MIT Libraries | DSpace@MIT

MIT Open Access Articles

*Control for Safety Specifications of Systems With Imperfect Information on a Partial Order*

The MIT Faculty has made this article openly available. ***Please share*** how this access benefits you. Your story matters.

**Citation:** Ghaemi, Reza, and Domitilla Del Vecchio. "Control for Safety Specifications of Systems With Imperfect Information on a Partial Order." IEEE Trans. Automat. Contr. 59, no. 4 (April 2014): 982–995.

**As Published:** http://dx.doi.org/10.1109/tac.2014.2301563

**Publisher:** Institute of Electrical and Electronics Engineers (IEEE)

**Persistent URL:** http://hdl.handle.net/1721.1/97408

**Version:** Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

**Terms of use:** Creative Commons Attribution-Noncommercial-Share Alike

Massachusetts Institute of Technology

# Control for Safety Specifications of Systems with Imperfect Information on a Partial Order

Reza Ghaemi, *Member, IEEE,* Domitilla Del Vecchio, *Member, IEEE*

**Abstract**

In this paper, we consider the control problem for uncertain systems with imperfect information, in which an output of interest must be kept outside an undesired region (the bad set) in the output space. The state, input, output, and disturbance spaces are equipped with partial orders. The system dynamics are either input/output order preserving with output in $\mathbb{R}^2$ or given by the parallel composition of input/output order preserving dynamics each with scalar output. We provide necessary and sufficient conditions under which an initial set of possible system states is safe, that is, the corresponding outputs are steerable away from the bad set with open loop controls. A closed loop control strategy is explicitly constructed, which guarantees that the current set of possible system states, as obtained from an estimator, generates outputs that never enter the bad set. The complexity of algorithms that check safety of an initial set of states and implement the control map is quadratic with the dimension of the state space. The algorithms are illustrated on two application examples: a ship maneuver to avoid an obstacle and safe navigation of an helicopter among buildings.

## I. Introduction

The problem of keeping the state of a dynamic system in a desired region via feedback control has been considered by researchers for decades [1], [2], [3], [4]. A common approach is to determine the set, called maximal controlled invariant set (MCIS), of all initial states that can be kept in the desired region via a control strategy [4], [5], [6]. This problem has also been casted as that of avoiding the complement of the desired region [7], called "bad set", and is referred to as safety control problem. In this case, the complement of the MCIS is called the "capture set" as it represents the set of all states that cannot be steered away from (are captured by) the bad set for any control strategy.

R. Ghaemi is with General Electrics.

D. Del Vecchio is with the Department of Mechanical Engineering at MIT, LIDS. E-mail ddv@mit.edu. This work was in part supported by NSF CAREER AWARD # CNS-0642719.

The safety control problem of uncertain dynamical systems can be considered as a min-max or pursuit-evasion problem where the disturbance tries to steer trajectories away from the desired region and the controller tries to counteract the disturbance. In [2], a finite horizon MCIS is characterized as the level set of the optimal cost of a min-max problem for discrete-time systems with perfect and imperfect state information and polyhedral and ellipsoidal algorithms for approximating the MCIS are provided. In the context of hybrid systems with perfect state information and infinite horizon, [8], [9], [10] represent the MCIS as the level set of the optimal cost of a min-max problem, which, for continuous nonlinear systems is computable by solving the Hamilton-Jacobi-Bellman (HJB) equation. The HJB equation involves issues such as existence, uniqueness, and smoothness of the solutions so that in general it is very hard to solve. Therefore, numerical methods for approximating the MCIS using level set methods [11], [12] and polygonal approximation of flow pipes [13] have been proposed. For linear systems, the reachability problem has been extensively studied and algorithms that finitely determine polyhedral approximations [14], [15], [16], ellipsoidal approximations [17] (see also [5] and the references therein), and approximations through union of zonotopes [18], [19] have been proposed.

Decidability theory is another approach to the reachability problem where mathematical logic is used to represent sets symbolically [20]-[24]. Within this approach, the reachable set is represented in the form of formulas with quantifiers and computational tools are developed to eliminate quantifiers and provide formulas that define reachable sets [25], [26]. Quantifier elimination is applicable to reachable sets that are decidable in the theory of real numbers with additive and multiplication functions. Therefore, this approach is only applicable to special classes of linear/affine systems [21], [22], [23]. Moreover, the computational demand is exponential in the size of input and output data [14]. Application-driven literature has also addressed the reachability problem for specific aerospace vehicles, such as helicopters [27], [28]. Different in scope but related to this work is also recent literature on observer-based stabilization of nonlinear and switched systems [29], [30], [31], [32].

Except for the discrete time systems work by [2], the above cited works have focused mostly on systems with perfect state information. The safety control problem when the state of the system is not exactly known has been receiving much less attention. In [33], [34], hybrid automata in which the mode is unknown to the controller and needs to be estimated are considered. For discrete-time systems, dynamic control of block triangular order preserving hybrid automata with imperfect state information is considered in [35]. In [36], [37], safety control results are extended to continuous time piecewise systems that are the parallel composition of two decoupled monotone systems [38], for which a scalar output must be controlled. These results have been extended in [39] to the case in which the system does not need to be the parallel composition of two decoupled systems, but still monotonicity and two-dimensional output are required.

In this paper, we extend the results of [39] to systems that do not need to be monotone, but whose two-dimensional output trajectories are enveloped by extremal trajectories corresponding to extremal control inputs. We refer to this property as input/output order preserving. We further extend these results to systems that are the parallel composition of an arbitrary number $k$ of input/output order preserving systems, each with output in $\mathbb{R}$ or $\mathbb{R}^2$. When some of the systems in the parallel composition have output in $\mathbb{R}^2$, perfect state information and no uncertainty are considered. Even if the dynamics of the $k$ subsystems are decoupled from each other, the control objective (avoiding a bad set in the Cartesian product of the whole system output) implicitly introduces coupling, so that the problem cannot be solved by solving $k$ separate simpler problems.

Our approach to deal with imperfect information is similar to that of open loop feedback control [40]. Specifically, we determine whether a current set of system states, obtained from a state estimator, generates outputs that can be steered away from the bad set as if no further measurements were received after the current time. As a consequence, we provide necessary and sufficient conditions to determine whether a set of possible system states belongs to the open loop MCIS, that is, it generates outputs that can be steered away from the bad set with open loop controls. Then, we explicitly provide a feedback control strategy that guarantees that the current set of possible system states, obtained from a state estimator, is kept in the computed MCIS. For $n$ dimensional systems, the computational demand of our algorithms is of order $n^2$. Therefore, the computational complexity scales at most quadratically with the number of states.

The class of input/output order-preserving systems can model a number of applications and include the class of monotone systems [38]. Several biological systems are shown to have the monotone property or to be composition of subsystems with monotone property [41], [42]. Transportation networks where each carrier, car or train, moves unidirectionally according to a predetermined path can be modeled as a group of interacting agents with monotone dynamics [43] or with input/output order preserving dynamics [44]. In this paper, we illustrate two different applications. First, we consider the free motion of a ship in $\mathbb{R}^2$ and tackle an obstacle collision avoidance problem. Second, we consider the free three dimensional motion of an helicopter among buildings. We model the helicopter dynamics by an 18 dimensional model and design

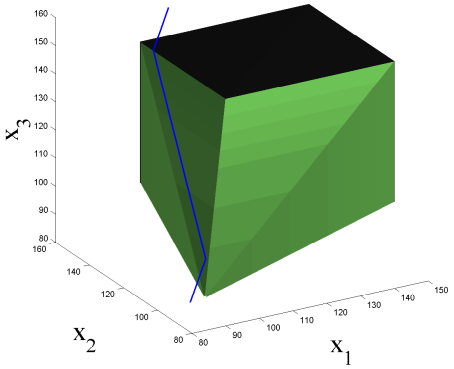


Fig. 1: Capture set and a safe trajectory obtained enforcing the control strategy explained in the text.

a supervisor that overrides the pilot with safe control actions whenever the system configuration hits the boundary of a building's capture set.

### A. *Motivating example*

In order to illustrate how the monotonicity property of the flow with respect to the input simplifies the problem of calculating the capture set of a bad set, we consider the free motion of an object in $\mathbb{R}^3$ as follows. Let $x = (x_1, x_2, x_3)$ denote the position of the object and assume that the motion can be described by the three integrators $\dot{x}_1 = u_1, \quad \dot{x}_2 = u_2, \quad \dot{x}_3 = u_3$, in which the input $u = (u_1, u_2, u_3)$ is bounded and subject to constraints $1 \leq u_i \leq 5,\ i = 1, 2, 3$. There is an obstacle (bad set) that must be avoided given by $\mathbf{B} := [100,\ 150] \times [100,\ 150] \times [100,\ 150] \subset \mathbb{R}^3$. We seek to determine the capture set of this obstacle and the control strategy that guarantees that any initial condition starting outside of the capture set is kept outside it.

Consider an initial condition $x(0)$ and let $x_{im}$ and $x_{iM}$ denote trajectories generated by the extremal inputs $u_i = 1$ or $u_i = 5$. It follows that $x_{im}(t) \leq x_i(t) \leq x_{iM}(t)$ for all $t \geq 0$. Systems with this property belong to the class of input/output order preserving systems. Consider all extremal trajectories of $x$ in $\mathbb{R}^3$ generated by all combinations of extremal inputs, pick a point on each of these trajectories, and consider the convex hull of these points. Because the system is input/output order preserving any $x$ trajectory corresponding to any arbitrary input will cross this convex hull. If all extremal trajectories cross the bad set $\mathbf{B}$, we can pick all the points on the extremal trajectories in such a way that they are all inside the bad set, so that their convex hull is also all contained in the bad set (since the bad set is convex). It follows that if all extremal trajectories cross the bad set, then any trajectory for any arbitrary input will also cross the bad set. As a consequence, $x(0)$ belongs to the capture set of the bad set.

