F is said to be *lower semicontinuous* at $x \in \mathcal{X}$ if for each $\epsilon > 0$ and $y_x \in F(x)$, there exists $\eta > 0$ such that the following property holds: for each $z \in \mathcal{B}_\eta(x) \cap \mathcal{X}$, there exists $y_z \in F(z)$ such that $\|y_z - y_x\| \leq \epsilon$;
- The map F is said to be *upper semicontinuous* at $x \in \mathcal{X}$ if, for each $\epsilon > 0$, there exists $\eta > 0$ such that $F(\mathcal{B}_\eta(x)) \cap \mathcal{X} \subset \mathcal{B}_\epsilon(F(x))$;
- The map F is said to be *continuous* at $x \in \mathcal{X}$ if it is both upper and lower semicontinuous at x .
- The map F is said to be lower, upper semicontinuous, or continuous if, respectively, it is lower, upper semicontinuous, or continuous for all $x \in \mathcal{X}$.
- For $L \geq 0$, the set valued map F is said to be *L -Lipschitz* if for all $x_1, x_2 \in \mathcal{X}$, $F(x_1) \subseteq \mathcal{B}_{L\|x_1-x_2\|}(F(x_2))$.

2.3 Discrete-time control systems

In this paper, we consider the class of discrete-time control systems Σ of the form:

$$x(k+1) = f(x(k), u(k), d(k)) \quad (1)$$

where $x(k) \in \mathcal{X}$ is a state, $u(k) \in \mathcal{U}$ is a control input and $d(k) \in \mathcal{D}$ is a disturbance input. The trajectories of (1) are denoted by $\Phi(\cdot, x_0, \mathbf{u}, \mathbf{d})$ where $\Phi(k, x_0, \mathbf{u}, \mathbf{d})$ is

the state reached at time $k \in \mathbb{N}_{\geq 0}$ from the initial state x_0 under the control input $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ and the disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{D}$. For $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$, we use the notation $f(X, U, D) = \{f(x, u, d) \mid x \in X, u \in U, d \in D\}$.

When the control inputs of system (1) are generated by a state-feedback controller $\kappa : \mathcal{X} \rightarrow \mathcal{U}$, the dynamics of the closed-loop system is given by

$$x(k+1) = f(x(k), \kappa(x(k)), \mathbf{d}(k)) \quad (2)$$

and its trajectories are denoted by $\Phi_\kappa(\cdot, x_0, \mathbf{d})$. By abuse of notation, in the rest of the paper we use $\Phi_\kappa(\cdot, x_0, D)$ to denote $\{\Phi_\kappa(\cdot, x_0, \mathbf{d}) \mid \mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D\}$.

3 Monotone control systems

In this section, we introduce classes of monotone discrete-time control systems, that preserve order with respect to states, disturbance inputs and control inputs. Then, we provide characterizations of the considered classes of systems.

Definition 4 Consider the discrete-time control system Σ in (1). The system Σ is said to be:

- *State monotone (SM)* if its set of states is equipped with a partial order $\leq_{\mathcal{X}}$, and for all $x_1, x_2 \in \mathcal{X}$, for all $u \in \mathcal{U}$ and for all $d \in \mathcal{D}$, if $x_1 \leq_{\mathcal{X}} x_2$ then $f(x_1, u, d) \leq_{\mathcal{X}} f(x_2, u, d)$;
- *Control-state monotone (CSM)* if its sets of states and control inputs are equipped with partial orders $\leq_{\mathcal{X}}$ and $\leq_{\mathcal{U}}$, respectively, and for all $x_1, x_2 \in \mathcal{X}$, for all $u_1, u_2 \in \mathcal{U}$ and for all $d \in \mathcal{D}$, if $x_1 \leq_{\mathcal{X}} x_2$ and $u_1 \leq_{\mathcal{U}} u_2$ then $f(x_1, u_1, d) \leq_{\mathcal{X}} f(x_2, u_2, d)$;
- *Disturbance-state monotone (DSM)* if its sets of states and disturbance inputs are equipped with partial orders $\leq_{\mathcal{X}}$ and $\leq_{\mathcal{D}}$, respectively, and for all $x_1, x_2 \in \mathcal{X}$, for all $u \in \mathcal{U}$ and for all $d_1, d_2 \in \mathcal{D}$, if $x_1 \leq_{\mathcal{X}} x_2$ and $d_1 \leq_{\mathcal{D}} d_2$ then $f(x_1, u, d_1) \leq_{\mathcal{X}} f(x_2, u, d_2)$;
- *Control-disturbance-state monotone (CDSM)* if its sets of states, inputs and disturbances are equipped with partial orders, $\leq_{\mathcal{X}}$, $\leq_{\mathcal{U}}$ and $\leq_{\mathcal{D}}$, respectively, and for all $x_1, x_2 \in \mathcal{X}$, $u_1, u_2 \in \mathcal{U}$ and for all $d_1, d_2 \in \mathcal{D}$, if $x_1 \leq_{\mathcal{X}} x_2$, $u_1 \leq_{\mathcal{U}} u_2$ and $d_1 \leq_{\mathcal{D}} d_2$ then $f(x_1, u_1, d_1) \leq_{\mathcal{X}} f(x_2, u_2, d_2)$.

Remark 1 In this paper, different types of monotonicity are defined with respect to the state, control input and disturbance input. The SM, (DSM and CDSM, respectively) properties defined in this paper correspond to the discrete-time versions of the concept of monotonicity in [25] ([26] and [27], respectively).

From the definitions above, it can be seen that a CDSM system is a CSM and DSM system and that a DSM or CSM is a SM system. The notions above can be easily verified via the Kamke–Muller conditions [25] for continuously differentiable vector fields as follows: The system Σ in (1) with $x(k) \in \mathcal{X} \subseteq \mathbb{R}^n$, $u(k) \in \mathcal{U} \subseteq \mathbb{R}^m$ and $d(k) \in \mathcal{D} \subseteq \mathbb{R}^p$ is

- SM if $\frac{\partial f_i}{\partial x_j} \geq 0$ for all $i, j \in \{1, 2, \dots, n\}$;
- CSM if $\frac{\partial f_i}{\partial x_j} \geq 0$ and $\frac{\partial f_i}{\partial u_h} \geq 0$ for all $i, j \in \{1, 2, \dots, n\}$ and for all $h \in \{1, 2, \dots, m\}$;
- DSM if $\frac{\partial f_i}{\partial x_j} \geq 0$ and $\frac{\partial f_i}{\partial d_h} \geq 0$ for all $i, j \in \{1, 2, \dots, n\}$ and for all $h \in \{1, 2, \dots, p\}$;
- CDSM if $\frac{\partial f_i}{\partial x_j} \geq 0$, $\frac{\partial f_i}{\partial u_h} \geq 0$ and $\frac{\partial f_i}{\partial d_l} \geq 0$ for all $i, j \in \{1, 2, \dots, n\}$, for all $h \in \{1, 2, \dots, m\}$ and for all $l \in \{1, 2, \dots, p\}$.

where ≥ 0 is the usual total order on \mathbb{R} .

The following examples illustrate the difference between the different versions of monotonicity introduced above.

Example 1 We present examples of the considered classes of systems:

- The system described by

$$x(k+1) = x(k) + u(k)d(k) \sin(u(k)d(k))$$

with $x(k), u(k), d(k) \in \mathbb{R}$, is SM without being DSM nor CDSM for the usual total order on \mathbb{R} .

- The system described by

$$x(k+1) = \begin{cases} A_1 x(k) + d(k) & \text{if } u = 1 \\ A_2 x(k) + d(k) & \text{if } u = 2 \end{cases}$$

with $x(k), d(k) \in \mathbb{R}^2$ and $u(k) \in \{1, 2\}$, $A_1 = \begin{pmatrix} 0.8 & 0.1 \\ 2 & 4 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 5 & 0.2 \\ 8 & 0 \end{pmatrix}$, is

DSM without being CSM nor CDSM for the usual partial order on \mathbb{R}^2 ;

- The system described by

$$x(k+1) = x(k) + u(k) + d(k)$$

with $x(k), u(k), d(k) \in \mathbb{R}$, is CDSM for the usual total order on \mathbb{R} .

Remark 2 Monotone systems constitute a broad class of systems that arise in biology [26], traffic flow models [28], microgrids [29], and other applications. Monotonicity may appear to be restrictive when judged from the sign conditions for monotonicity with respect to the positive orthant, but graphical tests exist to detect monotonicity with respect to other orthants and can be modified with changes of variables to detect monotonicity with respect to broader cones. In addition, physical insights, e.g., restricting the dynamics to hyperplanes associated with conservation laws, may reveal monotonicity that is not apparent; this has been observed in biomolecular signaling cascades. Finally, algorithms exist to decompose systems into monotone components [30].

Next we give an auxiliary lemma, which enables us to present equivalent characterizations of the proposed classes of monotone systems.

Lemma 1 Let \mathcal{L} be a partially ordered set and $A, B \subseteq \mathcal{L}$. We have $A \subseteq \downarrow B$ if and only if for any $a \in A$, there exists $b \in B$ such that $a \leq_{\mathcal{L}} b$.

The proof follows immediately from the fact that $\downarrow B = \{z \in \mathcal{L} \mid \exists b \in B \text{ satisfying } z \leq_{\mathcal{L}} b\}$.

Proposition 2 Consider the discrete-time control system Σ in (1), the following properties hold:

(i) The system Σ is SM if and only if for all $x \in X$, $u \in U$ and $d \in D$ we have

$$f(\downarrow x, u, d) \subseteq \downarrow f(x, u, d)$$

(ii) The system Σ is CSM if and only if for all $x \in X$, $u \in U$ and $d \in D$ we have

$$f(\downarrow x, \downarrow u, d) \subseteq \downarrow f(x, u, d)$$

(iii) The system Σ is DSM if and only if for all $x \in X$, $u \in U$ and $d \in D$ we have

$$f(\downarrow x, u, \downarrow d) \subseteq \downarrow f(x, u, d)$$

(iv) The system Σ is CDSM if and only if for all $x \in X$, $u \in U$ and $d \in D$ we have

$$f(\downarrow x, \downarrow u, \downarrow d) \subseteq \downarrow f(x, u, d)$$

The following auxiliary result characterizes the monotonicity property of the closed loop controlled system.

Lemma 2 Consider the system Σ in (1). If the system Σ is CDSM and if the controllers $\kappa_1, \kappa_2 : \mathcal{X} \rightarrow \mathcal{U}$ satisfy

$$\kappa_1(x_1) \leq_{\mathcal{U}} \kappa_2(x_2), \quad \forall x_1, x_2 \in \mathcal{X}, \text{ with } x_1 \leq_{\mathcal{X}} x_2, \quad (3)$$

then for all $x_1^0, x_2^0 \in X$, with $x_1^0 \leq_{\mathcal{X}} x_2^0$, and for all $\mathbf{d}_1, \mathbf{d}_2 : \mathbb{N}_{\geq 0} \rightarrow \mathcal{D}$ satisfying $\mathbf{d}_1 \leq_{D^w} \mathbf{d}_2$, we have $\Phi_{\kappa_1}(\cdot, x_1^0, \mathbf{d}_1) \leq_{\mathcal{X}^w} \Phi_{\kappa_2}(\cdot, x_2^0, \mathbf{d}_2)$.

