Characterizations and Computation of Controlled Invariants for Monotone Dynamical Systems

Adnane Saoud
Murat Arcak

Electrical Engineering and Computer Sciences
University of California, Berkeley

Technical Report No. UCB/EECS-2022-2
http://www2.eecs.berkeley.edu/Pubs/TechRpts/2022/EECS-2022-2.html

March 31, 2022

Characterizations and Computation of Controlled Invariants for Monotone Dynamical Systems

Adnane Saoud[1] and Murat Arcak[2]

***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 an algorithmic approach to the computation of controlled invariants. Finally, we illustrate the proposed approach on an adaptive cruise control problem.**

I. INTRODUCTION

The concept of controlled invariance plays an important role in control theory [1], this concept reflects the ability to control the system so that all trajectories initialized in a set remain there for all future time. Formulation of the concept of controlled invariance of a set are presented in [1] for discrete-time systems. 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 [2] for piecewise affine systems and more recently in [3] for linear systems systems. Controlled invariants for polynomial systems have been explored using linear programming in [4] and semidefinite programming in [5]. For general nonlinear systems, interval controlled invariants have been investigated in [6] Other approaches have been proposed recently using symbolic control techniques [7], [8]. In this paper, we are interested in the study of 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 different types characterization on the structure of the robust controlled invariants. Then we present an algorithmic procedure allowing to compute robust controlled invariants using the 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 and for the particular class of sets given by intervals in [9]. In [10], the authors used symbolic control techniques to compute robust controlled invariants for discrete time monotone dynamical systems. In spirit, the closest work in the literature is [11] where the authors introduce a notion of s-sequence to characterize a controlled invariant of the system. Our approach differs from the one proposed in [11] in several directions:

- While the authors in [11] deal with the particular class of disturbance state monotone systems, we present a general framework for different classes of monotone systems;
- In [11], the authors focus on open loop strategies. In our paper, we present results for both open loop and control loop strategies. moreover, we provide conditions under which open-loop and closed-loop strategies are equivalent;
- We present new characterizations of the structure of the robust controlled invariants for different classes of monotone dynamical systems;
- Our algorithmic procedure to compute robust controlled invariants is different from the one in [11] and relies on tools from multidimensional binary search algorithms used in multi-objective optimization [12].

The remainder of this paper is organized as follows. In Section III we introduce the class of systems we consider. Section IV introduces the concept of robust controlled invariants. In Section V and VI, we present different characterizations of robust controlled invariants. Section VII presents an algorithm to compute controlled invariants. Finally, Section V presents numerical results validating the merits of the proposed approach.

a) Notation: The symbols $\mathbb{N}$, $\mathbb{N}_{>0}$, and $\mathbb{R}$ 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 $f : \mathbb{R}^n \to \mathbb{R}^m$, $domf := \{x \in \mathbb{R}^n : f(x) \text{ is well defined}\}$. Given a nonempty set K, $Int(K)$ denotes it interior, $\mathrm{cl}(K)$ denotes its closure, ∂K denotes its boundary and $\overline{K}$ its complement. For a set K, the operator (K) randomly selects a unique element from the set K. The Euclidean norm is denoted by $\|.\|$. 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 $K \subseteq \mathbb{R}^n$, $\mathcal{B}_\varepsilon(K) = \cup_{x \in K} \mathcal{B}_\varepsilon(x)$.

II. PRELIMINARIES

A. 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)

[1] Adnane Saoud is with Laboratoire des Signaux et Systèmes, CentraleSupélec, Université Paris Saclay, Gif-sur-Yvette, France. adnane.saoud@centralesupelec.fr

[2]Murat Arcak are with the Dept. of Electrical Engineering and Computer Sciences, University of California, Berkeley, USA arcak@berkeley.edu

This work was supported by the grants NSF ECCS-1906164, AFOSR FA9550-21-1-0288, ONR N00014-18-1-2209.

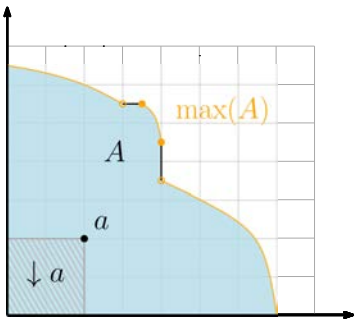

Fig. 1: A lower closed set $A \subseteq \mathbb{R}^2_{\geq 0}$, with the standard ordering, in blue. The set of its maximal elements $\max(A)$ is presented in orange. The lower closure of a point $a \in A$ is presented in dashed gray.