This reasoning illustrates that for an input/output order preserving system we can determine whether an initial state is in the capture set by only checking whether all its extremal trajectories cross the bad set. This also implies that the capture set (depicted in Figure 1) can be geometrically determined by intersecting all the backward reachable sets of the bad set obtained with extremal inputs. Denote the extremal inputs by $u^1, u^2, ..., u^8$ and denote the backward reachable set of **B** corresponding to each of these inputs by $C_{u^j}$ for $j \in \{1, ..., 8\}$. A control strategy that leaves the input free and constrains it only on the boundary of the capture set is easily constructed by enforcing input $u^j$ whenever the position is on the boundary of $C_{u^j}$ and inside $C_{u^k}$ for all $k \neq j$. An example of state trajectory obtained employing this strategy is illustrated in Figure 1. We will show in this paper that we need to actually calculate only $6$ extremal trajectories for this system. That is, for an $n$ dimensional system we need to calculate only $n(n-1)$ extremal trajectories.

In this paper, we extend this reasoning to general systems that are input/output order preserving, with disturbance inputs, and with imperfect state information. The paper is organized as follows. Section II introduces the class of systems and the control problem. Section III provides necessary and sufficient conditions for the set of initial states to be steerable away from the bad set and Section IV provides a control strategy. Implementation details are addressed in Section V. In Sections VI and VII, we address the application examples. The Appendix contains basic definitions, intermediate results, and proofs.

## II. System Class and Problem Formulation

A system $\Sigma$ is a tuple $\Sigma = (X, \mathcal{D}, \mathcal{U}, \mathcal{Y}, f, g)$, where $X \subset \mathbb{R}^n$ is the state space, $\mathcal{D} \subset \mathbb{R}^p$ and $\mathcal{U} \subset \mathbb{R}^m$ are the sets of disturbances and inputs, respectively, $\mathcal{Y}$ is the space of outputs to be controlled, $f : X \times \mathcal{D} \times \mathcal{U} \to X$ is a piecewise continuous vector field, $g : X \to \mathcal{Y}$ is the output map. Let $\phi : \mathbb{R}_+ \times X \times \mathcal{C}(\mathcal{D}) \times \mathcal{C}(\mathcal{U}) \to X$ denote the flow of the system where $\mathcal{C}(\mathcal{U})$ is the set of control input signals and $\mathcal{C}(\mathcal{D})$ is the set of disturbance input signals. In addition, let $y := g(\phi) : \mathbb{R}_+ \times X \times \mathcal{C}(\mathcal{D}) \times \mathcal{C}(\mathcal{U}) \to \mathcal{Y}$ denote the output to be controlled. We assume that the space of disturbance signals $\mathcal{C}(\mathcal{D})$ is connected, that $\mathcal{Y} \subseteq \mathbb{R}^2$, that the flow of the system $\Sigma$ is continuous with respect to time, to initial condition, and to disturbance, and that $g$ is continuous. In this paper, we denote signals in bold. For two sets $A, B \subset \mathbb{R}^2$, we say $A$ is below $B$ denoted by $A \preceq B$, if for all $(x_1, x_2) \in A$ and $(y_1, y_2) \in B$ such that $x_1 = y_1$, $x_2 \leq y_2$. We say that $A$ is strictly below $B$ denoted by $A \prec B$, if for all $(x_1, x_2) \in A$ and $(y_1, y_2) \in B$ such that $x_1 = y_1$, $x_2 < y_2$.

*Definition 1:* System $\Sigma$ is said to be input/output order preserving provided that

(i) The set $\mathcal{U}$ is partially ordered with respect to a cone $\Delta_u \subset \mathbb{R}^m$. Moreover, there are $u_m,\ u_M \in \mathcal{U}$ such that for all $u \in \mathcal{U}$, $u \geq u_m$ and $u \leq u_M$.

(ii) For all $\mathbf{u} \in \mathcal{C}(\mathcal{U})$, we have that

- $y(\mathbb{R}_+, x, \mathbf{d}, \mathbf{u}_m) \preceq y(\mathbb{R}_+, x, \mathbf{d}, \mathbf{u}) \preceq y(\mathbb{R}_+, x, \mathbf{d}, \mathbf{u}_M)$, for all $x \in X$, $\mathbf{d} \in \mathcal{C}(\mathcal{D})$, if $\mathcal{Y} = \mathbb{R}^2$ and
- $y(t, x, \mathbf{d}, \mathbf{u}_m) \leq y(t, x, \mathbf{d}, \mathbf{u}) \leq y(t, x, \mathbf{d}, \mathbf{u}_M)$, for all $x \in X$, $\mathbf{d} \in \mathcal{C}(\mathcal{D})$, and $t \in \mathbb{R}_+$, if $\mathcal{Y} = \mathbb{R}^1$,

in which $\mathbf{u}_m(t) = u_m$ and $\mathbf{u}_M(t) = u_M$ for all $t \geq 0$.

The above definition is weaker than the order preserving property of [37], [39] as it only requires the output trajectories corresponding to the extremal control signals to envelop all other trajectories. The order preserving property of [37], [39] instead requires that the flow is an order preserving map [45]. A sufficient condition for $\Sigma$ to be input/output order preserving is to be an input/output monotone system for which algebraic checks exist [38].

*Definition 2:* Given systems $\Sigma^i = (X^i, \mathcal{D}^i, \mathcal{U}^i, \mathcal{Y}^i, f^i, g^i),\ i = 1, \cdots, k$, the parallel composition $\Sigma = \Sigma^1 \parallel \cdots \parallel \Sigma^k$ is a system $\Sigma = (X, \mathcal{D}, \mathcal{U}, \mathcal{Y}, f, g)$ in which $X = X^1 \times \cdots \times X^k$, $\mathcal{D} = \mathcal{D}^1 \times \cdots \times \mathcal{D}^k$, $\mathcal{U} = \mathcal{U}^1 \times \cdots \times \mathcal{U}^k$, $\mathcal{Y} = \mathcal{Y}^1 \times \cdots \times \mathcal{Y}^k$, for $x = (x^1, \cdots, x^k)$, $f(x) = (f^1(x^1), \cdots, f^k(x^k))$, $g(x) = (g^1(x^1), \cdots, g^k(x^k))$, the flow of the system $\Sigma$ is $\phi = (\phi^1, \cdots, \phi^k)$ and the output is $y = (y^1, \cdots, y^k)$.

In this paper, we consider systems $\Sigma$ given by the parallel composition of $k$ subsystems in which $\mathcal{Y}^i \subseteq \mathbb{R}^2$ and assume that the state of $\Sigma$ is not perfectly measured. Specifically, let $\mathcal{M}$ denote the measured output space and let $h : \mathcal{M} \to 2^X$ be the measurement map that for each measurement $z \in \mathcal{M}$ returns a set of possible states that can have generated such a measurement. In particular, we have that the signal $\mathbf{z}(t)$ measured in correspondence to flow $\phi(t, x_0, \mathbf{d}, \mathbf{u})$ must be such that $\phi(t, x_0, \mathbf{d}, \mathbf{u}) \in h(\mathbf{z}(t))$ for all $t$. Let $\hat{x}(t, S, \mathbf{u}, \mathbf{z})$ denote the set of all possible states at time $t$ compatible with the measurement signal $\mathbf{z}$ up to time $t$, the control input signal $\mathbf{u}$ applied up to the time $t$, and the set of possible initial states $S$. This set, often referred to as non-deterministic information state [46], is formally defined as

$$\begin{aligned} &\hat{x}(t, S, \mathbf{u}, \mathbf{z}) := \{x \in X \mid \exists\ x_0 \in S, \mathbf{d} \in \mathcal{C}(\mathcal{D}),\ s.t. \\ &x = \phi(t, x_0, \mathbf{d}, \mathbf{u})\ , \phi(\tau, x_0, \mathbf{d}, \mathbf{u}) \in h(\mathbf{z}(\tau))\ \forall \tau \in [0, t]\}. \end{aligned} \tag{1}$$

Consider a bad set in the output space, denoted $\mathbf{B} \subseteq \mathcal{Y}$. We seek to determine the set of initial sets $S$ such that the corresponding output trajectories are steerable away from the bad set $\mathbf{B}$. The problem is formally stated as follows.

**Problem 1:** Given system $\Sigma$ and a bad set $\mathbf{B} \subseteq \mathcal{Y}$, determine the open loop maximal safe controlled invariant set given by

$$\begin{aligned} \mathcal{W} = \{S \subseteq X \mid \exists\ \mathbf{u} \in \mathcal{C}(\mathcal{U}),\ s.t.\ \forall\ \mathbf{d} \in \mathcal{C}(\mathcal{D}), \\ y(\mathbb{R}_+, S, \mathbf{d}, \mathbf{u})) \cap \mathbf{B} = \emptyset\}. \end{aligned} \tag{2}$$

Set $\mathcal{W}$ is the set of all state uncertainties $S \subseteq X$ for which an open loop control signal $\mathbf{u}$ exists that keeps all the possible output trajectories outside of the bad set $\mathbf{B}$. At each time instant $t$, we have current information given by the information state (or its estimate, as we will see in the sequel) $\hat{x}(t)$, so that if $\hat{x}(t) \in \mathcal{W}$ we can compute a set-valued feedback map $K(\hat{x}(t))$ such that if $\mathbf{u}(t) \in K(\hat{x}(t))$ then $g(\hat{x}(t))$ is kept outside $\mathbf{B}$ for all $t$. This is formally introduced by the following problem.