4 Controlled invariants

We start by recalling the concept of controlled invariant [1]. In simple words, a controlled invariant set is a set for which there exists a controller such that if the state of the system is initialized in this set, then its solutions remain there for all time.

Definition 5 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. The set $K \subseteq \mathcal{X}$ is said to be a *robust controlled invariant* for the system Σ and constraint set (X, U, D) if $K \subseteq X$ and there exists a controller $\kappa : X \rightarrow U$, with $\text{dom}(\kappa) = K$ and such that for all $x_0 \in K$ and for any disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ the solution of the closed

loop system $\Phi_\kappa(., x_0, \mathbf{d}) : \mathbb{N}_{\geq 0} \rightarrow \mathcal{X}$ satisfies $\Phi_\kappa(k, x_0, \mathbf{d}) \in K$ for all $k \in \mathbb{N}_{\geq 0}$ ¹. In this case, κ is said to be an *invariance controller* for the system Σ and constraint set (X, U, D) .

While the characterization of controlled invariants in Definition 5 is the most commonly used in the literature [1, 31], the equivalent characterization below has also been used in the literature [32].

Proposition 3 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. The set $K \subseteq \mathcal{X}$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) if and only if $K \subseteq X$ and the following holds:

$$\forall x \in K, \exists u \in U \text{ s.t. } f(x, u, D) \subseteq K. \quad (4)$$

From Proposition 3, one can readily see that the robust controlled invariance property is closed under union. Hence, there exists a unique robust controlled invariant that is maximal, in the sense that it contains all the robust controlled invariants.

Definition 6 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. The set $K \subseteq \mathcal{X}$ is the *maximal* robust controlled invariant set for the system Σ and constraint set (X, U, D) if:

- $K \subseteq \mathcal{X}$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) ;
- K contains any robust controlled invariant for the system Σ and constraint set (X, U, D) .

In this case, any invariance controller $\kappa : X \rightarrow U$ satisfying $\text{dom}(\kappa) = K$ is said to be a maximal invariance controller for the system Σ and constraint set (X, U, D) .

The following auxiliary result characterizes the effect of enlarging the set of control inputs and shrinking the set of disturbance inputs on the robust controlled invariance problem. The proof of this result is straightforward and thus omitted.

Lemma 3 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U_1, U_2 \subseteq \mathcal{U}$ and $D_1, D_2 \subseteq \mathcal{D}$ be constraints sets on the states, inputs and disturbances, respectively, satisfying $U_1 \subseteq U_2$ and $D_2 \subseteq D_1$. If K is a robust controlled invariant for the system Σ and constraint set (X, U_1, D_1) , then K is a robust controlled invariant for the system Σ and constraint set (X, U_2, D_2) .

5 Set-based characterization of controlled invariants

First, we have the following general characterization of the topological structure of controlled invariants for nonlinear systems under more regularity on the dynamics of the system.

¹ The condition $\Phi_\kappa(k, x_0, \mathbf{d}) \in K$ for all $k \in \mathbb{N}_{\geq 0}$ can be equivalently replaced by the following condition: $\Phi_\kappa(k, x_0, \mathbf{d}) \in X$ for all $k \in \mathbb{N}_{\geq 0}$.

Proposition 4 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be constraints sets on the states, inputs and disturbances, respectively. Suppose that the map $f : \mathcal{X} \times \mathcal{U} \times \mathcal{D}$ describing the system Σ is lower semicontinuous on its first argument and the set of control inputs U and disturbance inputs D are compact. The following properties hold:

- (i) If the set $K \subseteq X$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) , then the set $\text{cl}(K)$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) ;
- (ii) If the set $K \subseteq X$ is the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) , then the set K is closed.

In the following, we provide different characterizations of robust controlled invariants when dealing with monotone dynamical systems and lower-closed safety specifications (i.e., lower closed set of constraints on the state-space X).

Theorem 5 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively, where the set X is lower closed. The following properties hold:

- (i) If the system Σ is SM and if a set K is a robust controlled invariant of the system Σ and constraint set (X, U, D) , then its lower closure is also a robust controlled invariant for the system Σ and constraint set (X, U, D) ;
- (ii) If the system Σ is SM then the maximal robust controlled invariant K for the system Σ and constraint set (X, U, D) is lower closed;
- (iii) If the system Σ is DSM and the set of disturbance inputs D is closed and bounded above then the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) is the maximal robust controlled invariant for the system Σ and the constraint set (X, U, D_{\max}) , where $D_{\max} = \max(D)$;
- (iv) If the system Σ is CSM, the set of control inputs U is closed and bounded below then the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) is the maximal robust controlled invariant for the system Σ and the constraint set (X, U_{\min}, D) , where $U_{\min} = \min(U)$;
- (v) If the system Σ is CDSM, the set of control inputs U is closed and bounded below and the set of disturbance inputs D is closed and bounded above, then the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) is the maximal robust controlled invariant for the system Σ and constraint set (X, U_{\min}, D_{\max}) , where $U_{\min} = \min(U)$ and $D_{\max} = \max(D)$.

The result in (ii) states that for SM systems, the maximal robust controlled invariant can be characterized using only its maximal values (in the sense of the partial order $\leq_{\mathcal{X}}$). The result in (iii) states that to compute the maximal robust controlled invariant for DSM systems, it is sufficient to use maximal disturbance inputs. Finally, the result in (v) states that to compute the maximal robust controlled invariant for CDSM systems, it is sufficient to use maximal disturbance inputs and minimal control inputs. We also have the following characterizations of controlled invariants for the considered classes of systems.

Proposition 6 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively, where the set X is lower closed. Consider a closed and lower closed set $K \subseteq X$. The following properties hold:

- (i) If the system Σ is SM then the set K is a robust controlled invariant of the system Σ and constraint set (X, U, D) , if and only if the following holds:

$$\forall x \in \max(K), \exists u \in U \text{ s.t. } f(x, u, D) \subseteq K, \quad (5)$$

- (ii) If the system Σ is DSM and the set of disturbance inputs D is closed and bounded above, then the set K is a robust controlled invariant of the system Σ and constraint set (X, U, D) , if and only if the following holds:

$$\forall x \in \max(K), \exists u \in U \text{ s.t. } f(x, u, D_{\max}) \subseteq K, \quad (6)$$

where $D_{\max} = \max(D)$;

- (iii) If the system Σ is CSM and the set of control inputs U is closed and bounded below, then the set K is a robust controlled invariant of the system Σ and constraint set (X, U, D) , if and only if the following holds:

$$\forall x \in \max(K), \exists u \in U_{\min} \text{ s.t. } f(x, u, D) \subseteq K, \quad (7)$$

where $U_{\min} = \min(U)$;

- (iv) If the system Σ is CDSM, the set of control inputs U is closed and bounded below and the set of disturbance inputs D is closed and bounded above then the set K is a robust controlled invariant of the system Σ and constraint set (X, U, D) , if and only if the following holds:

$$\forall x \in \max(K), \exists u \in U_{\min} \text{ s.t. } f(x, u, D_{\max}) \subseteq K, \quad (8)$$

where $U_{\min} = \min(U)$ and $D_{\max} = \max(D)$.

Proposition 6 is critical from a computational point of view, when the objective is to check whether a lower-closed set is a robust controlled invariant. Indeed, while the invariance condition needs to be checked for all the elements $x \in K$, $u \in U$ and $d \in D$ for general nonlinear systems [see Eq. (4)], it has to be checked only for the elements:

- $x \in \max(K)$, $u \in U$ and $d \in D$ for SM systems;
- $x \in \max(K)$, $u \in U$ and $d \in D_{\max}$ for DSM systems;
- $x \in \max(K)$, $u \in U_{\min}$ and $d \in D$ for CSM systems;
- $x \in \max(K)$, $u \in U_{\min}$ and $d \in D_{\max}$ for CDSM systems.

Moreover, one can also see that this property is very useful in practice when $\max(K)$, D_{\max} and U_{\min} are finite while K , D and U are infinite.

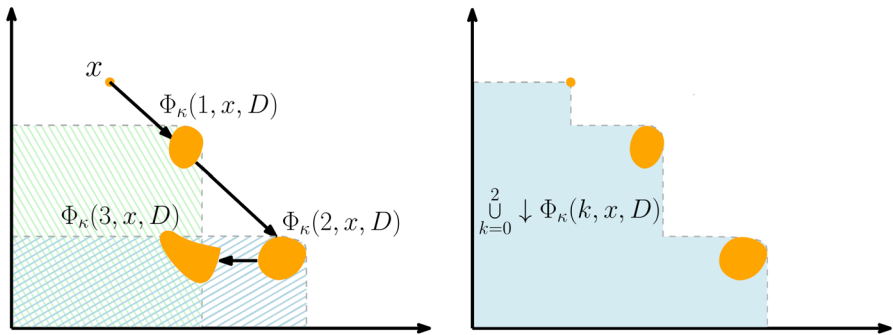


Fig. 2 Illustration of the concept of closed-loop feasibility. Left: the 3-step reachable set from the initial condition x for a system Σ . Note that $\Phi_\kappa(3, x, D) \subseteq \downarrow \Phi_\kappa(1, x, D) \cup \downarrow \Phi_\kappa(2, x, D)$. Right: The set $\downarrow \bigcup_{k=0}^2 \Phi_\kappa(k, x, D)$ is a robust controlled invariant of the system Σ in view of Proposition 7

6 Trajectory-based characterizations of controlled invariants

In this section, we provide trajectory-based characterizations of controlled invariants. We start by introducing the concept of lower feasibility.

Definition 7 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. A point $x_0 \in X$ is said to be *closed-loop feasible* w.r.t the constraint set (X, U, D) if there exists a controller $\kappa : X \rightarrow U$ and $N \in \mathbb{N}_{>0}$ such that

$$\Phi_\kappa(k, x_0, D) \subseteq X, \quad \forall k \in \{0, 1, \dots, N-1\}, \quad (9)$$

and

$$\Phi_\kappa(N, x_0, D) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_\kappa(k, x_0, D), \quad (10)$$

Similarly, a point $x_0 \in X$ is said to be *open-loop feasible* w.r.t the constraint set (X, U, D) if there exists an input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that

$$\Phi(k, x_0, \mathbf{u}, D) \subseteq X, \quad \forall k \in \{1, 2, \dots, N-1\} \quad (11)$$

and

$$\Phi(N, x_0, \mathbf{u}, D) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D). \quad (12)$$

An illustration of the concept of closed-loop feasibility is presented in Fig. 2 (Left). The following proposition shows the usefulness of feasible points to compute controlled invariants for SM systems. Conclusion (i) of this proposition is illustrated in Fig. 2 (right).

Proposition 7 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively, where the set X is lower closed. If the system Σ is SM, then the following holds:

- (i) If x_0 is closed loop feasible w.r.t the constraint set (X, U, D) then there exists a controller $\kappa : X \rightarrow U$ and $N \in \mathbb{N}_{>0}$ such that the set

$$K = \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_{\kappa}(k, x_0, D) \quad (13)$$

is a robust controlled invariant for the system Σ and constraint set (X, U, D) .