$l_1 \leq_{\mathcal{L}} l_1$, (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 $m = m_0 m_1 \ldots$ and $n = n_1 n_2 \ldots$ holds if and only if $m_k \leq_{\mathcal{L}} n_k$ for all $k \in \mathbb{N}_{\geq 0}$.

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 2.1: 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 2.2: 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 Figure 1. It was shown in [13] that lower and upper-closed sets satisfy the following property.

Proposition 2.3: Let $\mathcal{L}$ be a partially ordered set and consider a collection of subsets $A_i \subseteq \mathcal{L}$, $i \in \{1, 2, \ldots, p\}$. The following holds:

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

(i) If for all $i \in \{1, 2, \ldots, p\}$, 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 using similar approaches.

B. Continuity of Set-Valued Maps

In this section, we recall the following continuity notions for set-valued maps [14].

Definition 2.4: 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 $F(\mathcal{B}_\eta(x)) \cap \mathcal{X}) \subset \mathcal{B}_\varepsilon(F(x))$;.
- 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 $x_1, x_2 \in \mathcal{X}$, $F(x_1) \subseteq \mathcal{B}_{L\|x_1 - x_2\|}(F(x_2))$.

•

C. Discrete-time control systems

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

$$x(k+1) = f(x(k), u(k), d(k)) \tag{1}$$

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 $\Phi(., x_0, \mathbf{u}, \mathbf{d})$ 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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$ and the disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \to \mathcal{D}$. 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 $\kappa : \mathcal{X} \to \mathcal{U}$, the dynamics of the closed-loop system is given by

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

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

III. 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 3.1: 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 distrubance 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 3.2: In this paper, different types of monotonicity are defined with respect to the state, control input and distrubance input. The SM, (DSM and CDSM, respectively) properties correspond to the discrete-time versions of the concept of monotonicity in [15] ([16] and [17], 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 [15] 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 $i, j \in \{1, 2, \ldots, n\}$;
- CSM if $\frac{\partial f_i}{\partial x_j} \geq 0$ and $\frac{\partial f_i}{\partial u_h} \geq 0$ for all $i, j \in \{1, 2, \ldots, n\}$ and for all $h \in \{1, 2, \ldots, m\}$;
- DSM if $\frac{\partial f_i}{\partial x_j} \geq 0$ and $\frac{\partial f_i}{\partial d_h} \geq 0$ for all $i, j \in \{1, 2, \ldots, n\}$ and for all $h \in \{1, 2, \ldots, p\}$;
- 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 $i, j \in \{1, 2, \ldots, n\}$, for all $h \in \{1, 2, \ldots, m\}$ and for all $l \in \{1, 2, \ldots, p\}$.

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 3.3: 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 $\mathbb{R}$.

□

We also have the following equivalent characterizations of the proposed classes of monotone systems. Before stating the result, we give the following auxiliary lemma.

Lemma 3.4: 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 3.5: 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
$$f(\downarrow x, \downarrow u, \downarrow d) \subseteq \downarrow f(x, u, d)$$

□

Proof. 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. ■

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

Lemma 3.6: Consider the system Σ in (1). If the system Σ is CDSM and if the controllers $\kappa_1, \kappa_2 : \mathcal{X} \to \mathcal{U}$ satisfy

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

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

Proof. Consider $x_1^0, x_2^0 \in \mathcal{X}$, with $x_1^0 \leq_{\mathcal{X}} x_2^0$ and $\mathbf{d}_1, \mathbf{d}_2 : \mathbb{N}_{\geq 0} \to \mathcal{D}$ 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 $\mathbf{d}_1 \leq_{D^w} \mathbf{d}_1$ 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, $\Phi_{\kappa_1}(., x_1^0, \mathbf{d}_1) \leq_{\mathcal{X}^w} \Phi_{\kappa_2}(., x_2^0, \mathbf{d}_2)$. ■

IV. 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 4.1: 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 $\kappa : X \to U$, with $dom(\kappa) = K$ and such that for all $x_0 \in K$ and for any disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ the solution of the closed loop system $\Phi_\kappa(., x_0, \mathbf{d}) : \mathbb{N}_{\geq 0} \to \mathcal{X}$ 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). •

Remark 4.2: While the characterization of controlled invariants in Definition 4.1 is the most commonly used in the literature [1], [18], the equivalent characterization below has also been used in the literature [19]. The proof of the equivalence of these characterizations is provided in the Appendix. •

Proposition 4.3: 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:

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

□

Proof. See Appendix. ■

Since the robust controlled invariance property is closed under union, there exists a unique robust controlled invariant that is maximal, in the sense that it contains all the robust controlled invariants.