**Problem 2:** Determine a control map $K : 2^X \to 2^{\mathcal{U}}$ such that for all output measurements $\mathbf{z} \in S(\mathcal{M})$ and $S \in \mathcal{W}$, we have that $g(\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z})) \cap \mathbf{B} = \emptyset$ if $\mathbf{u}(t) \in K(\hat{x}(t, S, \mathbf{u}, \mathbf{z}))$, for all $t \in \mathbb{R}_+$.

Note that the control strategy sought in Problem 2 is a (closed loop) feedback control strategy. This approach is similar to that of open loop feedback control [40], in which existence of a controller is established based on open loop controls as if no further information on the system state were acquired in the future, but the control applied at time $t$ is based on a map from a state estimate, which progressively reduces the uncertainty on the state.

When $\Sigma = \Sigma^1 || \cdots || \Sigma^k$, we have that $\mathcal{M} = \mathcal{M}^1 \times \cdots \times \mathcal{M}^k$, $z = (z^1, ..., z^k)$, and that $h(z) = (h^1(z^1), ..., h^k(z^k))$. In such a case, we also have that the set of initial states is such that $S = S^1 \times \cdots \times S^k$. We solve the above two problems under the assumption that systems $\Sigma^i$ are input/output order preserving, that $S^i$ are connected, that the bad set $\mathbf{B} = \mathbf{B}^1 \times \cdots \times \mathbf{B}^k$ with $\mathbf{B}^i \subseteq \mathcal{Y}^i$ is also connected, and that the map $h^i : \mathcal{M}^i \to 2^{X^i}$ is such that for all $z^i \in \mathcal{M}^i$, $h^i(z^i)$ is a closed and connected set. Under these assumptions, it follows that $\hat{x}(t)$ is also connected.

We also assume the following liveness property:

*Assumption 1:* There exists $\xi > 0$ such that $\frac{d}{dt} y_1^i(t, x, \mathbf{d}^i(t), \mathbf{u}^i(t)) \geq \xi,\ i = 1, \cdots, k$ for all $t \in \mathbb{R}_+$, $\mathbf{u}^i \in \mathcal{C}(\mathcal{U}^i)$, $\mathbf{d}^i \in \mathcal{C}(\mathcal{D}^i)$, and $x \in X$.

This assumption basically prevents the trivial solution in which the bad set is avoided by stopping the system from evolving.

## III. Solution to Problem 1

In this section, we provide necessary and sufficient conditions to determine whether a given set $S$ is in $\mathcal{W}$. First, we consider the case where system $\Sigma$ is an input/output order preserving system with $\mathcal{Y} = \mathbb{R}^2$. Then, we employ this result to provide the solution to Problem 1 for the case in which system $\Sigma$ is the parallel composition of input/output order preserving systems, each with scalar output ($\mathcal{Y}^i = \mathbb{R}$). This result can be, in turn, extended to the case in which $\mathcal{Y}^i = \mathbb{R}^2$ in the case of perfect state information and no disturbance inputs.

Given $\mathbf{u} \in \mathcal{C}(\mathcal{U})$, define the set

$$C_{\mathbf{u}} := \{x \in X \mid \exists\ \mathbf{d} \in \mathcal{C}(\mathcal{D})\ s.t.\ y(\mathbb{R}_+, x, \mathbf{d}, \mathbf{u}) \cap \mathbf{B} \neq \emptyset\}. \tag{3}$$

The set $C_{\mathbf{u}}$ is the set of all initial states such that there exists a disturbance signal whose corresponding output trajectory intersects the bad set when the input signal is fixed to $\mathbf{u}$. This set is the backward reachable set of $g^{-1}(\mathbf{B})$ under fixed control signal $\mathbf{u}$.

**Theorem 1:** Consider an input/output order preserving system with $\mathcal{Y} = \mathbb{R}^2$. Then, $S \in \mathcal{W}$ if and only if $C_{\mathbf{u}_m} \cap S = \emptyset$ or $C_{\mathbf{u}_M} \cap S = \emptyset$.

*Proof:* Since $C_{\mathbf{u}} \cap S \neq \emptyset$ if and only if $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$, the statement of the theorem can be rephrased as: $S \notin \mathcal{W}$ if and only if $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_m) \cap \mathbf{B} \neq \emptyset$ and $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_M) \cap \mathbf{B} \neq \emptyset$. This is what we prove, that is, that there is no control input signal $\mathbf{u}$ if and only if both extremal control signals take some output trajectory into $\mathbf{B}$.

If $S \notin \mathcal{W}$, then for all $\mathbf{u} \in \mathcal{C}(\mathcal{U})$ we have $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$. Hence, $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_m) \cap \mathbf{B} \neq \emptyset$ and $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_M) \cap \mathbf{B} \neq \emptyset$.

Now, we proceed to prove that if $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_m) \cap \mathbf{B} \neq \emptyset$ and $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}_M) \cap \mathbf{B} \neq \emptyset$ then $S \notin \mathcal{W}$. Assume $b^1, b^2 \in \mathbf{B}$, $x^1, x^2 \in S$, $\mathbf{d}^1, \mathbf{d}^2 \in \mathcal{C}(\mathcal{D})$, and $t^1, t^2 \geq 0$ are such that $y(t^1, x^1, \mathbf{d}^1, \mathbf{u}_m) = b^1$ and $y(t^2, x^2, \mathbf{d}^2, \mathbf{u}_M) = b^2$. Let $\mathbf{u} \in \mathcal{C}(\mathcal{U})$. By continuity of the output flow $y$ with respect to time and Assumption 1, there exists $t \in \mathbb{R}_+$ such that $y_1(t, x^1, \mathbf{d}^1, \mathbf{u}) = b^1_1$. Moreover, since $\Sigma$ is an input/output order preserving system, we have that $y_2(t, x^1, \mathbf{d}^1, \mathbf{u}) \geq b^1_2$. If $y_2(t, x^1, \mathbf{d}^1, \mathbf{u}) = b^1_2$ then $y(t, x^1, \mathbf{d}^1, \mathbf{u}) = b^1 \in \mathbf{B}$. Since $x^1 \in S$ and $\mathbf{u} \in \mathcal{C}(\mathcal{U})$ is chosen arbitrarily, $S \notin \mathcal{W}$. Hence, the theorem is proved. Otherwise, define $\gamma^o(x, \mathbf{d}, \mathbf{u}) := \{y(t, x, \mathbf{d}, \mathbf{u}) \mid t \in \mathbb{R}_+\}$, $\gamma^+(x, \mathbf{d}, \mathbf{u}) := \{(y_1(t, x, \mathbf{d}, \mathbf{u}), y) \mid t \in \mathbb{R}_+ \text{ and } y > y_2(t, x, \mathbf{d}, \mathbf{u})\}$, and $\gamma^-(x, \mathbf{d}, \mathbf{u}) := \{(y_1(t, x, \mathbf{d}, \mathbf{u}), y) \mid t \in \mathbb{R}_+ \text{ and } y < y_2(t, x, \mathbf{d}, \mathbf{u})\}$. Since $\Sigma$ is input/output order preserving, we must have that $b^1 \in \gamma^-(x^1, \mathbf{d}^1, \mathbf{u})$. Following the same argument for the point $b^2$, we have $b^2 \in \gamma^+(x^2, \mathbf{d}^2, \mathbf{u})$. Without loss of generality, one can assume $b^1_1 \geq b^2_1$. Then $b^1_1, b^2_1 \geq g_1(x^2)$.

If $y(\mathbb{R}_+, x^2, \mathbf{d}^2, \mathbf{u}) \cap \mathbf{B} \neq \emptyset$ then the theorem is proved. Otherwise, $\{b \in \mathbf{B} \mid b \geq g_1(x^2)\} \subset \gamma^+(x^2, \mathbf{d}^2, \mathbf{u}) \cup \gamma^-(x^2, \mathbf{d}^2, \mathbf{u})$. To proceed, define the following mapping. For $\alpha \in \mathbb{R}$, $\mathbf{u} \in \mathcal{C}(\mathcal{U})$, $\mathbf{d} \in \mathcal{C}(\mathcal{D})$, and $x \in S_\alpha := \{x \in S \mid g_1(x) \leq \alpha\}$, let $\bar{t}$ be such that $y_1(\bar{t}, x, \mathbf{d}, \mathbf{u}) = \alpha$. Define the map $W(\cdot; \alpha, \mathbf{u}) : S_\alpha \times \mathcal{C}(\mathcal{D}) \to \mathbb{R}$ as $W(x, \mathbf{d}; \alpha, \mathbf{u}) := y_2(\bar{t}, x, \mathbf{d}, \mathbf{u})$, in which we think of $\alpha$ and $\mathbf{u}$ as fixed parameters. Given $\alpha \in \mathbb{R}$, the map $W$ determines the intersection of the line $y_1 = \alpha$ and the path $y(\mathbb{R}_+, x, \mathbf{d}, \mathbf{u})$. Given Assumption 1 and the continuity of $y$ with respect to time, for all $\alpha \in \mathbb{R}$ and $x \in S$ with $g_1(x) \leq \alpha$ ($x \in S_\alpha$), there exists a unique $\bar{t} \in \mathbb{R}_+$ such that $y_1(\bar{t}, x, \mathbf{d}, \mathbf{u}) = \alpha$. Hence, the mapping $W$ is a function. It can also be shown that this function is continuous with respect to its arguments $x$ and $\mathbf{d}$ by the continuity of the flow. According to Assumption 1, and openness of the sets $\gamma^+(x^2, \mathbf{d}^2, \mathbf{u})$ and $\gamma^-(x^2, \mathbf{d}^2, \mathbf{u})$, we have $b^1 \in \gamma^+(x^2, \mathbf{d}^2, \mathbf{u})$. Hence, $W(x^2, \mathbf{d}^2; b^1_1, \mathbf{u}) < b^1_2$. From $b^1 \in \gamma^-(x^1, \mathbf{d}^1, \mathbf{u})$, we have $W(x^1, \mathbf{d}^1; b^1_1, \mathbf{u}) > b^1_2$. Since $S_{b_1}$ is connected, $\mathcal{C}(\mathcal{D})$ is connected, and $W$ is continuous, we have that $W(S_{b_1}, \mathcal{C}(\mathcal{D}); b^1_1, \mathbf{u})$ is connected. Since $x^1, x^2 \in S_{b_1}$, we have $b^1 \in W(S_{b_1}, \mathcal{C}(\mathcal{D}); b^1_1, \mathbf{u})$. Therefore, $b^1 \in y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u})$. Hence, $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$, which implies $S \notin \mathcal{W}$. ■