- (ii) If $x_0 \in X$ is open-loop feasible w.r.t the constraint set (X, U, D) , then there exists an input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that the set

$$K = \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D) \quad (14)$$

is a robust controlled invariant for the system Σ and constraint set (X, U, D) .

In the following, we characterize open-loop feasibility for DSM systems. Before providing the result, we give the following auxiliary lemma.

Lemma 4 Consider the system Σ in (1). If the system Σ is DSM and the set of disturbance inputs D is closed and bounded above, then for any point $x_0 \in X$ and any input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$, we have $\Phi(k, x_0, \mathbf{u}, D) \subseteq \downarrow \Phi(k, x_0, \mathbf{u}, D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$.

Proposition 8 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. If the system Σ is DSM, the set of states X is lower closed and the set of disturbance inputs D is closed and bounded above, then a point $x_0 \in X$ is open-loop feasible w.r.t the constraint set (X, U, D_{\max}) if and only if it is open-loop feasible w.r.t the constraint set (X, U, D) , where $D_{\max} = \max(D)$.

We also have the following characterization of open-loop feasibility for a particular class of CSM systems.

Proposition 9 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively, where X is lower closed. If the system Σ is CDSM, the set of states X is lower closed, the set of control inputs U is closed and bounded below, and for all $\varepsilon \in \mathbb{R}_{\geq 0}^n$, for all $x_1, x_2 \in \mathcal{X}$ and for all $u \in U$, following condition is satisfied:

$$x_1 \geq x_2 + \varepsilon \implies \mathcal{B}_{\varepsilon}(f(x_2, u, D)) \subseteq \downarrow f(x_1, u, D) \quad (15)$$

then a point $x_0 \in X$ is open-loop feasible w.r.t the constraint set (X, U, D) if and only if it is open-loop feasible w.r.t the constraint set (X, U_{\min}, D) , where $U_{\min} = \min(U)$.

In the following result, we provide a comparison between the closed-loop and open-loop feasibility.

Proposition 10 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. If a point $x_0 \in X$ is open-loop feasible w.r.t the constraint set (X, U, D) , then it is closed-loop feasible w.r.t the constraint set (X, U, D) . Moreover, the converse holds if one of the following conditions is satisfied:

- The system Σ is disturbance free, i.e., $D = \{\bar{d}\}$.
- The system Σ is DSM and $\text{card}(D_{\max}) = 1$.

Moreover, we have the following result, characterizing a special case of open-loop feasibility for the particular class of monotone systems with Lipschitz dynamics.

Theorem 11 Consider the SM system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively. Assume that the map $f : \mathcal{X} \times \mathcal{U} \times \mathcal{D} \rightarrow \mathcal{X}$ defining the system Σ is continuous on its first and third arguments, and the sets of control inputs U and disturbance inputs D are compact. Consider $x_0 \in \mathcal{X}$. If the following conditions are satisfied:

- (i) x_0 is open-loop feasible w.r.t the constraint set (X, U, D) and there exists $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$, $N \in \mathbb{N}_{>0}$ and ε_N such that

$$\mathcal{B}_{\varepsilon_N}(\Phi_{\kappa}(N, x_0, \mathbf{u}, D)) \subseteq \bigcup_{0 \leq k \leq N-1} \Phi_{\kappa}(k, x_0, \mathbf{u}, D). \quad (16)$$

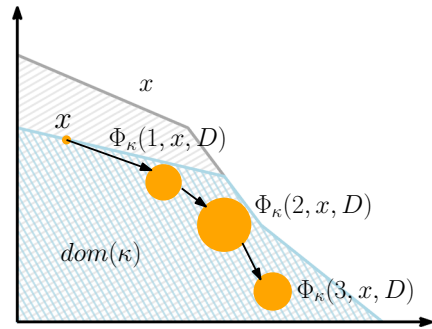
- (ii) there exists $\gamma > 0$ such that $\mathcal{B}_{\gamma}(\Phi(k, x_0, \mathbf{u}, D)) \subseteq X$, $\forall k \in \{1, 2, \dots, N-1\}$ then there exists $\beta > 0$ such that for any $x_1 \in \{\uparrow x_0\} \cap \mathcal{B}_{\beta}(x_0)$, x_1 is open-loop feasible w.r.t the constraint set (X, U, D) . Moreover, when the map f is L -Lipschitz on \mathcal{X} on its first argument, then one can explicitly determine the value of β as a function of the parameters ε_N and γ .

We have analyzed in Theorem 5 the structural properties of the maximal robust controlled invariant set for monotone systems and lower-closed safety specifications. In the following, and under more regularity assumptions on the system, we provide a characterization of the trajectories initiated at the boundaries of the maximal robust controlled invariant.

Proposition 12 Consider the system Σ in (1) and let $X \subseteq \mathcal{X}$, $U \subseteq \mathcal{U}$ and $D \subseteq \mathcal{D}$ be the constraints sets on the states, inputs and disturbances, respectively, where the set X is lower closed. Let κ be a robust maximal invariance controller for the system Σ and the constraint set (X, U, D) . If the system Σ is SM, the map $f : \mathcal{X} \times \mathcal{U} \times \mathcal{D} \rightarrow \mathcal{X}$ defining the system Σ is continuous on its first and third arguments, and the sets of control inputs U and disturbance inputs D are compact, then for all $x_0 \in \partial(\text{dom}(\kappa))$ one of the following scenarios hold:

- (i) $\Phi_{\kappa}(k, x_0, D) \cap \partial(\text{dom}(\kappa)) \neq \emptyset$ for all $k \in \mathbb{N}_{\geq 0}$;

Fig. 3 An illustration of scenario (ii) in Proposition 12 where we have a lower closed set X (in gray) and the corresponding maximal robust controlled invariant set K (in blue). For an initial condition $x \in K$, the reachable set $\Phi_\kappa(\cdot, x, D) : \mathbb{N}_{\geq 0} \rightarrow X$ has a non-empty intersection with the boundaries of the set ∂X , before reaching the interior of the set K



(ii) There exists $p \in \mathbb{N}_{>0}$ such that

- $\Phi_\kappa(p-1, x_0, D) \cap (\partial(\text{dom}(\kappa)) \setminus \partial X) = \emptyset$
- $\Phi_\kappa(p-1, x_0, D) \cap \partial X \neq \emptyset$
- $\Phi_\kappa(p, x_0, D) \subseteq \text{Int}(\text{dom}(\kappa))$.

The result of Proposition 12 is illustrated in Fig. 3. Intuitively, the result of Proposition 12 states that for any initial condition x in the boundary of the maximal robust controlled invariant K , either the reachable set $\Phi_\kappa(\cdot, x, D) : \mathbb{N}_{\geq 0} \rightarrow X$ will always have a non-empty intersection with the boundaries, which corresponds to case (i), or it will have a non-empty intersection with the boundaries of the set X (i.e., ∂X) before reaching the interior of the set K , which corresponds to case (ii).

7 Verification and computation of controlled invariants

7.1 Verification of controlled invariants

The result of Proposition 6 shows that robust controlled invariants for monotone dynamical systems enjoy useful properties, in the sense that the verification of whether a set is controlled invariant or not boils down to checking only the properties of its maximal elements. Based on this intuition, in this section, we present an algorithm to the verification of robust controlled invariants. In the following, we present the main algorithm for the class of SM systems. Then, we explain how the algorithm can be improved for CSM and DSM systems.

Algorithm 1 works as follows: it explores all the elements x of the set $\max(K)$. If for each element $x \in \max(K)$, we have the existence of $u \in U$ such that $f(x, u, D) \subseteq K$, then, in view of Proposition 6, the set K is a robust controlled invariant for the system Σ and constraint set (X, U, D) ; otherwise, if there exists $x \in \max(K)$ such that for all $u \in U$, $f(x, u, D) \not\subseteq K$, then the set K is not a controlled invariant.

Moreover, other properties can be used to improve the proposed algorithm. Indeed, if the system Σ is DSM, then the condition $f(x, u, D) \subseteq K$ can be replaced by the simpler condition $f(x, u, D_{\max}) \subseteq K$, where $D_{\max} = \max(D)$. Similarly, if the system Σ is CSM, then only the set of inputs $U_{\min} = \min(U)$ is explored, instead of the whole set of control inputs U .

Algorithm 1 Verification of controlled invariants

Input: A SM system Σ as in (1), a constraint set (X, U, D) , where X a lower closed set, and a lower closed set $K \subset X$

Output: True, if K is a robust controlled invariant for the system Σ and constraint set (X, U, D) .

```

1  begin,
2     $a := 1$ ,
3    for  $x \in \max(K)$ 
4      if there exists  $u \in U$  such that  $f(x, u, D) \subseteq K$  then
5         $a = a \times 1$ 
6      else  $a = a \times 0$ .
7    end if
8  end for
9  return True if  $a == 1$ .
```

7.2 Computation of controlled invariants

As shown in Theorem 5 and Proposition 7, controlled invariants for monotone systems and lower closed safety specifications are lower closed and can be computed using feasible points. This property implies that the boundary of the maximal robust controlled invariant set has the structure of a Pareto front and can therefore be approximated arbitrarily close, by resorting to multi-dimensional binary search algorithms used in multi-objective optimization [21, 33].² Based on such approaches, in the following we present the main algorithm for the computation of robust controlled invariants for the class of SM systems. Then, we explain the parts that needs to be modified for the case of DSM and CSM systems.

For a given x , the command *open loop-feasible* in Algorithm 2 checks if x is open-loop feasible, i.e., if it satisfies (12) for some input trajectory $\mathbf{u} : \mathbb{N} \rightarrow U$. If this is the case, any point in the lower closure of the set Z defined below is feasible, and there is no need to explore it:

$$Z = \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D). \quad (17)$$

Hence, all the elements of the set Z are stored in the set \mathcal{F}_1 representing the set of states belonging to the maximal robust controlled invariant. Similarly, we use the set \mathcal{F}_2 to store the elements that do not belongs to the maximal robust controlled invariant set. The command *leads to the unsafe set* $\mathcal{F}_2 \cup \bar{X}$ in Algorithm 2 checks if for all possible input trajectories $\mathbf{u} : \mathbb{N} \rightarrow U$ there exists $k \in \{1, 2, \dots, N\}$ such that $\Phi(k, x_0, \mathbf{u}, D) \cap \mathcal{F}_2 \cup \bar{X} \neq \emptyset$. If x leads to the unsafe set, then any state from the upper closure of the set Y defined below will lead to the unsafe set, and there is no need to explore it:

$$Y = \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D) \quad (18)$$

² Similar approaches, based on the approximation of the boundaries of Pareto fronts has been explored for the computation of timing and safety contracts in [34, 35].