Definition 4.4: 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 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 $\kappa : X \to U$ satisfying $dom(\kappa) = K$ is said to be a maximal invariance controller for the system Σ and constraint set (X, U, D). •

We have the following auxiliary result characterizing the effect of enlarging the set of control inputs and shrinking the set of disturbance inputs on the robust controlled invariance problem.

Lemma 4.5: 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). □

V. 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.

Proposition 5.1: 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 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 $\mathrm{cl}(K)$ 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.

□

Proof. 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 $\mathrm{cl}(K)$ is a robust controlled invariant for the system Σ and constraint set (X, U, D). Consider $x \in \mathrm{cl}(K) \backslash K$ and assume that for all $u \in U$ we have that $f(x, u, D) \cap \overline{\mathrm{cl}(K)} \neq \emptyset$. Consider $u \in U$, since the set $\overline{\mathrm{cl}(K)}$ is open, we have the existence of $\varepsilon_u > 0$ and $y_{x,u} \in f(x, u, D) \cap \overline{\mathrm{cl}(K)}$ such that $\mathcal{B}_{\varepsilon_u}(y_{x,u}) \subseteq \overline{\mathrm{cl}(K)}$. Since, the set D is compact and f is lower semicontinuous on its first argument, one has that

[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 $k \in \mathbb{N}_{\geq 0}$.

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 $y_{z,u} \in \mathcal{B}_{\varepsilon_u}(y_{x,u}) \subseteq \overline{\mathrm{cl}(K)}$. 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 $z \in \mathit{Int}(K) \cap \mathcal{B}_\eta(x)$ and for any $u \in U$, we have the existence of $y_{z,u} \in F(z,u)$ satisfying $y_{z,u} \in \overline{\mathrm{cl}(K)}$, which contradicts the robust controlled invariance of the set K. Hence, the set $\mathrm{cl}(K)$ 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 $\mathrm{cl}(K)$ 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 $\mathrm{cl}(K) = K$. ∎

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 5.2: 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 and 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 the and constraint set $(X,U_{\min},D_{\max})$, where $U_{\min} = \min(U)$ and $D_{\max} = \max(D)$.*

□

Proof. 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 4.3. 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 4.3 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 4.3. 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 controlled invariant for the system Σ and constraint set (X,U,D) and let $\overline{K}$ be the maximal 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 4.5 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 4.3 to the following condition:

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

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 3.5 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 controlled invariant for the system Σ and constraint set (X,U,D) and let $\underline{K}$ be the maximal controlled invariant for the system Σ and the constraint set $(X,U_{\min},D)$. First, since $U_{\min} \subseteq U$, we have from Lemma 4.5 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 4.3 to the following condition:

$$\forall x \in K,\ \exists u \in U_{\min} \quad \text{s.t} \quad f(x,u,D) \subseteq K. \tag{6}$$

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 bellow we have the existence of $u' \in U_{\min}$ such that $u' \leq_{\mathcal{U}} u$. Since the system Σ is CSM, one has from (iii) in Proposition 3.5 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.

■

The result in (ii) states that for SM systems, the maximal 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 5.3: 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, 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:

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

(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:

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

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:

$$\forall x \in \max(K),\ \exists u \in U_{\min} \quad s.t \quad f(x,u,D) \subseteq K, \tag{9}$$

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:

$$\forall x \in \max(K),\ \exists u \in U_{\min} \quad s.t \quad f(x,u,D_{\max}) \subseteq K, \tag{10}$$

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

□

Proof. 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 4.3 and using the fact that $\max(K) \subseteq K$ one gets (7). Now assume that (7) holds and let us show that (4) holds. Consider $x \in K$, we have the existence of $x' \in \max(K)$ such that $x \leq_{\mathcal{X}} x'$. Then, from (7) 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 3.5 and the last inclusion comes from (ii) in Theorem 5.2. 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 (7) and (8). Since $D_{\max} \subseteq D$, one gets directly that (7) implies (8). Let us show the converse result, consider $x \in \max K$, from (8) 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 3.5 and the last inclusion comes from (iii) in Theorem 5.2. Hence, condition (7) holds.

proof of (iii): From (ii) and since the system Σ is CSM, to show (iii), it is sufficient to show the equivalence between conditions (7) and (9). Since $U_{\min} \subseteq U$, one gets directly that (9) implies (7). Let us show the converse result, consider $x \in \max K$, from (7) 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 $u' \leq_{\mathcal{U}} u$. 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 3.5 and the last inclusion comes from (iv) in Theorem 5.2. Hence, condition (7) 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. ■

Proposition 5.3 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 equation (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.