Theorem 1 implies that to check whether $S \in \mathcal{W}$, it is sufficient to only consider the trajectories of the system with constant inputs $\mathbf{u}_M$ and $\mathbf{u}_m$. In particular, one can check membership of $S$ in $\mathcal{W}$ by simply checking whether either of the fixed signals $\mathbf{u}_M$ and $\mathbf{u}_m$ keep all the outputs $y$ outside $\mathbf{B}$. If none of the extremal signals can keep the outputs outside of the bad set, no other open loop control can. This dramatically reduces the computational demand since it removes the need to search for all possible control signals to determine whether a set is a member of $\mathcal{W}$.

Consider now system $\Sigma = \Sigma^1 \parallel \Sigma^2 \parallel \cdots \parallel \Sigma^k$, in which $\Sigma^i$ are input/output order preserving with scalar output $\mathcal{Y}^i = \mathbb{R}$. For $a, b = 1, \cdots, k$ with $a < b$, define $\Sigma^{ab} := \Sigma^a \parallel \Sigma^b$ and use superscript $ab$ for all signals, states, and outputs of system $\Sigma^{ab}$. Also define the bad set for system $\Sigma^{ab}$ as $\mathbf{B}^{ab} := \mathbf{B}^a \times \mathbf{B}^b$. Since $\mathbf{B}^i \subseteq \mathbb{R}$ are connected, we have that $\mathbf{B}^i$ is an interval. Since systems $\Sigma^i$ are input/output order preserving, system $\Sigma^{ab}$ is also input/output order preserving according to Definition 1 with minimal and maximal input values given by $u^{ab}_m = (u^a_M, u^b_m)$ and $u^{ab}_M = (u^a_m, u^b_M)$, respectively, according to the cone $\Delta^{ab}_u := \{(u^a, u^b) \mid u^a \leq_{\Delta^a_u} 0 \text{ and } u^b \geq_{\Delta^b_u} 0\}$, and minimal and maximal control signals given by $\mathbf{u}^{ab}_m(t) = u^{ab}_m$ and $\mathbf{u}^{ab}_M(t) = u^{ab}_M$ for all $t \in \mathbb{R}_+$, respectively. For systems $\Sigma^{ab},\ a, b = 1, \cdots, k,\ a < b$ and a given $\mathbf{u}^{ab} \in \mathcal{C}(\mathcal{U}^{ab})$ we define the set

$$\begin{aligned} C_{\mathbf{u}^{ab}} := \{x^{ab} \in X^{ab} \mid \exists\ \mathbf{d} \in \mathcal{C}(\mathcal{D}^{ab})\ s.t. \\ y^{ab}(\mathbb{R}_+, x^{ab}, \mathbf{d}^{ab}, \mathbf{u}^{ab}) \cap \mathbf{B}^{ab} \neq \emptyset\}. \end{aligned} \tag{4}$$

**Theorem 2:** Given system $\Sigma = \Sigma^1 \parallel \Sigma^2 \parallel \cdots \parallel \Sigma^k$, in which $\Sigma^i$ are input/output order preserving with $\mathcal{Y}^i = \mathbb{R}$. Then $S = S^1 \times ... \times S^k \in \mathcal{W}$ if and only if there exist $a, b \in \{1, \cdots, k\}$ with $a < b$, such that

$$S^a \times S^b \cap C_{\mathbf{u}_m^{ab}} = \emptyset \text{ or } S^a \times S^b \cap C_{\mathbf{u}_M^{ab}} = \emptyset. \tag{5}$$

*Proof:* We first prove that if $S \notin \mathcal{W}$, then (5) does not hold. If $S \notin \mathcal{W}$, then for all $\mathbf{u} \in \mathcal{C}(\mathcal{U})$ we have $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$. Therefore, for all $a, b \in \{1, \cdots, k\}$ and $a < b$, for system $\Sigma^{ab}$ the output trajectory intersects $\mathbf{B}^a \times \mathbf{B}^b = \mathbf{B}^{ab}$, i.e., (5) does not hold.

Second, we prove that if (5) does not hold, then $S \notin \mathcal{W}$. Given an arbitrary signal $\mathbf{u} = (\mathbf{u}^1, \cdots, \mathbf{u}^k) \in \mathcal{C}(\mathcal{U})$, we want to show that $y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$. The proof proceeds in two steps. First we show that for all $a, b \in \{1, \cdots, k\}$ and $a < b$,

$$(y_a(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}), y_b(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u})) \cap \mathbf{B}^a \times \mathbf{B}^b \neq \emptyset. \tag{6}$$

Then using (6), we show that there exists $t \in \mathbb{R}_+$ such that for all $s = 1, \cdots, k$, $y_s(t, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B}^s \neq \emptyset$, which will be shown to be equivalent to $y(t, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$.

According to Definition 1, we have that $y^s(t, x_0^s, \mathbf{d}^s, \mathbf{u}_m^s) \leq y^s(t, x_0^s, \mathbf{d}^s, \bar{\mathbf{u}}^s) \leq y^s(t, x_0^s, \mathbf{d}^s, \mathbf{u}_M^s)$, $t \in \mathbb{R}_+, s = 1, \cdots, k$. Therefore, for system $\Sigma^{ab}$, $y^{ab}(t, x_0^{ab}, \mathbf{d}^{ab}, \mathbf{u}^{ab})$ belongs to the rectangle defined by opposite vertexes $y^{ab}(t, x_0^{ab}, \mathbf{d}^{ab}, \mathbf{u}_m^{ab})$ and $y^{ab}(t, x_0^{ab}, \mathbf{d}^{ab}, \mathbf{u}_M^{ab})$. Since output trajectories are strictly increasing with respect to time according to Assumption 1, the output trajectories generated by $\mathbf{u}_m^{ab}$ and $\mathbf{u}_M^{ab}$ envelope all trajectories from below and above, respectively. Therefore, Definition 1 holds for system $\Sigma^{ab}$ when the input space $\mathcal{U}^a \times \mathcal{U}^b$ is ordered with respect to the cone $\Delta_u^{ab} := \{(u^a, u^b) \mid u^a \leq_{\Delta_u^a} 0 \text{ and } u^b \geq_{\Delta_u^b} 0\}$. From (5) not holding, we have that there exists $t \in \mathbb{R}_+$ such that $(y^a(t, S^a, \mathcal{C}(\mathcal{D}^a), \mathbf{u}_M^a), y^b(t, S^b, \mathcal{C}(\mathcal{D}^b), \mathbf{u}_m^b)) \cap \mathbf{B}^{ab} \neq \emptyset$ and $(y^a(t, Sa, \mathcal{C}(\mathcal{D}^a), \mathbf{u}_m^a), y^b(t, S^b, \mathcal{C}(\mathcal{D}^b), \mathbf{u}_M^b)) \cap \mathbf{B}^{ab} \neq \emptyset$. Therefore, applying Theorem 1 to system $\Sigma^{ab}$, for any arbitrary control signal $\mathbf{u}$, there exists $t \in \mathbb{R}_+$ such that

$$(y^a(t, S^a, \mathcal{C}(\mathcal{D}^a), \mathbf{u}^a), y^b(t, S^a, \mathcal{C}(\mathcal{D}^b), \mathbf{u}^b)) \cap \mathbf{B}^{ab} \neq \emptyset. \tag{7}$$

According to Assumption 1, trajectories $y^a$ and $y^b$ are strictly increasing with respect to time. Moreover, since $S$ is connected, the flow is continuous with respect to time and with respect to initial state and disturbance signal, we have that $y^a(t, S^a, \mathcal{C}(\mathcal{D}^a), \mathbf{u}^a)$ and $y^b(t, S^b, \mathcal{C}(\mathcal{D}^b), \mathbf{u}^b)$ are intervals. Therefore, there are time intervals $T_a := [t(a)_m, t(a)_M]$ and $T_b := [t(b)_m, t(b)_M]$ such that

$$y^a(t, S^a, \mathcal{C}(\mathcal{D}^a), \mathbf{u}^a) \cap \mathbf{B}^a \neq \emptyset \text{ if and only if } t \in T_a \tag{8}$$

$$y^b(t, S^b, \mathcal{C}(\mathcal{D}^b), \mathbf{u}^b) \cap \mathbf{B}^b \neq \emptyset \text{ if and only if } t \in T_b. \tag{9}$$