Algorithm 2 consists of three parts. In the first part (lines 2–11), the elements of the set $\max(X)$ are explored. In the second part (lines 12–18), the elements of the set $\min(X)$ ³ are explored. Finally, lines 22–29 describe the main loop of the algorithm. We start by picking an element from the set of non-explored points and for which we did not decide yet if they are open-loop feasible, or leading to the unsafe set. The strategy to pick a new point to explore is adapted from [21]. The algorithm stops when the Hausdorff distance between the sets \mathcal{F}_1 and \mathcal{F}_2 is smaller than the precision parameter $\varepsilon > 0$. In this case, we get that the set $K = X \cap \mathcal{F}_1$ is a controlled invariant for the system Σ and the constraint set (X, U, D) , and moreover, we also have that $K \subseteq K^* \subseteq \mathcal{B}_\varepsilon(K)$, where K^* is the maximal robust controlled invariant for the system Σ and the constraint set (X, U, D) . This last statement follows directly from the construction of the sets \mathcal{F}_1 and \mathcal{F}_2 since:

- any element of \mathcal{F}_1 belongs to the maximal robust controlled invariant and which is due to the fact that it is constructed based on feasible points;
- any elements of \mathcal{F}_2 leads to the unsafe set, and do not belong to the maximal robust controlled invariant.

Let us now explain how other different structural properties of the system allow to improve the proposed algorithm; these details were removed from the description of the algorithm to improve its readability.

- DSM systems: For both *open loop feasible* and *leads to unsafe set* commands, and in view of Proposition 8, the trajectories of the system are computed only with respect to the set of maximal disturbances $D_{\max} = \max(D)$ when the system is DSM;
- CSM systems: For both *open loop feasible* and *leads to unsafe set*, and in view of Proposition 9, the trajectories of the system are computed only with respect to the set of minimal inputs $U_{\min} = \min(U)$ when the system is CSM and condition (15) is satisfied;
- L -Lipschitz systems: For the *open-loop feasible* command and if for some $x_0 \in X$ conditions (i) and (ii) of Theorem 11 are satisfied, with some $\varepsilon_N, \gamma > 0$, any point in the set $\{\uparrow x_0\} \cap \mathcal{B}_\beta(x_0)$ is feasible, and there is no need to explore it, where β is given in the proof of Theorem 11 as a function of β_N, γ and the Lipschitz constant L .

8 Numerical examples

8.1 Verification of robust controlled invariants

Consider the two-dimensional switched system Σ described by

$$x(k+1) = \begin{cases} A_1 x(k) + d(k) & \text{if } u = 1 \\ A_2 x(k) + d(k) & \text{if } u = 2 \end{cases}$$

³ Let us mention that in general, the set X may not be bounded from below. In this case the set $\min(X)$ can be replaced by any collection of open loop feasible points, and which can be computed before running the algorithm.

Algorithm 2 Computation of controlled invariants

Input: A SM system Σ as in (1), a constraint set (X, U, D) , where X a lower closed set, and a precision $\varepsilon > 0$

Output: A controlled invariant set $K \subseteq X$.

```

1  begin,  $\mathcal{F}_1 = \mathcal{F}_2 = \emptyset$ 
2    for  $x \in \max(X)$ 
3      if  $x$  is open-loop feasible then
4         $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$ , with  $Z$  from (17)
5      else if  $x$  leads to the unsafe set  $\mathcal{F}_2 \cup \bar{X}$ 
6         $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$ , with  $Y$  from (18)
7      end if
8    end for
9    if  $X = \mathcal{F}_1$ 
10     return  $K = X$ 
11  end if
12  for  $x \in \min(X)$ 
13    if  $x$  is open-loop feasible then
14       $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$ , with  $Z$  from (17)
15    else if  $x$  leads to the unsafe set  $\mathcal{F}_2 \cup \bar{X}$ 
16       $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$ , with  $Y$  from (18)
17    end if
18  end for
19  if  $\min(X) \subseteq \mathcal{F}_2$ 
20    return  $K = \emptyset$ 
21  end if
22  while  $d(\mathcal{F}_2, \mathcal{F}_1) > \varepsilon$ 
23    Pick  $x' \in (X \setminus \mathcal{F}_2) \cap (X \setminus \mathcal{F}_1)$ 
24    if  $x'$  is open-loop feasible then
25       $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$ , with  $Y$  from (18)
26    else if  $x'$  leads to the unsafe set  $\mathcal{F}_2 \cup \bar{X}$ 
27       $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$ , with  $Z$  from (17)
28    end if
29  end while
30 return  $K = X \cap \mathcal{F}_1$ .
```

with $x(k) \in \mathbb{R}_{\geq 0}^2$, $d(k) \in \mathcal{D} \in [0, 0.2] \times [0, 0.2]$ and $u(k) \in \{1, 2\}$

$$A_1 = \begin{pmatrix} 1.2 & 0.1 \\ 0.2 & 0.5 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 0.4 & 0.1 \\ 0.1 & 1.1 \end{pmatrix}$$

One can easily check that if the input u of the switched system is fixed, the trajectory will grow unbounded. The objective here is to verify that the set $K = \mathbb{R}_{\geq 0} \cap \{\downarrow a_1\} \cup \{\downarrow a_2\} \cup \{\downarrow a_3\}$ is a robust controlled invariant, with $a_1 = [50, 25]$, $a_2 = [25, 50]$ and $a_3 = [36, 31]$.

Using Algorithm 1, and by exploiting the fact that the system Σ is DSM for the usual partial order on $\mathbb{R}_{\geq 0}^2$, we only explore the maximal elements of the set K , namely a_1 , a_2 and a_3 , while using the maximal disturbance input. Indeed, one can readily see in Fig. 4 that $A_2 a_1 + \max(\mathcal{D}) = [22.7, 35.2] \in K$, $A_1 a_2 + \max(\mathcal{D}) = [35.2, 30.1] \in K$ and $A_1 a_3 + \max(\mathcal{D}) = [35.2, 30.1] \in K$, which shows in view of Proposition 6 that the set K is a robust controlled invariant set for the system Σ and constraint set (X, U, D) . The computation time to implement Algorithm 1 for this particular example

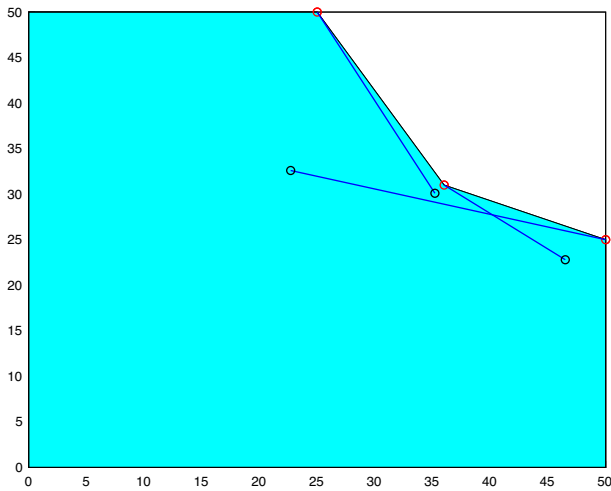


Fig. 4 The light blue region represents set K . The three blue trajectories are initiated from the maximal points (in red) a_1 , a_2 and a_3

is given by 0.18 seconds. The resolution of the proposed verification problem using the classical safety fixed-point algorithm [1, 10, 15] took almost 1 second. The numerical implementations have been done in MATLAB and a computer with processor Apple M1 Max and Memory of 64 GB.

8.2 Computation of robust controlled invariants

We consider a vehicle model moving along a straight road. The dynamics of the vehicle is adapted from [5] and described as:

$$m\dot{v} = \alpha(u, v) = \begin{cases} u - f_0 - f_2 v^2 & \text{if } v > 0 \\ \max(u - f_0, 0) & \text{if } v = 0 \end{cases} \quad (19)$$

where $m > 0$ is the mass of the vehicle, u is the net engine torque applied to the wheels, $v \geq 0$ represents the velocity of the vehicle, and the term $f_0 + f_2 v^2$ includes the rolling resistance and aerodynamics. For this system, u is the control input and satisfies $u \in [U_{\min}, U_{\max}]$. Moreover, we include a lead vehicle whose velocity satisfies $d \in D$, is considered as a disturbance. The dynamics of the system is given by:

$$\begin{cases} \dot{h} = d - v \\ m\dot{v} = \alpha(u, v). \end{cases} \quad (20)$$

From this continuous-time system, we generate a discrete-time model using the sampling period $\tau = 0.5s$, while conserving the monotonicity property of the system.

Remark 3 The system can be easily transformed to a CDSM system one by using the following change of coordinates: $d' = -d$ and $z = -h$.

Table 1 Vehicle and safety parameters

Parameter	Value	Unit
M	1370	Kg
f_0	51.0709	N
f_2	0.4161	Ns ² /m ²
U_{\min}	-4031.9	mKg/s ²
U_{\max}	2687.9	mKg/s ²
d_{\min}	10	m
d'	70	m
v_{\max}	15	m/s

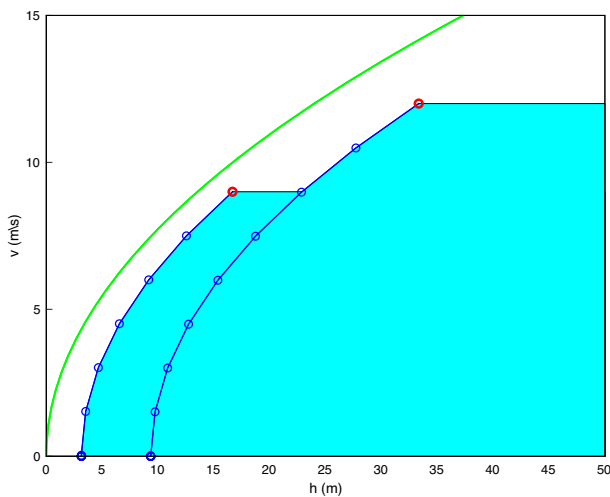


Fig. 5 The light blue region represents the domain of the robust controlled invariant. The blue trajectories are initiated from two feasible points (in red) $x_1 = [33.75; 13.5]$ and $x_2 = [16.25; 9.75]$. The green curve represents the boundary of the maximal robust controlled invariant. The precision ε chosen for Algorithm 2 is $\varepsilon = 1.5$

The objective is to compute a controlled invariant for the system in order to ensure that the velocity remains between 0 and v_{\max} , and the relative distance between the leader and the follower remains larger than 0, while assuming that the velocity of the leader d belongs to the set $D = [0, v_{\max}]$. Moreover, since the constraint $v \geq 0$ is directly satisfied from the model description in (19), the constraint set is a lower closed set. For the computation of a robust controlled invariant, we use Algorithm 2. The parameters model are taken from [5] and are presented in Table 1. Figures 5 and 6 represent the computed robust controlled invariant set for two different precisions $\varepsilon = 1.5$ and $\varepsilon = 0.01$. Moreover, we also present in green the boundary of the maximal robust controlled invariant set, which can be computed analytically for this problem, following the approach presented in [36]. One can see in Fig. 6 that the domain of the obtained controller using a precision $\varepsilon = 0.01$ is almost the same as the domain of the maximal safety controller.