VI. 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 feasibiliy.

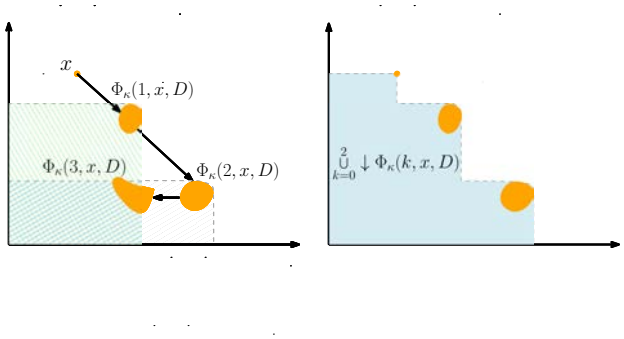

Fig. 2: Illustration of the concept of closed-loop feasibility. Left: the 3-step reachable set from the initial condition x for a system Σ. Note that $\Phi_\kappa(3,x,D) \subseteq\downarrow \Phi_\kappa(1,x,D) \bigcup \downarrow \Phi_\kappa(2,x,D)$. Right: The set $\downarrow \bigcup_{0\leq k\leq 2} \Phi_\kappa(k,x_0,D)$ is a robust controlled invariant of the system Σ in view of Proposition 6.2.

Definition 6.1: 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 $\kappa : X \to U$ and $N \in \mathbb{N}_{>0}$ such that

$$\Phi_\kappa(k,x_0,D) \subseteq X, \quad \forall\, k \in \{0,1,\dots,N-1\} \tag{11}$$

and

$$\Phi_\kappa(N,x_0,D) \subseteq\downarrow \bigcup_{0\leq k\leq N-1} \Phi_\kappa(k,x_0,D) \tag{12}$$

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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that

$$\Phi(k,x_0,\mathbf{u},D) \subseteq X, \quad \forall\, k \in \{1,2,\dots,N-1\} \tag{13}$$

and

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

•

An illustration of the concept of closed-loop feasibility is presented in Figure 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 Figure 2 (right).

Proposition 6.2: 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 exist a controller $\kappa : X \to U$ and $N \in \mathbb{N}_{>0}$ such that the set

$$K =\downarrow \bigcup_{0\leq k\leq N-1} \Phi_\kappa(k,x_0,D) \tag{15}$$

is a 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 exist an input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that the set

$$K =\downarrow \bigcup_{0\leq k\leq N-1} \Phi(k,x_0,\mathbf{u},D) \tag{16}$$

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

□

Proof. 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 $\kappa : X \to U$ and $N \in \mathbb{N}_{>0}$ such that conditions (11) and (12) are satisfied. To show the result we use the characterization of controlled invariants in Proposition 4.3. 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 $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ 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 (12) 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 4.3 that the set K is a 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 have the following auxilliary lemma.

Lemma 6.3: 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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$, we have $\Phi(k,x_0,\mathbf{u},D) \subseteq\downarrow \Phi(k,x_0,\mathbf{u},D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$. □

Proof. Consider $x \in \Phi(k,x_0,\mathbf{u},D)$, we have the existence of $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ such that $x = \Phi(k,x_0,\mathbf{u},\mathbf{d})$. Moreover, we have the existence of $\mathbf{d}_{\max} : \mathbb{N}_{\geq 0} \to D_{\max}$ such that $\mathbf{d} \leq_{\mathcal{D}^w} \mathbf{d}_{\max}$. Then, using the fact that the system Σ is DSM, one has $x = \Phi(k,x_0,\mathbf{u},\mathbf{d}) \leq \Phi(k,x_0,\mathbf{u},\mathbf{d}_{\max}) \in \Phi(k,x_0,\mathbf{u},D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$, which implies from Lemma 3.4 that $\Phi(k,x_0,\mathbf{u},D) \subseteq\downarrow \Phi(k,x_0,\mathbf{u},D_{\max})$, for all $k \in \mathbb{N}_{\geq 0}$. ■

Proposition 6.4: 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 $D_{\max} = \max(D)$. □

Proof. **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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to U$ and $N \in \mathbb{N}_{>0}$ such that (13) and (14) hold. Using (13) 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 (14) and the last inclusion comes from Lemma 6.3.