According to (7), there exists $t \in \mathbb{R}_+$ such that $y^a(t, S^a, \mathcal{C}(\mathcal{D}^a), \mathbf{u}^a) \cap \mathbf{B}^a \neq \emptyset$ and $y^b(t, S^b, \mathcal{C}(\mathcal{D}^b), \mathbf{u}^b) \cap \mathbf{B}^b \neq \emptyset$. Hence, from (8) and (9), we have that $T_a \cap T_b \neq \emptyset$. Since $a$ and $b$ were arbitrarily chosen, for all $a, b \in \{1, \cdots, k\}$, $T_a \cap T_b \neq \emptyset$. Therefore, $t(a)_m \leq t(b)_M$ for all $a, b \in \{1, \cdots, n_r\}$. Define $t_{min} := \max_{p \in \{1, \cdots, k\}} t(p)_m$, for all $p \in \{1, \cdots, k\}$, $t_{min} \in T_p$. Hence, according to (8) and (9), for all $p \in \{1, \cdots, k\}$ $t_{min} \leq t(p)_M$. By definition, we have $t_{min} \geq t(p)_m$. Therefore, for all $p \in \{1, \cdots, k\}$, $y^p(t_{min}, S^p, \mathcal{C}(\mathcal{D}^p), \mathbf{u}^p) \cap \mathbf{B}^p \neq \emptyset$. Since, $y(t_{min}, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) = \prod_{p=1}^{k} y^p(t_{min}, S^p, \mathcal{C}(\mathcal{D}^p), \mathbf{u}^p)$ and $\mathbf{B} := \mathbf{B}^1 \times \cdots \mathbf{B}^k$, we have $y(t_{min}, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \cap \mathbf{B} \neq \emptyset$. Since $\mathbf{u}$ is any arbitrary control signal, we have $S \notin \mathcal{W}$. ■

This result implies that to check membership of $S$ in $\mathcal{W}$, it is enough to check for all non-repeated $n(n-1)$ pairs of systems $(\Sigma^i, \Sigma^j)$ whether $S^i \times S^j$ intersect both $C_{\mathbf{u}_m^{i,j}}$ and $C_{\mathbf{u}_M^{i,j}}$. If there is at least one pair $(i, j)$ for which these two sets are not both intersected, then $S \in \mathcal{W}$. Explicit checks to determine this intersection are given in Section V.

### A. The case of perfect state information and no disturbance input

In the case in which the state is exactly measured and no disturbance inputs are present ($\mathcal{D} = \emptyset$), Theorem 2 can be extended to the case in which some of $\Sigma_i$ have two-dimensional output $\mathcal{Y}^i = \mathbb{R}^2$. Let then $r_i \in \{1, 2\}$ be the dimension of the output space for system $\Sigma^i$ and define $n_r := \sum_{i=1}^{k} r_i$. In this case, the $s$th element of the output vector $y$ of $\Sigma$, denoted by $y_s$, corresponds to a system $\Sigma^i$ with output $y^i$. If the dimension of the output space of system $\Sigma^i$ is one then $y_s = y^i$ and if the dimension of the output space is two then either $y_s = y_1^i$ or $y_s = y_2^i$. For $a, b \in \{1, \cdots, n_r\}$, $a \neq b$, let $\Sigma^i$ and $\Sigma^j$ be the systems corresponding to $y_a$ and $y_b$, respectively. We define the system $\Sigma^{ab}$ as follows:

- If $i \neq j$, then $\Sigma^{ab} := \Sigma^i || \Sigma^j$, $y^{ab} = (y_a, y_b)$, and $\mathcal{U}^{ab} := \mathcal{U}^i \times \mathcal{U}^j$.
- If $i = j$, then $\Sigma^{ab} := \Sigma^i$, $y^{ab} = y^i$, and $\mathcal{U}^{ab} := \mathcal{U}^i$.

We introduce the following additional assumption.

*Assumption 2:* For all those systems $\Sigma^i$ with $\mathcal{Y}^i = \mathbb{R}^2$, we have the following properties

(i) For all $\mathbf{u}^i \in \mathcal{C}(\mathcal{U}^i)$ $y^i(t, x^i, \mathbf{d}^i, \mathbf{u}_m^i) \leq_{\Delta_y} y^i(t, x^i, \mathbf{d}^i, \mathbf{u}^i) \leq_{\Delta_y} y^i(t, x^i, \mathbf{d}^i, \mathbf{u}_M^i)$, for all $x^i \in X^i$, $\mathbf{d}^i \in \mathcal{C}(\mathcal{D}^i), t \in \mathbb{R}_+$, where the inequalities are defined with respect to the cone $\Delta_y = \{y \in \mathbb{R}^2 \mid y_1 \leq 0, y_2 \geq 0\}$;

(ii) There exists $\xi > 0$ such that $\frac{d}{dt} y_l^i(t, x^i, \mathbf{d}^i(t), \mathbf{u}^i(t)) \geq \xi$, $i = 1, \cdots, k$ and $l = 1, 2$ for all $t \in \mathbb{R}_+$, $\mathbf{u}^i \in \mathcal{C}(\mathcal{U}^i)$, and $\mathbf{d}^i \in \mathcal{C}(\mathcal{D}^i)$;

(iii) The bad set $\mathbf{B}^i$ is a rectangle.

Assumption 2(i) implies, in particular, that $\Sigma^i$ is input/output order preserving, but it has a stronger requirement. It requires that extremal output trajectories "envelop" all others time-wise as opposed to just geometrically in the plane (Definition 1). We let $\mathbf{B}_s$ denote the $s^{th}$ interval of $\mathbf{B}$. If $i = j$, then $\Sigma^{ab} = \Sigma^i$ and therefore it is input/output order preserving according to Definition 1. If $i \neq j$, then $\Sigma^{ab}$ will be a system with two outputs, one corresponding to an output of system $\Sigma^i$ and the other corresponding to an output of system $\Sigma^j$. For system $\Sigma^{ab}$ to be input/output order preserving according to Definition 1 we define its maximal and minimal inputs $u_M^{ab}$ and $u_m^{ab}$ as follows. If $i \neq j$, $y_a = y_1^i$, $y_b = y_1^j$, set $u_m^{ab} = (u_m^i, u_M^j)$ and $u_M^{ab} = (u_M^i, u_m^j)$. If $i \neq j$, $y_a = y_1^i$, $y_b = y_2^j$, set $u_m^{ab} = (u_m^i, u_m^j)$ and $u_M^{ab} = (u_M^i, u_M^j)$. If $i \neq j$, $y_a = y_2^i$, $y_b = y_1^j$, set $u_m^{ab} = (u_M^i, u_M^j)$ and $u_M^{ab} = (u_m^i, u_m^j)$. If $i \neq j$, $y_a = y_2^i$, $y_b = y_2^j$, set $u_m^{ab} = (u_M^i, u_m^j)$ and $u_M^{ab} = (u_m^i, u_M^j)$. If $i = j$, $u_l^{ab} = u_l^i,\ l = m, M$. The maximal and minimal input signals are $\mathbf{u}_M^{ab}(t) = u_M^{ab}$ and $\mathbf{u}_m^{ab}(t) = u_m^{ab}$ for all $t \in \mathbb{R}_+$, respectively.

Once perfect state information is available and no disturbance is present, i.e., $\mathcal{D} = \emptyset$, the maximal safe controlled invariant set for system $\Sigma$ takes the following form:

$$\mathcal{W} = \{x \in X \mid \exists\ \mathbf{u} \in \mathcal{C}(\mathcal{U}),\ s.t.\ y(\mathbb{R}_+, x, \mathbf{u}) \cap \mathbf{B} = \emptyset\}. \tag{10}$$

Given $\mathbf{u} \in \mathcal{C}(\mathcal{U})$, the set $C_{\mathbf{u}}$ defined in (3) also modifies to

$$C_{\mathbf{u}} = \{x \in X \mid y(\mathbb{R}_+, x, \mathbf{u}) \cap \mathbf{B} \neq \emptyset\}. \tag{11}$$

Similarly, for a given $\mathbf{u}^{ab}$, the set $C_{\mathbf{u}^{ab}}$ defined in (4) for system $\Sigma^{ab}$ with $\mathbf{B}^{ab} = \mathbf{B}_a \times \mathbf{B}_b$ takes the form

$$C_{\mathbf{u}^{ab}} := \{x^{ab} \in X^{ab} \mid y^{ab}(\mathbb{R}_+, x^{ab}, \mathbf{u}^{ab}) \cap \mathbf{B}^{ab} \neq \emptyset\}. \tag{12}$$

**Theorem 3:** Let $\Sigma = \Sigma^1 \parallel \Sigma^2 \parallel \cdots \parallel \Sigma^k$, in which $\Sigma^i$ can have output $\mathcal{Y}^i = \mathbb{R}^2$, it is input/output order preserving, and satisfies Assumption 2. Then, $x_0 \in \mathcal{W}$ if and only if there exist $a, b \in \{1, \cdots, n_r\}$ with $a < b$ such that $x_0^{ab} \notin C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$.