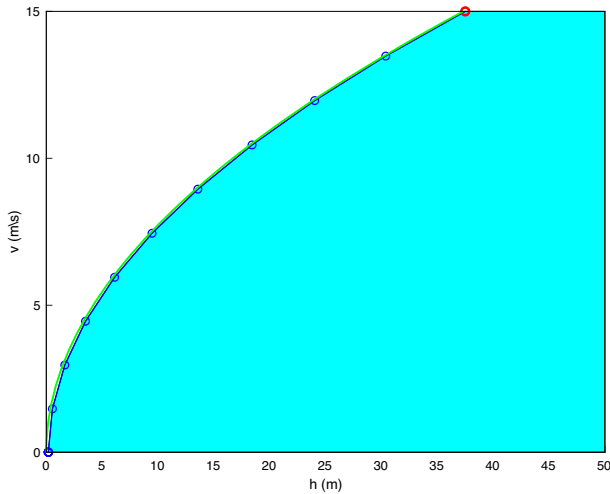


Fig. 6 The light blue region represents the domain of the robust controlled invariant. The blue trajectory is initiated from the feasible point (in red) $x = [37.5; 15]$. The green curve represents the boundary of the maximal robust controlled invariant. The precision ε chosen for Algorithm 2 is $\varepsilon = 0.01$

9 Conclusion

In this paper, we have presented different characterizations of robust controlled invariants for discrete-time monotone dynamical systems, together with an algorithmic procedure to compute the invariants for the considered class of systems. An illustrative example is presented showing the merits of the proposed approach. In future work, we will develop more general algorithms allowing to extend the approach from safety to other types of specifications, such as stability or more general properties described by signal temporal logic formulas.

Acknowledgements This work was supported by the ANR PIA funding: ANR-20-IDEES-0002, by the NSF Grants CNS-2111688, ECCS-1906164, and AFOSR Grant FA9550-21-1-0288.

Declarations

Conflict of interest The authors declare no conflict of interest related to this work.

Appendix A: Proofs

Proof of Proposition 2 We only show (iv), the proofs of (i), (ii) and (iii) can be derived similarly. Let us start with the sufficient condition. Assume that Σ is a CDSM system and consider $x', x \in \mathcal{X}$, $u', u \in \mathcal{U}$ and $d', d \in \mathcal{D}$ satisfying $x' \in (\downarrow x)$, $u' \in (\downarrow u)$ and $d' \in (\downarrow d)$. Using the fact that Σ is a CDSM system, we have that $f(x', u', d') \leq_{\mathcal{X}} f(x, u, d)$, which in turn implies that $f(\downarrow x, \downarrow u, \downarrow d) \subseteq \downarrow f(x, u, d)$. Let us now show the necessary condition. Let $x_1, x_2 \in \mathcal{X}$, $u_1, u_2 \in \mathcal{U}$ and $d_1, d_2 \in \mathcal{D}$ with $x_1 \leq_{\mathcal{X}} x_2$, $u_1 \leq_{\mathcal{U}} u_2$ and $d_1 \leq_{\mathcal{D}} d_2$ and let us show that Σ is CDSM. We have that

$x_1 \in (\downarrow x_2)$, $u_1 \in (\downarrow u_2)$ and $d_1 \in (\downarrow d_2)$. Then, from our assumption, we have that $f(x_1, u_1, d_1) \in f(\downarrow x_2, \downarrow u_2, \downarrow d_2) \subseteq \downarrow f(x_2, u_2, d_2)$, which in turn implies that $f(x_1, u_1, d_1) \leq_{\mathcal{X}} f(x_2, u_2, d_2)$. Hence, Σ is a CDSM system and (iv) holds. \square

Proof of Lemma 2 Consider $x_1^0, x_2^0 \in \mathcal{X}$, with $x_1^0 \leq_{\mathcal{X}} x_2^0$ and $\mathbf{d}_1, \mathbf{d}_2 : \mathbb{N}_{\geq 0} \rightarrow D$ satisfying $\mathbf{d}_1 \leq_{D^w} \mathbf{d}_2$. To show the result, we proceed by induction. First, we have that $\Phi_{\kappa_1}(0, x_1^0, \mathbf{d}_1) = x_1^0 \leq_{\mathcal{X}} x_2^0 = \Phi_{\kappa_2}(0, x_2^0, \mathbf{d}_2)$. Now, consider $k \in \mathbb{N}_{\geq 0}$ and assume that $\Phi_{\kappa_1}(k, x_1^0, \mathbf{d}_1) \leq_{\mathcal{X}} \Phi_{\kappa_2}(k, x_2^0, \mathbf{d}_2)$. Since the system Σ is CDSM and using (3) and the fact that $\mathbf{d}_1 \leq_{D^w} \mathbf{d}_2$ we have that

$$\begin{aligned} \Phi_{\kappa_1}(k+1, x_1^0, \mathbf{d}_1) &= f(\Phi_{\kappa_1}(k, x_1^0, \mathbf{d}_1), \kappa_1(\Phi_{\kappa_1}(k, x_1^0, \mathbf{d}_1)), \mathbf{d}_1(k)) \\ &\leq_{\mathcal{X}} f(\Phi_{\kappa_2}(k, x_2^0, \mathbf{d}_2), \kappa_2(\Phi_{\kappa_2}(k, x_2^0, \mathbf{d}_2)), \mathbf{d}_2(k)) \\ &= \Phi_{\kappa_2}(k+1, x_2^0, \mathbf{d}_2) \end{aligned}$$

Hence, $\Phi_{\kappa_1}(\cdot, x_1^0, \mathbf{d}_1) \leq_{\mathcal{X}^w} \Phi_{\kappa_2}(\cdot, x_2^0, \mathbf{d}_2)$. \square

Proof of Proposition 3 *Sufficient condition:* Consider a controller $\kappa : X \rightarrow U$ defined as

$$\kappa(x) := \text{Single}(\{u \in U \mid f(x, u, d) \in K \text{ for all } d \in D\})$$

Let us show that κ is a robust invariance controller for the system Σ and constraint set (X, U, D) . Consider $x_0 \in K$ and $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ and let us show by induction that $\Phi_{\kappa}(k, x_0, \mathbf{d}) \in K$ for all $k \in \mathbb{N}_{\geq 0}$. First, we have that $\Phi_{\kappa}(0, x_0, \mathbf{d}) = x_0 \in K$. Now assume that $\Phi_{\kappa}(k, x_0, \mathbf{d}) \in K$ and let us show that $\Phi_{\kappa}(k+1, x_0, \mathbf{d}) \in K$. Since $\Phi_{\kappa}(k, x_0, \mathbf{d}) \in K$, we have the existence of $u = \kappa(\Phi_{\kappa}(k, x_0, \mathbf{d})) \in U$ such that for $\mathbf{d}(k) \in D$, $\Phi_{\kappa}(k+1, x_0, \mathbf{d}) = f(\Phi_{\kappa}(k, x_0, \mathbf{d}), \kappa(\Phi_{\kappa}(k, x_0, \mathbf{d})), \mathbf{d}(k)) \in K$. Hence, κ is a robust invariance controller for the system Σ and constraint set (X, U, D) .

Necessary condition: Assume the existence of a controller $\kappa : X \rightarrow U$, with $\text{dom}(\kappa) = K$ and such that for all $x_0 \in K$ and for any disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ the solution of the closed loop system $\Phi_{\kappa}(\cdot, x_0, \mathbf{d}) : \mathbb{N}_{\geq 0} \rightarrow \mathcal{X}$ satisfies $\Phi_{\kappa}(k, x_0, \mathbf{d}) \in K$ for all $k \in \mathbb{N}_{\geq 0}$. Consider $x \in K$, we have the existence of $u = \kappa(x) \in U$ such that $f(x_0, \kappa(x), d) = \Phi_{\kappa}(1, x_0, \mathbf{d}) \in K$ for all $d \in D$, where $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ is any disturbance input trajectory satisfying $\mathbf{d}(0) = d \in D$, which ends the proof. \square

Proof of Proposition 4 We provide a proof for each item separately.

Proof of (i): Let K be a robust controlled invariant for the system Σ and constraint set (X, U, D) and let us show, by contradiction, that $\text{cl}(K)$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) . Consider $x \in \text{cl}(K) \setminus K$ and assume that for all $u \in U$ we have that $f(x, u, D) \cap \text{cl}(K) \neq \emptyset$. Consider $u \in U$, since the set $\text{cl}(K)$ is open, we have the existence of $\varepsilon_u > 0$ and $y_{x,u} \in f(x, u, D) \cap \text{cl}(K)$ such that $\mathcal{B}_{\varepsilon_u}(y_{x,u}) \subseteq \text{cl}(K)$. Since, the set D is compact and f is lower semicontinuous on its first argument, one has that the set valued map $F : \mathcal{X} \times \mathcal{U} \rightrightarrows \mathcal{X}$ defined for $x \in \mathcal{X}$ and $u \in \mathcal{U}$ by $F(x, u) := f(x, u, D)$ is lower semicontinuous on its first argument. Hence, for $\varepsilon_u > 0$ and $y_{x,u} \in F(x, u)$, we have the existence of $\eta_u > 0$ such that for all $z \in \mathcal{B}_{\eta_u}(x)$, there exists $y_{z,u} \in F(z, u)$ satisfying $y_{z,u} \in \mathcal{B}_{\varepsilon_u}(y_{x,u}) \subseteq \text{cl}(K)$. Now consider $\eta = \min_{u \in U} \eta_u$. Since the set U is compact, we have that $\eta > 0$. Hence,

it follows from above that for any $z \in \text{Int}(K) \cap \overline{\mathcal{B}_\eta(x)}$ and for any $u \in U$, we have the existence of $y_{z,u} \in F(z, u)$ satisfying $y_{z,u} \in \text{cl}(K)$, which contradicts the robust controlled invariance of the set K . Hence, the set $\text{cl}(K)$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) .

Proof of (ii): Let K be the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) . From (i) it follows that $\text{cl}(K)$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) . Hence, it follows from maximality of the set K that $\text{cl}(K) = K$. \square

Proof of Theorem 5 We provide a proof for each item separately.

proof of (i): To show the result, we use the characterization of robust controlled invariance from Proposition 3. Let K be a robust controlled invariant for the system Σ and constraint set (X, U, D) . Consider the set $H = \downarrow K$ and let us show that the set H is a robust controlled invariant for the system Σ and constraint set (X, U, D) . Consider $x \in H = \downarrow K$, we have the existence of $x' \in K$ such that $x \leq_{\mathcal{X}} x'$. Since $x' \in K$, which is a robust controlled invariant, we have from Proposition 3 the existence of $u \in U$ such that $f(x', u, d) \in K$ for all $d \in D$. Using the fact that Σ is a SM system we have that $f(x, u, d) \leq_{\mathcal{X}} f(x', u, d)$ for all $d \in D$. Hence, it follows that $f(x, u, d) \in \downarrow K = H$, for all $d \in D$, which implies that $H = \downarrow K$ is a robust controlled invariant for the system Σ and constraint set (X, U, D) .

proof of (ii): To show the result, we use the characterization of robust controlled invariance from Proposition 3. Let K be the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) and consider the set $H = \downarrow K$. First, we have from (i) that the set H is a robust controlled invariant for the system Σ and constraint set (X, U, D) . Moreover, since K is the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) , one has $H = \downarrow K \subseteq K$. Finally, using the fact that $K \subseteq \downarrow K = H$, one gets $K = \downarrow K$ which implies that K is a lower closed set.