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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to U$ and $N \in \mathbb{N}_{>0}$ such that the following conditions are satisfied

$$\Phi(k, x_0, \mathbf{u}, D_{\max}) \subseteq X, \quad \forall\ k \in \{1, 2, \ldots, N-1\} \tag{17}$$

and

$$\Phi(N, x_0, \mathbf{u}, D_{\max}) \subseteq\downarrow \bigcup_{0\leq k\leq N-1} \Phi(k, x_0, \mathbf{u}, D_{\max}) \tag{18}$$

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 6.3, the second inequality follows from (17) and the last inequality comes from the lower closedeness of the set X. To show that (14) holds, we have the following

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

where the first inclusion comes from Lemma 6.3, 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 $D_{\max} \subseteq D$. ■

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

Proposition 6.5: 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. If the system Σ is CSM, the set of states X is lower closed and the set of inputs inputs U is closed and bounded below, and for all $\varepsilon >= 0$, for all $x_1, x_2 \in \mathcal{X}$ and for all $u \in U$, following condition is satisfied:

$$x_1 \geq x_2 + \varepsilon \implies \mathcal{B}_\varepsilon(f(x_2, u, D)) \subseteq\downarrow f(x_1, u, D) \tag{19}$$

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 $U_{\min} = \min(U)$. □

Proof. The proof is immediate and follows directly from (19), the fact that $U_{\min} \subseteq U$. ■

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

Proposition 6.6: 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. 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, $D = \{\overline{d}\}$.*
- *The system Σ is DSM and card$(D_{\max}) = 1$.*

□

Proof. 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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that (13) and (14) are satisfied. Consider the controller $\kappa : \mathcal{X} \to \mathcal{U}$ defined as follows: for $k \in \{1, 2, \ldots, N-1\}$, $\kappa(\Phi(k, x_0, \mathbf{u}, D)) = \mathbf{u}(k)$, 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 (11) and (12) 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 $D = \{\overline{d}\}$. 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 $\kappa : \mathcal{X} \to \mathcal{U}$ and $N \in \mathbb{N}_{>0}$ such that (11) and (12). Consider the control input trajectory $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$ defined as follows: for $k \in \{1, 2, \ldots, N-1\}$, $\mathbf{u}(k) = \kappa(\Phi(k, x_0, \mathbf{u}, \overline{d}))$ and $\mathbf{u}(k) \in \mathcal{U}$ for all $k \geq N$. Using the control input trajectory $\mathbf{u}$, one can easily check that (13) and (14) 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 *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 6.4. ■

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

Theorem 6.7: 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 $f : \mathcal{X} \times \mathcal{U} \times \mathcal{D} \to \mathcal{X}$ 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 $\mathbf{u} : \mathbb{N}_{\geq 0} \to \mathcal{U}$, $N \in \mathbb{N}_{>0}$ and ε_N such that

$$\mathcal{B}_{\varepsilon_N}(\Phi_\kappa(N, x_0, \mathbf{u}, D)) \subseteq\downarrow \bigcup_{0\leq k\leq N-1} \Phi_\kappa(k, x_0, \mathbf{u}, D). \tag{20}$$

(ii) There exists $\gamma > 0$ such that $\mathcal{B}_\gamma(\Phi(k, x_0, \mathbf{u}, D)) \subseteq X, \quad \forall\ k \in \{1, 2, \ldots, N-1\}$

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. □

Proof. 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 compacteness of D we have that $\Phi(N-1, x_0, \mathbf{u}, D)$ is compact. Hence, for $\beta_N = \min(_N, \gamma) > 0$, where $\gamma > 0$ is defined in (ii), we have from Lemma A.1 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 A.1 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