*Proof:* First we prove that if $x_0 \notin \mathcal{W}$ then $x_0^{ab} \in C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$ for all $a, b \in \{1, \cdots, n_r\}$ with $a < b$. If $x_0 \notin \mathcal{W}$, then according to (10), for all $a, b \in \{1, \cdots, k\}$ with $a \neq b$, and $\mathbf{u} \in \mathcal{C}(\mathcal{U})$, $x_0 \in C_{\mathbf{u}}$. Therefore, there exists $t \in \mathbb{R}_+$ such that $y^i(t, x_0, \mathbf{u}^i) \in \mathbf{B}^i$ for all $i = 1, \cdots, n_r$, so that $x_0^{ab} \in C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$ for all $a, b \in \{1, \cdots, n_r\}$. Second, we prove that if $x_0^{ab} \in C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$ for all $a, b \in \{1, \cdots, n_r\}$, then $x_0 \notin \mathcal{W}$.

Given an arbitrary signal $\mathbf{u} = (\mathbf{u}^1, \cdots, \mathbf{u}^k) \in \mathcal{C}(\mathcal{U})$, we want to show that $y(\mathbb{R}_+, x_0, \mathbf{u}) \cap \mathbf{B} \neq \emptyset$. The proof proceeds in two steps. First we show that for all $a, b \in \{1, \cdots, n_r\}$ and $a < b$,

$$(y_a(\mathbb{R}_+, x_0, \mathbf{u}), y_b(\mathbb{R}_+, x_0, \mathbf{u})) \cap \mathbf{B}_a \times \mathbf{B}_b \neq \emptyset. \tag{13}$$

Then, using (13), we show there exists $t \in \mathbb{R}_+$ such that $y_s(t, x_0, \mathbf{u}) \cap \mathbf{B}_s \neq \emptyset$. This is equivalent to $y(t, x_0, \mathbf{u}) \cap \mathbf{B} \neq \emptyset$.

Depending on the choices of $a$ and $b$, two cases may occur: Case(a): $y_a$ and $y_b$ are trajectories corresponding to a subsystem, i.e., there exists $i \in \{1, \cdots, k\}$ such that $y^i = (y_a, y_b)$. Case(b): $y_a$ and $y_b$ are trajectories corresponding to two different subsystems. Note that Case(a) occurs if for system $\Sigma^i$, $r_i = 2$, $b = a + 1$, and $a = \sum_{j=1}^{i-1} r_j + 1$. In the following, we consider Case(a) and Case(b) separately.

We first introduce the following definition. Let $y_a$ correspond to system $\Sigma^i$ and $y_b$ correspond to system $\Sigma^j$. According to Assumption 2(ii), trajectories $y_a$ and $y_b$ are strictly increasing with respect to time. Therefore, there are time intervals $T_a := [t(a)_m, t(a)_M]$ and $T_b := [t(b)_m, t(b)_M]$ such that

$$y_a(t, x_0^i, \mathbf{u}^i) \in \mathbf{B}_a \text{ if and only if } t \in T_a, \tag{14}$$

$$y_b(t, x_0^j, \mathbf{u}^j) \in \mathbf{B}_b \text{ if and only if } t \in T_b. \tag{15}$$

*Case(a).* If $x_0^{ab} \in C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$ for all $a, b \in \{1, \cdots, n_r\}$, we have $x_0^i \in C_{\mathbf{u}_m^i}$ and $x_0^i \in C_{\mathbf{u}_M^i}$. Therefore, $y^i(\mathbb{R}_+, x_0^i, \mathbf{u}_m^i) \cap \mathbf{B}^i \neq \emptyset$. Similarly, we have $y^i(\mathbb{R}_+, x_0^i, \mathbf{u}_M^i) \cap \mathbf{B}^i \neq \emptyset$. From these and Theorem 1, we have

$$y^i(\mathbb{R}_+, x_0, \mathbf{u}^i) \cap \mathbf{B}^i \neq \emptyset. \tag{16}$$

Since $y^i = (y_a, y_b)$ and $\mathbf{B}^i = \mathbf{B}_a \times \mathbf{B}_b$, (16) leads to (13) for all $a, b = 1, \cdots, n_r,\ a < b$.

*Case(b).* Now we show that (13) holds when $y_a$ and $y_b$ are trajectories corresponding to two subsystems $\Sigma^i$ and $\Sigma^j$, respectively. If $r_i = 1$, then $y_a = y^i$. If $r_i = 2$, then either $y_a = y_1^i$ or $y_a = y_2^i$. According to Assumption 2, if $y_s = y_1^i$ we have $y_s(t, x_0^i, \mathbf{d}^i, \mathbf{u}_M^i) \leq y_s(t, x_0^i, \mathbf{d}^i, \bar{\mathbf{u}}^i) \leq y_s(t, x_0^i, \mathbf{d}^i, \mathbf{u}_m^i),\ t \in \mathbb{R}_+,\ s = 1, \cdots, n_r$, and if $y_s = y_2^i$ we have that $y_s(t, x_0^i, \mathbf{d}^i, \mathbf{u}_m^i) \leq y_s(t, x_0^i, \mathbf{d}^i, \bar{\mathbf{u}}^i) \leq y_s(t, x_0^i, \mathbf{d}^i, \mathbf{u}_M^i),\ t \in \mathbb{R}_+,\ s = 1, \cdots, n_r$, for $s \in \{a, b\}$. Let $\mathbf{B}^{ij} := \mathbf{B}_a \times \mathbf{B}_b$. Then, system $\Sigma^{ab}$ is input/output order preserving according to Definition 1 when the input space $\mathcal{U}^i \times \mathcal{U}^j$ is ordered with respect to the cone $\Delta_u^{ij} := \{(u^i, u^j) \mid (-1)^l u^i >_{\Delta_u^i} 0 \text{ and } (-1)^{l'} u^j >_{\Delta_u^j} 0\}$ with appropriate choice of $l \in \{0, 1\}$ and $l' \in \{0, 1\}$. Let $\mathbf{u}_m^{ij}$ and $\mathbf{u}_M^{ij}$ denote the minimal and maximal point of $\mathcal{C}(\mathcal{U}^i) \times \mathcal{C}(\mathcal{U}^j)$. Depending on the values of $l$ and $l'$, the pair of the minimal and maximal points, $[\mathbf{u}_m^{ij}, \mathbf{u}_M^{ij}]$, is one of the pairs $[(\mathbf{u}_m^i, \mathbf{u}_M^j), (\mathbf{u}_M^i, \mathbf{u}_m^j)]$, $[(\mathbf{u}_m^i, \mathbf{u}_m^j), (\mathbf{u}_M^i, \mathbf{u}_M^j)]$,

$[(\mathbf{u}_M^i, \mathbf{u}_M^j), (\mathbf{u}_m^i, \mathbf{u}_m^j)]$, or $[(\mathbf{u}_M^i, \mathbf{u}_m^j), (\mathbf{u}_m^i, \mathbf{u}_M^j)]$. From $x_0^{ab} \in C_{\mathbf{u}_m^{ab}} \cap C_{\mathbf{u}_M^{ab}}$ for all $a, b \in \{1, \cdots, n_r\}$, we have that the trajectories, corresponding to maximal and minimal control signals in the control space $\mathcal{C}(\mathcal{U}^i) \times \mathcal{C}(\mathcal{U}^j)$ intersect $\mathbf{B}^{ij}$. Therefore, Theorem 1 holds for system $\Sigma^{ab}$. Consequently, according to Theorem 1, (13) holds.

Considering Cases (a) and (b), we know (13) holds. Namely, there exists $t \in \mathbb{R}_+$ such that $y_a(t, x_0, \mathbf{u}) \in \mathbf{B}_a$ and $y_b(t, x_0, \mathbf{u}) \in \mathbf{B}_b$. Hence, according to (14) and (15), $t \in T_a$ and $t \in T_b$. Consequently, we have that for all $a, b \in \{1, \cdots, n_r\}$, $T_a \cap T_b \neq \emptyset$. Therefore, $t(a)_m \leq t(b)_M$ for all $a, b \in \{1, \cdots, n_r\}$. Defining $t_{min} := \max_{s \in \{1, \cdots, n_r\}} t(s)_m$, for all $s \in \{1, \cdots, n_r\}$, $t_{min} \in T_s$. Hence, according to (14) and (15), for all $s \in \{1, \cdots, n_r\}$, $y_s(t_{min}, x_0, \mathbf{u}) \in \mathbf{B}_s$. Therefore, $y(t_{min}, x_0, \mathbf{u}) \in \mathbf{B}$. ■

## IV. Solution to Problem 2: The control strategy

First, we solve Problem 2 for the case in which $\Sigma$ is an input/output order preserving system with $\mathcal{Y} = \mathbb{R}^2$. Then, we exploit this result to provide the solution to Problem 2 for the parallel composition of input/output order preserving systems. Specifically, consider the following set-valued map $K : 2^X \to 2^{\mathcal{U}}$:

$$K(S) = \begin{cases} u_m & \text{if } S \cap C_{\mathbf{u}_M} \neq \emptyset, \\ & S \cap C_{\mathbf{u}_m} = \emptyset \text{ and } S \cap \partial C_{\mathbf{u}_m} \neq \emptyset \\ u_M & \text{if } S \cap C_{\mathbf{u}_m} \neq \emptyset,\ S \cap C_{\mathbf{u}_M} = \emptyset \\ & \text{and } S \cap \partial C_{\mathbf{u}_M} \neq \emptyset \\ \{u_m, u_M\} & \text{if } S \cap C_{\mathbf{u}_M} = \emptyset,\ S \cap C_{\mathbf{u}_m} = \emptyset, \\ & S \cap \partial C_{\mathbf{u}_m} \neq \emptyset \text{ and } S \cap \partial C_{\mathbf{u}_M} \neq \emptyset \\ \mathcal{U} & \text{otherwise,} \end{cases} \tag{17}$$

then, we have the following result.