proof of (iii): Let K be the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) and let \overline{K} be the maximal robust controlled invariant for the system Σ and the and constraint set (X, U, D_{\max}) . First, since $D_{\max} \subseteq D$, we have from Lemma 3 that $K \subseteq \overline{K}$. In order to show that $\overline{K} \subseteq K$, and from the maximality of the set K it is sufficient to show that the set \overline{K} is a controlled invariant of the system Σ and constraint set (X, U, D) , and which is equivalent, from Proposition 3 to the following condition:

$$\forall x \in \overline{K}, \exists u \in U \text{ s.t. } f(x, u, D) \subseteq \overline{K}. \quad (\text{A1})$$

Consider $x \in \overline{K}$, we have the existence of $u \in U$ such that $f(x, u, D_{\max}) \subseteq \overline{K}$. Moreover, since the set of disturbance inputs D is closed and bounded above and using the fact that Σ is DSM, one has from (iii) in Proposition 2 that $f(x, u, D) = f(x, u, \downarrow D_{\max}) \subseteq \downarrow f(x, u, D_{\max})$. Hence, one gets that $f(x, u, D) \subseteq \downarrow f(x, u, D_{\max}) \subseteq \downarrow \overline{K} = \overline{K}$, where the last equality follows from (i). Hence $\overline{K} \subseteq K$ and (iii) holds.

proof of (iv): Let K be the maximal robust controlled invariant for the system Σ and constraint set (X, U, D) and let \underline{K} be the maximal robust controlled invariant for the system Σ and the constraint set (X, U_{\min}, D) . First, since $U_{\min} \subseteq U$, we have from Lemma 3 that $\underline{K} \subseteq K$. In order to show that $K \subseteq \underline{K}$, from the maximality of

the set \underline{K} , it is sufficient to show that the set K is a controlled invariant of the system Σ and constraint set (X, U_{\min}, D) , and which is equivalent, from Proposition 3 to the following condition:

$$\forall x \in K, \exists u \in U_{\min} \text{ s.t. } f(x, u, D) \subseteq K. \quad (\text{A2})$$

Consider $x \in K$, we have the existence of $u \in U$ such that $f(x, u, D) \subseteq K$. Moreover, since the set of control inputs U is closed and bounded below we have the existence of $u' \in U_{\min}$ such that $u' \leq_U u$. Since the system Σ is CSM, one has from (iii) in Proposition 2 that $f(x, u', D) \subseteq \downarrow f(x, \downarrow u, D) \downarrow f(x, u, D) \subseteq \downarrow K = K$, where the last equality follows from (i). Hence $K \subseteq \underline{K}$ and (v) holds.

proof of (v): The proof is a direct conclusion from (iii), (iv) and the fact that any CDSM system is a CSM and DSM system. \square

Proof of Proposition 6 We provide a proof for each item separately.

proof of (i): First, it can be easily seen that if the set K is a robust controlled invariant for the system Σ and constraint set (X, U, D) then from Proposition 3 and using the fact that $\max(K) \subseteq K$ one gets (5). Now assume that (5) holds and let us show that (4) holds. Consider $x \in K$, we have the existence of $x' \in \max(K)$ such that $x \leq_X x'$. Then, from (5) we have the existence of $u \in U$ such that $f(x', u, D) \subseteq K$. Hence, one gets $f(x, u, D) \subseteq f(\downarrow x', u, D) \subseteq \downarrow f(x', u, D) \subseteq \downarrow K \subseteq K$, where the second inclusion comes from (i) in Proposition 2 and the last inclusion comes from (ii) in Theorem 5. Hence, condition (4) holds, and the set K is a robust controlled invariant for the system Σ and the constraint set (X, U, D) .

proof of (ii): From (i) and since the system Σ is DSM, to show (ii), it is sufficient to show the equivalence between conditions (5) and (6). Since $D_{\max} \subseteq D$, one gets directly that (5) implies (6). Let us show the converse result, consider $x \in \max(K)$, from (6) one has the existence of $u \in U$ such that $f(x, u, D_{\max}) \subseteq K$. Hence, one gets that $f(x, u, D) \subseteq f(x, u, \downarrow D_{\max}) \subseteq \downarrow f(x, u, D_{\max}) \subseteq \downarrow K \subseteq K$, where the first inclusion comes from the fact that $D \subseteq \downarrow D_{\max}$, the second inclusion comes from (iii) in Proposition 2 and the last inclusion comes from (iii) in Theorem 5. Hence, condition (5) holds.

proof of (iii): From (i) and since the system Σ is CSM, to show (iii), it is sufficient to show the equivalence between conditions (5) and (7). Since $U_{\min} \subseteq U$, one gets directly that (7) implies (5). Let us show the converse result, consider $x \in \max(K)$, from (5) one has the existence of $u \in U$ such that $f(x, u, D) \subseteq K$. Moreover, we have the existence of $u' \in U_{\min}$ such that $u' \leq_U u$. Hence, one gets that $f(x, u', D) \subseteq f(x, \downarrow u, D) \subseteq \downarrow f(x, u, D) \subseteq \downarrow K \subseteq K$, where the second inclusion comes from (ii) in Proposition 2 and the last inclusion comes from (iv) in Theorem 5. Hence, condition (5) holds.

proof of (iv): The proof is a direct conclusion from (ii), (iii) and the fact that any CDSM system is a CSM and DSM system. \square

Proof of Proposition 7 We only provide a proof of (i), the proof of (ii) can be derived similarly. Assume that x_0 is closed loop lower feasible w.r.t the constraint set (X, U, D) ; hence, then there exist a controller $\kappa : X \rightarrow U$ and $N \in \mathbb{N}_{>0}$ such

that conditions (9) and (10) are satisfied. To show the result we use the characterization of controlled invariants in Proposition 3. Consider $x \in K$, we have the existence of $p \in \{0, 1, \dots, N-1\}$ such that $x \in \downarrow \Phi_\kappa(p, x_0, D)$. Hence, there exists $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ such that $x \leq_{\mathcal{X}} \Phi_\kappa(p, x_0, \mathbf{d})$. Consider $u = \kappa(\Phi_\kappa(p, x_0, \mathbf{d}))$ and any $d = \mathbf{d}(p) \in D$, using the fact that the system Σ is SM we have $f(x, u, d) \in \downarrow f(\Phi_\kappa(p, x_0, \mathbf{d}), \kappa(\Phi_\kappa(p, x_0, \mathbf{d})), \mathbf{d}(p)) = \downarrow \Phi_\kappa(p+1, x_0, \mathbf{d})$. Hence, we have two cases

- If $p \in \{0, 1, \dots, N-2\}$, then one has $f(x, u, d) \subseteq \downarrow \Phi_\kappa(p+1, x_0, \mathbf{d}) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_\kappa(k, x_0, D) = K$.
- If $p = N-1$, then one has from (10) that $f(x, u, d) \subseteq \downarrow \Phi_\kappa(p+1, x_0, \mathbf{d}) \subseteq \downarrow \Phi_\kappa(N, x_0, D) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_\kappa(k, x_0, D) = K$

Hence, it follows from Proposition 3 that the set K is a controlled invariant for the system Σ and constraint set (X, U, D) . \square

Proof of Lemma 4 Consider $x \in \Phi(k, x_0, \mathbf{u}, D)$, we have the existence of $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow D$ such that $x = \Phi(k, x_0, \mathbf{u}, \mathbf{d})$. Moreover, we have the existence of $\mathbf{d}_{\max} : \mathbb{N}_{\geq 0} \rightarrow D_{\max}$ such that $\mathbf{d} \leq_{\mathcal{D}^w} \mathbf{d}_{\max}$. Then, using the fact that the system Σ is DSM, one has $x = \Phi(k, x_0, \mathbf{u}, \mathbf{d}) \subseteq \Phi(k, x_0, \mathbf{u}, \mathbf{d}_{\max}) \in \Phi(k, x_0, \mathbf{u}, D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$, which implies from Lemma 1 that $\Phi(k, x_0, \mathbf{u}, D) \subseteq \downarrow \Phi(k, x_0, \mathbf{u}, D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$. \square

Proof of Proposition 8 Necessary condition: From the open-loop feasibility of x_0 w.r.t the constraint set (X, U, D) we have the existence of a control input $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow U$ and $N \in \mathbb{N}_{>0}$ such that (11) and (12) hold. Using (11) and the fact that $D_{\max} \subseteq D$, we have that $\Phi(k, x_0, \mathbf{u}, D_{\max}) \subseteq \Phi(k, x_0, \mathbf{u}, D) \subseteq X$ for all $0 \leq k \leq N-1$. Let us show that the second condition holds, we have

$$\begin{aligned} \Phi(N, x_0, \mathbf{u}, D_{\max}) &\subseteq \Phi(N, x_0, \mathbf{u}, D) \\ &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D) \\ &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D_{\max}) \end{aligned}$$

where the first inclusion follows from the fact that $D_{\max} \subseteq D$, the second inclusion comes from (12) and the last inclusion comes from Lemma 4.

Sufficient condition: From the feasibility of x_0 w.r.t the constraint set (X, U, D_{\max}) we have the existence of a control input $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow U$ and $N \in \mathbb{N}_{>0}$ such that the following conditions are satisfied

$$\Phi(k, x_0, \mathbf{u}, D_{\max}) \subseteq X, \quad \forall k \in \{1, 2, \dots, N-1\} \quad (\text{A3})$$

and

$$\Phi(N, x_0, \mathbf{u}, D_{\max}) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D_{\max}) \quad (\text{A4})$$

First, we have $\Phi(k, x_0, \mathbf{u}, D) \subseteq \Phi(k, x_0, \mathbf{u}, \downarrow D_{\max}) \downarrow \Phi(k, x_0, \mathbf{u}, D_{\max}) \subseteq \downarrow X = X$, for all $0 \leq k \leq N-1$, where the first inequality comes from Lemma 4, the second inequality follows from (A3) and the last inequality comes from the lower closedness of the set X . To show that (12) holds, we have the following

$$\begin{aligned} \Phi(N, x_0, \mathbf{u}, D) &\subseteq \downarrow \Phi(N, x_0, \mathbf{u}, D_{\max}) \\ &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D_{\max}) \\ &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D) \end{aligned}$$

where the first inclusion comes from Lemma 4, the second inclusion comes from the fact that x_0 is feasible w.r.t the constraint set (X, U, D_{\max}) and the last inclusion follows from the fact that $D_{\max} \subseteq D$. \square

Proof of Proposition 9 Consider $x_0 \in X$, first since $U_{\min} \subseteq U$ one directly has that x_0 is open-loop feasible w.r.t the constraint set (X, U, D) if x_0 is open-loop feasible w.r.t the constraint set (X, U_{\min}, D) . Let us show the second implication. Since x_0 is open-loop feasible w.r.t the constraint set (X, U, D) , one gets the existence of an input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that

$$\Phi(k, x_0, \mathbf{u}, D) \subseteq X, \quad \forall k \in \{1, 2, \dots, N-1\} \quad (\text{A5})$$

and

$$\Phi(N, x_0, \mathbf{u}, D) \subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi(k, x_0, \mathbf{u}, D) \quad (\text{A6})$$

Now consider any input trajectory $\underline{\mathbf{u}} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}_{\min}$ such that $\underline{\mathbf{u}} \leq_{\mathcal{U}^w} \mathbf{u}$. Using the fact that the system Σ is CDSM and since the set X is lower closed, it follows from (A5) that for all $k \in \{1, 2, \dots, N-1\}$

$$\Phi(k, x_0, \underline{\mathbf{u}}, D) \subseteq \Phi(k, x_0, \downarrow \mathbf{u}, D) \subseteq \downarrow \Phi(k, x_0, \mathbf{u}, D) \subseteq \downarrow X \subseteq X \quad (\text{A7})$$

and condition (9) in Definition 7 is satisfied.