$$\begin{aligned} \Phi(N, \mathcal{B}_{\beta_0}(x_0), \mathbf{u}) &\subseteq \Phi(N, \mathcal{B}_{\varepsilon_0}(x_0), \mathbf{u}) \\ &\subseteq \Phi(N-1, \mathcal{B}_{\beta_1}(\Phi(1, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \Phi(N-1, \mathcal{B}_{\varepsilon_1}(\Phi(1, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \Phi(N-2, \mathcal{B}_{\beta_2}(\Phi(2, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \Phi(N-2, \mathcal{B}_{\varepsilon_2}(\Phi(2, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \dots \\ &\subseteq \Phi(1, \mathcal{B}_{\beta_{N-1}}(\Phi(N-1, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \Phi(1, \mathcal{B}_{\varepsilon_{N-1}}(\Phi(N-1, x_0, \mathbf{u}), \mathbf{u}) \\ &\subseteq \mathcal{B}_{\varepsilon_N}(\Phi(N, x_0, \mathbf{u})) \\ &\subseteq\downarrow \bigcup_{0 \le k \le N-1} \Phi_\kappa(k, x_0, \mathbf{u}, D) \end{aligned} \tag{21}$$

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

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

Where the second inclusion comes from (21) and the last inclusion follows from the fact that Σ is a SM system. Hence, condition (14) of Definition 6.1 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 (14) of Definition 6.1 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 A.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 $\varepsilon_{k-1} = \frac{\beta_k}{L}$. hence, the result holds with $\beta = \min \beta_i$, $i \in \{1, \dots, N\}$.

■

VII. Computation of controlled invariants

As shown in Theorem 5.2 and Proposition 6.2, controlled invariants for monotone system and lower closed safety specification are lower closed and can be computed used feasible points. This property implies that the boundary of the maximal controlled invariant set has the structure of a Pareto front and can therefore be approximated arbitrarily close, by resorting to multidimensional binary search algorithms used in multi-objective optimization [12], [20][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" checks if x is open-loop feasible, i.e. it satisfies (14) for some input trajectory $\mathbf{u} : \mathbb{N} \to U$, in this case, any point in the lower closure of the set Z defined below is feasible, and there no need to explore it.

$$Z = \bigcup_{0 \le k \le N-1} \Phi(k, x_0, \mathbf{u}, D) \tag{22}$$

Similarly, the command "leads to the unsafe set $\mathcal{F}_2 \cup \overline{X}$" checks if for all possible input trajectories $\mathbf{u} : \mathbb{N} \to U$ there exists $k \in \{1, 2 \dots, N\}$ such that $\Phi(k, x_0, \mathbf{u}, D) \cap \mathcal{F}_2 \cup \overline{X} \neq \emptyset$. 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.

$$Y = \bigcup_{0 \le k \le N-1} \Phi(k, x_0, \mathbf{u}, D) \tag{23}$$

Algorithm 1 is made 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 decided yet if

[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 [21], [22].

[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.

they are open-loop feasible, or leading to the unsafe set. The strategy to pick a point can be found in [12]. The algorithm stops when the Hausdorff distance between the sets $\mathcal{F}_1$ and $\mathcal{F}_2$ smaller than a precision $\varepsilon > 0$. 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, one also has that $K \subseteq K^* \subseteq \mathcal{B}_\varepsilon(K)$, where K^* is the maximal 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 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 controlled invariant.

Let us now explain how other different structural properties of the system allow to improve the proposed algorithm, all 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 6.4, 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" commands, and in view of Proposition 6.5, 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 (19) 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 6.7 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 them, where β is given in the proof of Theorem 6.7 as a function of β_N, γ and the Lipschitz constant L.

VIII. Numerical Example

We consider a vehicle model moving along a straight road. The dynamics of the vehicle is adapted from [23] and described as:

$$m\dot{v} = \alpha(u, v) = \begin{cases} u - f_0 - f_2 v^2 & \text{if} \quad v > 0 \\ \max(u - f_0, 0) & \text{if} \quad v = 0 \end{cases} \tag{24}$$

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 $f_0 + f_2 v^2$ include 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 $d \in D$, considered as a disturbance. The dynamics of the global system is given by:

$$\begin{cases} \dot{h} &= d - v \\ m\dot{v} &= \alpha(u, v). \end{cases} \tag{25}$$

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.