**Theorem 4:** Let $\Sigma$ be an input/output order preserving system. Let $S \subset \mathbb{R}^n$ be a compact set such that $S \in \mathcal{W}$. If

$$\mathbf{u}(t) \in K(\hat{x}(t, S, \mathbf{u}([0, t)), \mathbf{z})),\ \forall t \tag{18}$$

then $g(\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z})) \cap \mathbf{B} = \emptyset$ for all $\mathbf{z} \in S(\mathcal{M})$.

*Proof:* Define $\mathbb{B} := g^{-1}(\mathbf{B})$ and note that $g(\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z})) \cap \mathbf{B} = \emptyset$ if and only if $\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z}) \cap \mathbb{B} = \emptyset$. Therefore, we prove the result for the latter.

We introduce a fictitious control strategy that is the same as the control strategy (17) as long as the state estimate set $\hat{x}$ does not intersect the sets $C_{\mathbf{u}_M}$ and $C_{\mathbf{u}_m}$ simultaneously. The introduced fictitious control strategy is different from (17) only if $\hat{x} \cap C_{\mathbf{u}_M} \neq \emptyset$ and $\hat{x} \cap C_{\mathbf{u}_m} \neq \emptyset$. Since $S \in \mathcal{W}$ is equivalent by Theorem 1 to $S \cap C_{\mathbf{u}_m} = \emptyset$ or $S \cap C_{\mathbf{u}_M} = \emptyset$, it will be shown that the latter implies that $\hat{x}$ does not intersect the sets $C_{\mathbf{u}_M}$ and $C_{\mathbf{u}_m}$ simultaneously, under the fictitious control strategy. Hence, the actual control strategy (17) also prevents $\hat{x}$ from intersecting both $C_{\mathbf{u}_m}$ and $C_{\mathbf{u}_M}$ at the same time and therefore $\hat{x}$ is kept in $\mathcal{W}$ and, as a consequence, does not intersect $\mathbb{B}$.

The fictitious control strategy is a map with memory defined as follows

$$\hat{K}(S([0,t])) = \left\{ \begin{array}{cc} u_m & \text{if } S(t) \cap C_{\mathbf{u}_M} \neq \emptyset, \\ & S(t) \cap C_{\mathbf{u}_m} = \emptyset \text{ and} \\ & S(t) \cap \partial C_{\mathbf{u}_m} \neq \emptyset \\ u_M & \text{if } S(t) \cap C_{\mathbf{u}_m} \neq \emptyset, \\ & S(t) \cap C_{\mathbf{u}_M} = \emptyset \\ & \text{and } S(t) \cap \partial C_{\mathbf{u}_M} \neq \emptyset \\ \{u_m, u_M\} & \text{if } S(t) \cap C_{\mathbf{u}_M} = \emptyset, \\ & S(t) \cap C_{\mathbf{u}_m} = \emptyset, \\ & S(t) \cap \partial C_{\mathbf{u}_m} \neq \emptyset \\ & \text{and } S(t) \cap \partial C_{\mathbf{u}_M} \neq \emptyset \\ \mathcal{U} & \text{if } S(t) \cap Cl(C_{\mathbf{u}_m}) = \emptyset \text{ or} \\ & S(t) \cap Cl(C_{\mathbf{u}_M}) = \emptyset \\ K(S(\tilde{t})) & \text{otherwise} \end{array} \right. \tag{19}$$

where $\tilde{t} := \sup\{\check{t} < t \mid S(\check{t}) \cap C_{\mathbf{u}_m} = \emptyset \text{ or } S(\check{t}) \cap C_{\mathbf{u}_M} = \emptyset\}$. We first show that with the control law

$$\mathbf{u}(t) \in \hat{K}(\hat{x}(t, S, \mathbf{u}([0,t)), \mathbf{z})) \tag{20}$$

the statement of the theorem holds.

Assume $S \cap C_{\mathbf{u}_m} = \emptyset$ and let $\mathbf{u}$ be the control signal that complies with (20). If for all $t \in \mathbb{R}_+$, $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$ or $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} = \emptyset$ then the proof is complete. Otherwise, there is a time $t_1 \in \mathbb{R}_+$ such that $\hat{x}(t_1, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} \neq \emptyset$ and $\hat{x}(t_1, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} \neq \emptyset$, Define $\bar{t}$ as $\bar{t} := \sup\{t \in [0, t_1] | \; \hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset\}$. Since $C_{\mathbf{u}_m}$ is open by the continuity of the flow and openness of $\mathbf{B}$, from Lemma 1 in Appendix we have $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$. Now, we show that

$$\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap \partial C_{\mathbf{u}_m} \neq \emptyset. \tag{21}$$

By contradiction argument, assume that $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap \partial C_{\mathbf{u}_m} = \emptyset$. By Lemma 1 in Appendix, we have that $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \subset\sim Cl(C_{\mathbf{u}_m})$. Since $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z})$ is compact, there exists $\epsilon > 0$ such that

$$\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \oplus B_\epsilon(0) \subset\sim Cl(C_{\mathbf{u}_m}). \tag{22}$$

Since $\phi$ is upper-hemicontinuous (by the continuity of the flow), there exists $\delta > 0$ such that for all $t \in [\bar{t}, \bar{t}+\delta)$, $\phi(t, \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}), \mathcal{C}(\mathcal{D}), \mathbf{u}) \subset \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) + B_\epsilon(0)$. Since $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \subset \phi(t, \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}), \mathcal{C}(\mathcal{D}), \mathbf{u})$, according to (22), we have

$$\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \subset\sim Cl(C_{\mathbf{u}_m}),\ \forall\ t \in [\bar{t}, \bar{t}+\delta). \tag{23}$$

Hence, $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$ for all $t \in [\bar{t}, \bar{t}+\delta)$, which contradicts the definition of $\bar{t}$. Therefore, equation (21) holds.

Let $\bar{t}_1$ be defined as $\bar{t}_1 := \sup\{t \in [0, t_1] |\ \hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} = \emptyset\}$. With a similar argument applied to $C_{u_M}$, we have that $\hat{x}(\bar{t}_1, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} = \emptyset$ and $\hat{x}(\bar{t}_1, S, \mathbf{u}, \mathbf{z}) \cap \partial C_{\mathbf{u}_M} \neq \emptyset$. We then have three possible cases: $\bar{t} > \bar{t}_1$, $\bar{t} = \bar{t}_1$, or $\bar{t} < \bar{t}_1$. We consider the first case where $\bar{t} > \bar{t}_1$. According to the definition of $\bar{t}_1$, for all $t \in (\bar{t}_1, t_1]$, we have that $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} \neq \emptyset$. Therefore, $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} \neq \emptyset$. Moreover, from (21) we have $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap \partial C_{\mathbf{u}_m} \neq \emptyset$ and $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$. According to (20), $\mathbf{u}(\bar{t}) = u_m$. Moreover (Lemma 1 in Appendix), for all $t \in (\bar{t}, t_1]$,

$$\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} \neq \emptyset. \tag{24}$$

Then, by control law (20), $\mathbf{u}(t) = u_m$, for $t \in [\bar{t}, t_1]$. Since, $\phi(0, \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}), \mathbf{u}, \mathbf{d}) \cap C_{\mathbf{u}_m} = \emptyset$, with control signal $\mathbf{u}(t) = u_m$ for $t \in [\bar{t}, t_1]$ and $\mathbf{d} \in \mathcal{C}(\mathcal{D})$, we have that $\phi(t - \bar{t}, \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}), \mathbf{u}, \mathbf{d}) \cap C_{\mathbf{u}_m} = \emptyset$, for $t \in (\bar{t}, t_1]$. Moreover, for $t \in [\bar{t}, t_1]$, $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \subset \phi(t - \bar{t}, \hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}), \mathbf{u}, \mathcal{C}(\mathcal{D}))$. Therefore, for $t \in (\bar{t}, t_1]$, $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$, which contradicts (24). Therefore, under the control law (20), $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_m} = \emptyset$ or $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C_{\mathbf{u}_M} = \emptyset$, for all $t \in \mathbb{R}_+$. Hence, under control law (20), $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap \mathbb{B} = \emptyset$, for all $t \in \mathbb{R}_+$. The cases where $\bar{t} = \bar{t}_1$ or $\bar{t} < \bar{t}_1$ can be treated in a similar way.

Hence, under the control law (20) the last condition in equation (20) will never occur. Therefore, it can be substituted by $\hat{K}(S(t)) = \mathcal{U}$ which results in the control law (18) with the same property as (20). That is, under control law (18), $\hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap \mathbb{B} = \emptyset$, for all $t \in \mathbb{R}_+$. ■

According to this theorem, the map (17) used as a feedback control law from the current state estimate $\hat{x}(t) \in \mathcal{W}$ guarantees that $\hat{x}(t)$ is kept in $\mathcal{W}$ and the output corresponding to the current state estimate never intersects the bad set. The employment of a closed loop control as opposed to an open loop control allows for less conservative controllers. In fact, while the initial state uncertainty $S$ may require restricting the control actions from $\mathcal{U}$ to $u_m$ or $u_M$, for example, the current state estimate $\hat{x}(t)$ may very well not require the same restriction.