Now consider $x \in \Phi(N, x_0, \underline{\mathbf{u}}, D)$ and let us show that there exists $k \in \{0, \dots, N-1\}$ and $\bar{x} \in \Phi(k, x_0, \underline{\mathbf{u}}, D)$ such that $x \leq \bar{x}$.

For $x \in \Phi(N, x_0, \underline{\mathbf{u}}, D)$, we have the existence of a trajectory $\mathbf{d} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{D}$ such that $x = \Phi(N, x_0, \underline{\mathbf{u}}, \mathbf{d})$. Moreover, from (A6) we have for $\Phi(N, x_0, \underline{\mathbf{u}}, \mathbf{d})$ the existence of a trajectory $\bar{\mathbf{d}} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{D}$ with $\mathbf{d} \leq_{\mathcal{D}^w} \bar{\mathbf{d}}$ and $k \in \{1, \dots, N-1\}$ such that

$$\Phi(N, x_0, \mathbf{u}, \mathbf{d}) \leq \Phi(k, x_0, \mathbf{u}, \bar{\mathbf{d}}). \quad (\text{A8})$$

Moreover, since the system Σ is CDSM, one has that

$$\Phi(k, x_0, \underline{\mathbf{u}}, \mathbf{d}) \leq \Phi(k, x_0, \mathbf{u}, \mathbf{d}). \quad (\text{A9})$$

Define $\varepsilon \in \mathbb{R}_{\geq 0}^n$ as $\varepsilon := \Phi(k, x_0, \mathbf{u}, \bar{\mathbf{d}}) - \Phi(k, x_0, \underline{\mathbf{u}}, \bar{\mathbf{d}})$. We have that

$$\begin{aligned} x &= \Phi(N, x_0, \underline{\mathbf{u}}, \mathbf{d}) \leq \Phi(N - k, \Phi(k, x_0, \mathbf{u}, \mathbf{d}), \underline{\mathbf{u}}, \mathbf{d}) - \varepsilon \\ &\leq \Phi(N, x_0, \mathbf{u}, \mathbf{d}) - \varepsilon \leq \Phi(k, x_0, \mathbf{u}, \bar{\mathbf{d}}) - \varepsilon = \Phi(k, x_0, \underline{\mathbf{u}}, \bar{\mathbf{d}}) \end{aligned}$$

where the first follow from the application of (15) to the inequality in (A9) $N - k$ times, the second inequality comes from the fact that the system Σ is CDSM, the third inequality comes from (A8) and the last equality comes from the definition of ε . Hence, we have the existence of $k \in \{0, \dots, N - 1\}$ and $\bar{x} = \Phi(k, x_0, \underline{\mathbf{u}}, \bar{\mathbf{d}}) \in \Phi(k, x_0, \underline{\mathbf{u}}, D)$ such that $x \leq \bar{x}$. Hence, condition (10) is satisfied and x_0 is open-loop feasible w.r.t the constraint set (X, U_{\min}, D) . \square

Proof of Proposition 10 Assume that $x_0 \in X$ is open-loop feasible w.r.t the constraint set (X, U, D) . We have the existence of a control input $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that (11) and (12) are satisfied. Consider the controller $\kappa : \mathcal{X} \rightarrow \mathcal{U}$ defined as follows: for $k \in \{1, 2, \dots, N - 1\}$, $\kappa(\Phi(k, x_0, \mathbf{u}, D)) = \mathbf{u}(k)$, and $\kappa(\Phi(k, x_0, \mathbf{u}, D)) \in \mathcal{U}$ for all $k \geq N$. Using the controller κ , one can easily check that (9) and (10) hold. Hence, x_0 is closed-loop feasible w.r.t the constraint set (X, U, D) .

Let us now show the converse result under the assumption that $D = \{\bar{d}\}$. Assume that $x_0 \in X$ is closed-loop feasible w.r.t the constraint set (X, U, D) . We have the existence of a controller $\kappa : \mathcal{X} \rightarrow \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that (9) and (10). Consider the control input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \rightarrow \mathcal{U}$ defined as follows: for $k \in \{1, 2, \dots, N - 1\}$, $\mathbf{u}(k) = \kappa(\Phi(k, x_0, \mathbf{u}, \bar{d}))$ and $\mathbf{u}(k) \in \mathcal{U}$ for all $k \geq N$. Using the control input trajectory \mathbf{u} , one can easily check that (11) and (12) hold. Hence, x_0 is open-loop feasible w.r.t the constraint set (X, U, D) . The converse result can also be obtained when the system Σ is DSM and $\text{card}(D_{\max}) = 1$, by using the equivalence between open-loop feasibility w.r.t the constraint sets (X, U, D) and (X, U, D_{\max}) for the case of DSM systems, as shown in Proposition 8. \square

Proof of Theorem 11 Since the set D is compact and f is upper semicontinuous on its first and third arguments, one has that the set valued map $F : X \times U \rightrightarrows X$ defined by $F(x, u) := f(x, u, D)$ is upper semicontinuous on x and for any $u \in U$. Moreover, from continuity of f and compactness of D we have that $\Phi(N - 1, x_0, \mathbf{u}, D)$ is compact. Hence, for $\beta_N = \min(\varepsilon_N, \gamma) > 0$, where $\gamma > 0$ is defined in (ii), we have from Lemma 5 the existence of $\varepsilon_{N-1} > 0$ such that

$$\begin{aligned} F(\mathcal{B}_{\varepsilon_{N-1}}(\Phi(N - 1, x_0, \mathbf{u}, D), \mathbf{u}(N - 1))) \\ \subseteq \mathcal{B}_{\beta_N}(F(\Phi(N - 1, x_0, \mathbf{u}, D), \mathbf{u}(N - 1))) \\ \subseteq \mathcal{B}_{\beta_N}(\Phi(N, x_0, \mathbf{u}, D)). \end{aligned}$$

Let us define the sequences $\varepsilon_k > 0, k \in \{1, \dots, N - 2\}$ and $\beta_k > 0, k \in \{1, \dots, N - 1\}$, iteratively as follows: for $k \in \{N - 1, N - 2, \dots, 1\}$, $\beta_k = \min\{\varepsilon_k, \gamma\}$, where $\gamma > 0$ is

defined in (ii), and ε_{k-1} is such that $F(\mathcal{B}_{\varepsilon_{k-1}}(\Phi(k-1, x_0, \mathbf{u}))) \subseteq \mathcal{B}_{\beta_k}(F(\Phi(k, x_0, \mathbf{u})))$. The existence of such ε_{k-1} , $k \in \{N-1, N-2, \dots, 1\}$ is guaranteed from Lemma 5 using the upper semicontinuity of the map F and the fact that $\Phi(k, x_0, \mathbf{u}, D)$ is compact for all $k \in \{1, 2, \dots, N\}$. Hence, one gets

$$\begin{aligned}
 \Phi(N, \mathcal{B}_{\beta_0}(x_0), \mathbf{u}) &\subseteq \Phi(N, \mathcal{B}_{\varepsilon_0}(x_0), \mathbf{u}) \\
 &\subseteq \Phi(N-1, \mathcal{B}_{\beta_1}(\Phi(1, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \Phi(N-1, \mathcal{B}_{\varepsilon_1}(\Phi(1, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \Phi(N-2, \mathcal{B}_{\beta_2}(\Phi(2, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \Phi(N-2, \mathcal{B}_{\varepsilon_2}(\Phi(2, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \dots \\
 &\subseteq \Phi(1, \mathcal{B}_{\beta_{N-1}}(\Phi(N-1, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \Phi(1, \mathcal{B}_{\varepsilon_{N-1}}(\Phi(N-1, x_0, \mathbf{u}), \mathbf{u})) \\
 &\subseteq \mathcal{B}_{\varepsilon_N}(\Phi(N, x_0, \mathbf{u})) \\
 &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_k(k, x_0, \mathbf{u}, D) \tag{A10}
 \end{aligned}$$

where the last inclusion comes from (i). Now let $\beta = \min \beta_i$, $i = \{1, 2, \dots, N-1\}$ consider $x_1 \in \{\uparrow x_0\} \cap \mathcal{B}_\beta(x_0)$. We have

$$\begin{aligned}
 \Phi(N, x_1, \mathbf{u}) &\subseteq \Phi(N, \mathcal{B}_\beta(x_0), \mathbf{u}) \\
 &\subseteq \Phi(N, \mathcal{B}_{\beta_0}(x_0), \mathbf{u}) \\
 &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_k(k, x_0, \mathbf{u}, D) \\
 &\subseteq \downarrow \bigcup_{0 \leq k \leq N-1} \Phi_k(k, x_1, \mathbf{u}, D).
 \end{aligned}$$

Where the second inclusion comes from (A10) and the last inclusion follows from the fact that Σ is a SM system. Hence, condition (12) of Definition 7 is satisfied.

Moreover, we have from (ii) that for all $k \in \{0, 1, \dots, N-1\}$

$$\begin{aligned}
 \Phi(k, x_1, \mathbf{u}) &\subseteq \Phi(k, \mathcal{B}_{\beta_{N-k}}(x_0), \mathbf{u}) \\
 &\subseteq \mathcal{B}_{\beta_{N-k+1}}(\Phi(k, x_0, \mathbf{u}, D)) \\
 &\subseteq \mathcal{B}_\gamma(\Phi(k, x_1, \mathbf{u}, D)) \subseteq X.
 \end{aligned}$$

Hence, condition (12) of Definition 7 is satisfied, and any $x_1 \in \{\uparrow x_0\} \cap \mathcal{B}_\beta(x_0)$ is feasible. Now, for the case when the map f is L -Lipschitz on its first argument, it follows that the set valued map $F : X \times U \rightrightarrows X$ defined by $F(x, u) := f(x, u, D)$ is L -Lipschitz on its first argument. Hence, the sequences $\varepsilon_k > 0$, $k \in \{1, \dots, N-1\}$ and $\beta_k > 0$, $k \in \{1, \dots, N\}$, can be constructed according to Lemma 5 iteratively as follows: for $k \in \{N-1, N-2, \dots, 1\}$, $\beta_k = \min\{\varepsilon_k, \gamma\}$, where $\gamma > 0$ is defined in (ii) and $\varepsilon_{k-1} = \frac{\beta_k}{L}$. hence, the result holds with $\beta = \min \beta_i$, $i \in \{1, \dots, N\}$. \square

Proof of Proposition 12 First, since the map $f : \mathcal{X} \times \mathcal{U} \times \mathcal{D}$ describing the system Σ is lower semicontinuous on its first argument and the set of control inputs U and disturbance inputs D are compact, one has from Proposition 4 that $\text{dom}(\kappa)$ is closed and $\partial(\text{dom}(\kappa)) \subseteq \text{dom}(\kappa)$.