Algorithm 1: Invariance

Input: A SM system Σ as in (1), a contraint set (X, U, D), where X a lower closed set X and a precision $\varepsilon > 0$
Output: A controlled invariant set $K \subseteq X$.

begin
  for $x \in \max(X)$
    if x is open-loop feasible **then**
      $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$, with Z from (22)
    else if x leads to the unsafe set $\mathcal{F}_2 \cup \overline{X}$
      $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$, with Y from (23
    end if
  end for
  if $X = \mathcal{F}_1$
    return $K = X$
  end if
  for $x \in \min(X)$
    if x is open-loop feasible **then**
      $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$, with Y from (23
    else if x leads to the unsafe set $\mathcal{F}_2 \cup \overline{X}$
      $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$, with Z from (22)
    end if
  end for
  if $\min(X) \subseteq \mathcal{F}_2$
    return $K = \emptyset$
  end if
  while $\mathbf{d}(\mathcal{F}_2, \mathcal{F}_1) > \varepsilon$
    Pick $x' \in (X \setminus \mathcal{F}_2) \cap (X \setminus \mathcal{F}_1)$
    if x is open-loop feasible **then**
      $\mathcal{F}_2 = \mathcal{F}_2 \cup \uparrow Y$, with Y from (23
    else if x leads to the unsafe set $\mathcal{F}_2 \cup \overline{X}$
      $\mathcal{F}_1 = \mathcal{F}_1 \cup \downarrow Z$, with Z from (22)
    end if
  end while
return $K = X \cap \mathcal{F}_1$.

TABLE I: 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

Remark 8.1: Let us remark that the system can be easily transformed to a CDSM system one by using the following change of coordinates: $d' = -d$ and $z = -h$. •

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 (24), the constraint set is a lower closed set. For the computation of the controlled invariant, we

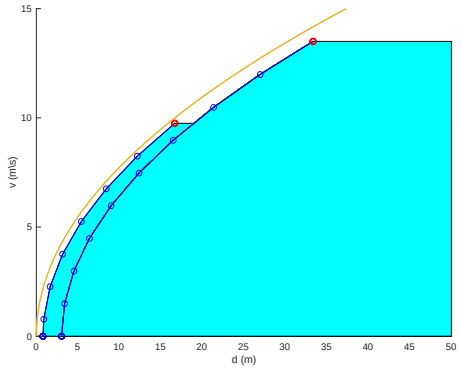

Fig. 3: The light blue region represents the domain of the robust controlled invariant. The blue trajectories are initiated from two feasible points (in red) $x_1 = [33.75; 13.5]$ and $x_2 = [16.25; 9.75]$. The orange curve represents the boundary of the maximal robust controlled invariant. The precision ε chosen for Algorithm 1 is $\varepsilon = 1.5$.

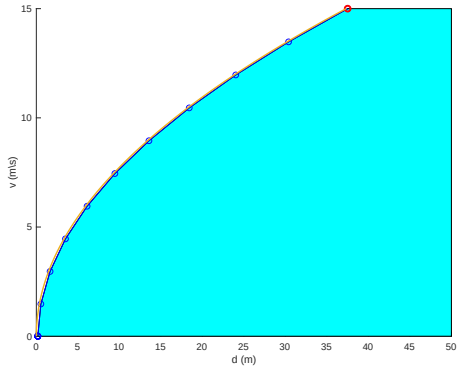

Fig. 4: The light blue region represents the domain of the robust controlled invariant. The blue trajectory is initiated from the feasible point (in red) $x = [37.5; 15]$. The orange curve represents the boundary of the maximal robust controlled invariant. The precision ε chosen for Algorithm 1 is $\varepsilon = 0.01$.

use Algorithm 1. The parameters model are taken from [23] and are presented in Table I. Figure 3 and 4 represent the computed robust controlled invariant set for two different precisions $\varepsilon = 1.5$ and $\varepsilon = 0.01$. Moreover, we also present in orange the boundary of the maximal robust controlled invariant set, which can be computed analytically for this problem, following the approach presented in [24].

IX. Conclusion

In this paper, we have presented different characterizations of robust controlled invariants for discrete-time monotone dynamical system, 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.

Appendix

Lemma A.1: 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 $L > 0$, then 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 $F(\mathcal{B}_{\eta_x}(x)) \cap \mathcal{X}) \subset \mathcal{B}_\varepsilon(F(x))$. Let $\eta = \min_{x \in Z} \eta_x$. It follows from the compacteness of the set Z that $\eta > 0$. Hence, one gets:

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

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

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

■

Proof of Proposition 4.3:

Sufficient condition: Consider a controller $\kappa : X \to U$ defined as

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

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 $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ 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 $\kappa : X \to U$, with $dom(\kappa) = K$ and such that for all $x_0 \in K$ and for any disturbance input $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ the solution of the closed loop system $\Phi_\kappa(., x_0, \mathbf{d}) : \mathbb{N}_{\geq 0} \to \mathcal{X}$ 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 $\mathbf{d} : \mathbb{N}_{\geq 0} \to D$ is any disturbance input trajectory satisfying $\mathbf{d}(0) = d \in D$, which ends the proof.

References

[1] Franco Blanchini and Stefano Miani. *Set-theoretic methods in control*. Springer, 2008.

[2] SV Rakovic, P Grieder, Michal Kvasnica, DQ Mayne, and Manfred Morari. 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)*, volume 2, pages 1418–1423. IEEE, 2004.

[3] Tzanis Anevlavis, Zexiang Liu, Necmiye Ozay, and Paulo Tabuada. Controlled invariant sets: implicit closed-form representations and applications. *arXiv preprint arXiv:2107.08566*, 2021.

[4] Milan Korda, Didier Henrion, and Colin N Jones. Convex computation of the maximum controlled invariant set for polynomial control systems. *SIAM Journal on Control and Optimization*, 52(5):2944–2969, 2014.

[5] Mohamed Amin Ben Sassi and Antoine Girard. Computation of polytopic invariants for polynomial dynamical systems using linear programming. *Automatica*, 48(12):3114–3121, 2012.

[6] Adnane Saoud and Ricardo G Sanfelice. Computation of controlled invariants for nonlinear systems: Application to safe neural networks approximation and control. *IFAC-PapersOnLine*, 54(5):91–96, 2021.

[7] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[8] Adnane Saoud. *Compositional and Efficient Controller Synthesis for Cyber-Physical Systems*. PhD thesis, Université Paris Saclay, 2019.

[9] Pierre-Jean Meyer, Antoine Girard, and Emmanuel Witrant. Robust controlled invariance for monotone systems: application to ventilation regulation in buildings. *Automatica*, 70:14–20, 2016.

[10] Elena Ivanova, Adnane Saoud, and Antoine Girard. Lazy controller synthesis for monotone transition systems and directed safety specifications. *Automatica*, 135:109993, 2022.

[11] Sadra Sadraddini and Calin Belta. Safety control of monotone systems with bounded uncertainties. In *2016 IEEE 55th Conference on Decision and Control (CDC)*, pages 4874–4879. IEEE, 2016.

[12] Julien Legriel, Colas Le Guernic, Scott Cotton, and Oded Maler. Approximating the pareto front of multi-criteria optimization problems. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 69–83. Springer, 2010.

[13] Brian A Davey and Hilary A Priestley. *Introduction to lattices and order*. Cambridge university press, 2002.

[14] Jean-Pierre Aubin and Hélène Frankowska. *Set-valued analysis*. Springer Science & Business Media, 2009.

[15] Hal L Smith. *Monotone dynamical systems: an introduction to the theory of competitive and cooperative systems*. Number 41. American Mathematical Soc., 2008.

[16] David Angeli and Eduardo D Sontag. Monotone control systems. *IEEE Transactions on Automatic Control*, 48(10):1684–1698, 2003.

[17] Pierre-Jean Meyer, Antoine Girard, and Emmanuel Witrant. Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Transactions on Automatic Control*, 63(6):1835–1841, 2017.

[18] Matthias Rungger and Paulo Tabuada. Computing robust controlled invariant sets of linear systems. *IEEE Transactions on Automatic Control*, 62(7):3665–3670, 2017.

[19] Saša V Rakovic and Miroslav Baric. Parameterized robust control invariant sets for linear systems: Theoretical advances and computational remarks. *IEEE Transactions on Automatic Control*, 55(7):1599–1614, 2010.

[20] Pranav Tendulkar. *Mapping and scheduling on multi-core processors using SMT solvers*. PhD thesis, Universite de Grenoble I-Joseph Fourier, 2014.

[21] Mohammad Al Khatib, Antoine Girard, and Thao Dang. Stability verification and timing contract synthesis for linear impulsive systems using reachability analysis. *Nonlinear Analysis: Hybrid Systems*, 25:211–226, 2017.

[22] D. Zonetti, A. Saoud, A. Girard, and L Fribourg. A symbolic approach to voltage stability and power sharing in time-varying DC microgrids. In *European Control Conference*, pages 903–909, 2019.

[23] A. Saoud, A. Girard, and L. Fribourg. Contract-based design of symbolic controllers for safety in distributed multiperiodic sampled-data systems. *IEEE Transactions on Automatic Control*, 2020. To appear.

[24] Alex Devonport and Murat Arcak. Data-driven reachable set computation using adaptive gaussian process classification and monte carlo methods. In *2020 American Control Conference (ACC)*, pages 2629–2634. IEEE, 2020.