Since κ is a maximal invariance controller, it follows directly that $\Phi_\kappa(k, x_0, D) \subseteq \text{dom}(\kappa)$ for all $k \in \mathbb{N}_{\geq 0}$. The latter property implies that either $\Phi_\kappa(k, x_0, D) \cap \partial(\text{dom}(\kappa)) \neq \emptyset$ for all $k \in \mathbb{N}_{\geq 0}$, which is consistent with (i), or there exists $p \in \mathbb{N}_{>0}$ such that $\Phi_\kappa(p, x_0, D) \subseteq \text{Int}(\text{dom}(\kappa))$. Assume w.l.o.g that p is the minimal integer such that $\Phi_\kappa(p, x_0, D) \subseteq \text{Int}(\text{dom}(\kappa))$. Let us show, by contradiction, that (ii) holds. Assume that $\Phi_\kappa(p-1, x_0, D) \cap (\partial(\text{dom}(\kappa)) \setminus \partial X) \neq \emptyset$ and let $z \in \Phi_\kappa(p-1, x_0, D) \cap (\partial(\text{dom}(\kappa)) \setminus \partial X)$. Since $\text{Int}(\text{dom}(\kappa))$ is open, we have the existence of $\varepsilon > 0$ such that $\mathcal{B}_\varepsilon(\Phi_\kappa(p, x_0, D)) \subseteq \text{Int}(\text{dom}(\kappa))$. Moreover, since the set D is compact and f is upper semicontinuous on its first and third arguments, one has that the set valued map $F : X \times U \rightrightarrows X$ defined by $F(x, u) := f(x, u, D)$ is upper semicontinuous on x . Since $z \in \partial(\text{dom}(\kappa))$, for $\varepsilon > 0$ and from the upper semicontinuity of F we have the existence of an $\eta > 0$ such that

$$\begin{aligned} F(\mathcal{B}_\eta(z), \kappa(z)) &\subseteq \mathcal{B}_\varepsilon(F(z, \kappa(z))) \\ &\subseteq \mathcal{B}_\varepsilon(F(\Phi_\kappa(p-1, x_0, D), \kappa(z))) \\ &= \mathcal{B}_\varepsilon(f(\Phi_\kappa(p-1, x_0, D), \kappa(z), D)) \\ &= \mathcal{B}_\varepsilon(\Phi_\kappa(p, x_0, D)) \subseteq \text{Int}(\text{dom}(\kappa)). \end{aligned}$$

Hence, there exists $z' \in (X \setminus \text{dom}(\kappa)) \cap \mathcal{B}_\eta(z)$ and $u' = \kappa(z) \in U$ such that

$$F(z', u') = f(z', \kappa(z), D) \subseteq F(\mathcal{B}_\eta(z), \kappa(z)) \subseteq \text{Int}(\text{dom}(\kappa)). \quad (\text{A11})$$

The last property contradicts the maximality of the set $\text{dom}(\kappa)$. Hence, we have necessarily that $\Phi_\kappa(p-1, x_0, D) \cap (\partial(\text{dom}(\kappa)) \setminus \partial X) = \emptyset$. Finally, since $\Phi_\kappa(p-1, x_0, D) \subseteq \text{dom}(\kappa)$ and $\Phi_\kappa(p-1, x_0, D) \not\subseteq \text{Int}(\text{dom}(\kappa))$, one gets $\Phi_\kappa(p-1, x_0, D) \cap \partial X \neq \emptyset$, which implies (ii). \square

Auxiliary result:

Lemma 5 Consider an upper semicontinuous set-valued map $F : \mathcal{X} \rightrightarrows \mathbb{R}^n$ and consider a compact set $Z \subseteq \mathcal{X}$. For all $\varepsilon > 0$, there exists $\eta > 0$ such that $F(\mathcal{B}_\eta(Z) \cap \mathcal{X}) \subseteq \mathcal{B}_\varepsilon(F(Z))$. Moreover, when the map F is L -Lipschitz on \mathcal{X} , for $L > 0$, the property holds for any $\eta \leq \varepsilon/L$.

Proof Consider $\varepsilon > 0$ and $x \in Z$. Since F is upper semicontinuous, we have the existence of $\eta_x > 0$ such that $F(\mathcal{B}_{\eta_x}(x)) \cap \mathcal{X} \subseteq \mathcal{B}_\varepsilon(F(x))$. Let $\eta = \min_{x \in Z} \eta_x$. It follows from the compactness of the set Z that $\eta > 0$. Hence, one gets:

$$\begin{aligned} F(\mathcal{B}_\eta(Z) \cap \mathcal{X}) &= \bigcup_{x \in Z} F(\mathcal{B}_\eta(x) \cap \mathcal{X}) \\ &\subseteq \bigcup_{x \in Z} F(\mathcal{B}_{\eta_x}(x) \cap \mathcal{X}) \end{aligned}$$

$$\begin{aligned}
&\subseteq \bigcup_{x \in Z} \mathcal{B}_\varepsilon(F(x)) \\
&= \mathcal{B}_\varepsilon(F(Z)).
\end{aligned}$$

The last result follows immediately from the fact that the map F is L -Lipschitz, since

$$F(\mathcal{B}_{\frac{\varepsilon}{L}}(Z) \cap \mathcal{X}) \subseteq \mathcal{B}_\varepsilon(F(Z)).$$

□

References

1. Blanchini F, Miani S (2008) Set-theoretic methods in control. Springer, Berlin
2. Aubin J-P (2009) Viability theory. Springer, Berlin
3. Nilsson P, Hussien O, Chen Y, Balkan A, Rungger M, Ames A, Grizzle J, Ozay N, Peng H, Tabuada P (2014) Preliminary results on correct-by-construction control software synthesis for adaptive cruise control. In: IEEE conference on decision and control, pp 816–823
4. Smith SW, Saoud A, Arcak M (2021) Monotonicity-based symbolic control for safety in driving scenarios. IEEE Control Syst Lett 6:830–835
5. Saoud A, Girard A, Fribourg L (2018) Contract based design of symbolic controllers for vehicle platooning. In: Proceedings of the 21st international conference on hybrid systems: computation and control (part of CPS Week), pp 277–278
6. Tomlin C, Pappas GJ, Sastry S (1998) Conflict resolution for air traffic management: a study in multiagent hybrid systems. IEEE Trans Autom Control 43(4):509–521
7. Wang L, Ames AD, Egerstedt M (2017) Safety barrier certificates for collisions-free multirobot systems. IEEE Trans Rob 33(3):661–674
8. Zanchettin AM, Ceriani NM, Rocco P, Ding H, Matthias B (2015) Safety in human-robot collaborative manufacturing environments: metrics and control. IEEE Trans Autom Sci Eng 13(2):882–893
9. Zonetti D, Saoud A, Girard A, Fribourg L (2019) A symbolic approach to voltage stability and power sharing in time-varying dc microgrids. In: 2019 18th European control conference (ECC), pp 903–909. IEEE
10. Rakovic S, Grieder P, Kvasnica M, Mayne D, Morari M (2004) Computation of invariant sets for piecewise affine discrete time systems subject to bounded disturbances. In: 2004 43rd IEEE conference on decision and control (CDC)(IEEE Cat. No. 04CH37601), vol 2, pp 1418–1423. IEEE
11. Anevlavis T, Liu Z, Ozay N, Tabuada P (2021) Controlled invariant sets: implicit closed-form representations and applications. arXiv preprint [arXiv:2107.08566](https://arxiv.org/abs/2107.08566)
12. Korda M, Henrion D, Jones CN (2014) Convex computation of the maximum controlled invariant set for polynomial control systems. SIAM J Control Optim 52(5):2944–2969
13. Sassi MAB, Girard A (2012) Computation of polytopic invariants for polynomial dynamical systems using linear programming. Automatica 48(12):3114–3121
14. Saoud A, Sanfelice RG (2021) Computation of controlled invariants for nonlinear systems: application to safe neural networks approximation and control. IFAC-PapersOnLine 54(5):91–96
15. Tabuada P (2009) Verification and control of hybrid systems: a symbolic approach. Springer, Berlin
16. Saoud A (2019) Compositional and efficient controller synthesis for cyber-physical systems. Ph.D. thesis, Université Paris Saclay
17. Abate A, Tiwari A, Sastry S (2009) Box invariance in biologically-inspired dynamical systems. Automatica 45(7):1601–1610
18. Meyer P-J, Girard A, Witrant E (2016) Robust controlled invariance for monotone systems: application to ventilation regulation in buildings. Automatica 70:14–20
19. Ivanova E, Saoud A, Girard A (2022) Lazy controller synthesis for monotone transition systems and directed safety specifications. Automatica 135:109993
20. Sadraiddini S, Belta C (2016) Safety control of monotone systems with bounded uncertainties. In: 2016 IEEE 55th conference on decision and control (CDC), pp 4874–4879. IEEE

21. Legriel J, Guernic CL, Cotton S, Maler O (2010) Approximating the Pareto front of multi-criteria optimization problems. In: International conference on tools and algorithms for the construction and analysis of systems. Springer, pp 69–83
22. Saoud A, Arcak M (2022) Characterizations and computation of controlled invariants for monotone dynamical systems. In: IEEE conference on decision and control (CDC). Submitted
23. Davey BA, Priestley HA (2002) Introduction to lattices and order. Cambridge University Press, Cambridge
24. Aubin J-P, Frankowska H (2009) Set-valued analysis. Springer, Berlin
25. Smith HL (2008) Monotone dynamical systems: an introduction to the theory of competitive and cooperative systems vol 41. American Mathematical Society
26. Angeli D, Sontag ED (2003) Monotone control systems. *IEEE Trans Autom Control* 48(10):1684–1698
27. Meyer P-J, Girard A, Witrant E (2017) Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Trans Autom Control* 63(6):1835–1841
28. Coogan S, Arcak M, Belta C (2017) Formal methods for control of traffic flow: automated control synthesis from finite-state transition models. *IEEE Control Syst Mag* 37(2):109–128
29. Zonetti D, Saoud A, Girard A, Fribourg L (2019) Decentralized monotonicity-based voltage control of dc microgrids with zip loads. *IFAC-PapersOnLine* 52(20):139–144
30. DasGupta B, Enciso GA, Sontag E, Zhang Y (2007) Algorithmic and complexity results for decompositions of biological networks into monotone subsystems. *Biosystems* 90(1):161–178
31. Rungger M, Tabuada P (2017) Computing robust controlled invariant sets of linear systems. *IEEE Trans Autom Control* 62(7):3665–3670
32. Rakovic SV, Baric M (2010) Parameterized robust control invariant sets for linear systems: theoretical advances and computational remarks. *IEEE Trans Autom Control* 55(7):1599–1614
33. Tendulkar P (2014) Mapping and scheduling on multi-core processors using smt solvers. Ph.D. thesis, Universite de Grenoble I-Joseph Fourier
34. Al Khatib M, Girard A, Dang T (2017) Stability verification and timing contract synthesis for linear impulsive systems using reachability analysis. *Nonlinear Anal Hybrid Syst* 25:211–226
35. Zonetti D, Saoud A, Girard A, Fribourg L (2019) A symbolic approach to voltage stability and power sharing in time-varying DC microgrids. In: European control conference, pp 903–909
36. Devonport A, Arcak M (2020) Data-driven reachable set computation using adaptive Gaussian process classification and Monte Carlo methods. In: 2020 American control conference (ACC), pp 2629–2634. IEEE

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.