When $\Sigma = \Sigma^1 \parallel \Sigma^2 \parallel \cdots \parallel \Sigma^k$ with $\Sigma^i$ input/output order preserving systems, consider system $\Sigma^{ab}$ and the sets defined in (4). Define the set valued map $K_{\Sigma^{ab}} : 2^{X^{ab}} \rightarrow \mathcal{U}^{ab}$ as follows

$$K_{\Sigma^{ab}}(S) = \begin{cases} u_m^{ab} & \text{if } S \cap C_{\mathbf{u}_M^{ab}} \neq \emptyset, \\ & S \cap C_{\mathbf{u}_m^{ab}} = \emptyset \\ & \text{and } S \cap \partial C_{\mathbf{u}_m^{ab}} \neq \emptyset \\ u_M^{ab} & \text{if } S \cap C_{\mathbf{u}_m^{ab}} \neq \emptyset, \\ & S \cap C_{\mathbf{u}_M^{ab}} = \emptyset \\ & \text{and } S \cap \partial C_{\mathbf{u}_M^{ab}} \neq \emptyset \\ \{u_m^{ab}, u_M^{ab}\} & \text{if } S \cap C_{\mathbf{u}_M^{ab}} = \emptyset, \\ & S \cap C_{\mathbf{u}_m^{ab}} = \emptyset, \\ & S \cap \partial C_{\mathbf{u}_m^{ab}} \neq \emptyset \\ & \text{and } S \cap \partial C_{\mathbf{u}_M^{ab}} \neq \emptyset \\ \mathcal{U}^{ab} & \text{otherwise.} \end{cases} \tag{25}$$

Given the set of states $S = S^1 \times \cdots \times S^k \subset X$ for system $\Sigma$, define the set of pairs $(a, b)$, $Pair(S)$, as follows

$$\begin{aligned} Pair(S) := \{(a, b) \mid a, b \in \{1, \cdots, n_r\},\ a < b, \\ S^{ab} \cap C_{\mathbf{u}_m^{ab}} = \emptyset \text{ or } S^{ab} \cap C_{\mathbf{u}_M^{ab}} = \emptyset\}. \end{aligned} \tag{26}$$

According to this definition, $(a, b) \in Pair(S)$ if the set of states $S^{ab}$ of system $\Sigma^{ab}$ with bad set $\mathbf{B}^{ab} = \mathbf{B}_a \times \mathbf{B}_b$ belongs to the corresponding maximal safe controlled invariant set.

The control map $K(S)$ for system $\Sigma$ is defined as follows

$$\begin{aligned} K_\Sigma(S) := \{u \in \mathcal{U} \mid \exists\ (a, b) \in Pair(S) \\ s.t.\ u^{ab} \in K_{\Sigma^{ab}}(S^{ab})\}. \end{aligned} \tag{27}$$

**Theorem 5:** Let $\Sigma = \Sigma^1 \parallel \Sigma^2 \parallel \cdots \parallel \Sigma^k$ with $\Sigma^i$ input/output order preserving systems. If some $\mathcal{Y}^i = \mathbb{R}^2$ we also let Assumption 2 hold, $\mathcal{D} = \emptyset$, and perfect state information. Let the set of initial states $S \subset X$ be a compact set such that $S \in \mathcal{W}$. If

$$\mathbf{u}(t) \in K_\Sigma(\hat{x}(t, S, \mathbf{u}([0, t)), \mathbf{z})),\ \forall t \tag{28}$$

then $g(\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z})) \cap \mathbf{B} = \emptyset$ for all $\mathbf{z} \in S(\mathcal{M})$.

*Proof:* Note that $g(\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z})) \cap \mathbf{B} = \emptyset$ if and only if $\hat{x}(\mathbb{R}_+, S, \mathbf{u}, \mathbf{z}) \cap \mathbb{B} = \emptyset$, with $\mathbb{B} = g^{-1}(\mathbf{B})$. Therefore, we prove the theorem for the latter. By virtue of Theorem 2 and Theorem 3, we have that $S \in \mathcal{W}$ is equivalent to $Pair(S) \neq \emptyset$. Assume there exists $t_1 \in \mathbb{R}_+$ such that

$$Pair(\hat{x}(t_1, S, \mathbf{u}, \mathbf{z})) = \emptyset. \tag{29}$$

Let $Pair(\hat{x}(0, S, \mathbf{u}, \mathbf{z})) = Pair(S) \neq \emptyset$ and define $\bar{t} := \sup\{t \in [0, t_1] \mid Pair(\hat{x}(t, S, \mathbf{u}, \mathbf{z})) \neq \emptyset\}$. We first show that $Pair(\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z})) \neq \emptyset$. Considering $\mathbf{z}^{ab}$ as the measurement signal and $\hat{x}^{ab}(\cdot)$ the estimated state of system $\Sigma^{ab}$, define $\bar{t}^{ab} := \sup\{t \in [0, t_1] \ \mid \hat{x}^{ab}(t, S^{ab}, \mathbf{u}^{ab}, \ \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_m} = \emptyset$ or $\hat{x}^{ab}(t, S^{ab}, \mathbf{u}^{ab}, \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_M} = \emptyset\}$. According to (26),

$$\bar{t} = \max\{\bar{t}^{ab} \mid (a, b) \in Pair(S)\}. \tag{30}$$

Since $C_{\mathbf{u}^{ab}_m}$ and $C_{\mathbf{u}^{ab}_M}$ are open sets, according to Lemma 1 in Appendix, for all $(a, b) \in Pair(S)$, $\hat{x}^{ab}(\bar{t}^{ab}, S^{ab}, \mathbf{u}^{ab}, \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_m} = \emptyset$ or $\hat{x}^{ab}(\bar{t}^{ab}, S^{ab}, \ \mathbf{u}^{ab}, \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_M} = \emptyset$. Therefore, from (30), we have $Pair(\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z})) \neq \emptyset$.

We proceed by introducing a fictitious control strategy that is the same as (28) as long as $Pair(\hat{x}(t, S, \mathbf{u}, \mathbf{z})) \neq \emptyset$. We prove that $Pair(\hat{x}(t, S, \mathbf{u}, \mathbf{z})) \neq \emptyset$ for all $t \in \mathbb{R}_+$ and thereby the proof is complete. The fictitious control strategy is a map with memory as follows:

$$\hat{K}(S([0, t])) = \begin{cases} K_\Sigma(S(t)) & \text{if } Pair(S(t)) \neq \emptyset \\ u & \text{otherwise}, \end{cases} \tag{31}$$

where $u \in \mathcal{U}$ is such that $u^{ab} \in K_{\Sigma^{ab}}(S^{ab}(\tilde{t}))$ for some $(a, b) \in Pair(S(\tilde{t}))$ with $\tilde{t} := \sup\{\check{t} < t \mid Pair(S(\check{t})) \neq \emptyset\}$. According to (31), for $t \in [\bar{t} \ t_1]$ we have

$$\mathbf{u}^{ab}(t) \in K_{\Sigma_{ab}}(\hat{x}^{ab}(t, S^{ab}, \mathbf{u}^{ab}, \mathbf{z}^{ab})). \tag{32}$$

By (26) and Theorem 4, system $\Sigma^{ab}$ is such that $\hat{x}^{ab}(t, S^{ab}, \mathbf{u}^{ab}, \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_m} = \emptyset$ or $\hat{x}^{ab}(t, S^{ab}, \mathbf{u}^{ab}, \mathbf{z}^{ab}) \cap C_{\mathbf{u}^{ab}_m} = \emptyset$ for $t \in [\bar{t} \ t_1]$. This contradicts (29). Therefore, under fictitious control strategy (31), and consequently under (28) we have $Pair(\hat{x}(t, S, \mathbf{u}, \mathbf{z})) \neq \emptyset$ for all $t \in \mathbb{R}_+$. ■

Control law (27) determines all possible inputs $u$ that can be applied while avoiding that $\hat{x}^{ab}(t)$ intersects $C_{\mathbf{u}^{ab}_m}$ and $C_{\mathbf{u}^{ab}_M}$ for all $s^1, s^2$. In particular, for restricting the control input $u$, it is required that for all pairs $(s^1, s^2)$ the control input $u^{ab}$ is restricted. In this case, only one pair of components of $u$ will need to be restricted, so that all $u$ that can be applied are those in which one pair $(a, b)$ of components are restricted according to $K_{\Sigma_{ab}}$. As long as there is one pair of components $(a, b)$ for which $K_{\Sigma_{ab}}(\hat{x}^{ab}) = \mathcal{U}^{ab}$, we have that $K_\Sigma(\hat{x}) = \mathcal{U}$.

## V. Algorithm Implementation

When $\Sigma$ is an input/output order preserving system or when it is the parallel composition of input/output order preserving systems with scalar output, Theorem 1 and Theorem 2 determine whether a set $S$ is in $\mathcal{W}$ by checking whether $S$ intersects the sets $C_{\mathbf{u}}$. Furthermore, to implement the control strategy of Theorem 4 and of Theorem 5, we need a procedure to determine whether

$\hat{x}(t, S, \mathbf{u}, \mathbf{z})$ intersects the set $C_{\mathbf{u}}$ or its boundary $\partial C_{\mathbf{u}}$. In order to provide this procedure, we introduce one additional structural assumption on the input/output order preserving systems $\Sigma^i$.

*Assumption 3:* There is a partial order in the state space $X^i$ and on the disturbance space $\mathcal{D}^i$ with the properties:

(i) There are $a^i_m \in S^i$ and $a^i_M \in S^i$ such that $a^i_m \leq a^i \leq a^i_M$ for $a^i \in S^i$.

(ii) There are disturbance signals $\mathbf{d}^i_m$ and $\mathbf{d}^i_M$ such that for all $\mathbf{d}^i \in \mathcal{C}(\mathcal{D}^i)$ we have that $\mathbf{d}^i \geq \mathbf{d}^i_m$ and $\mathbf{d}^i \leq \mathbf{d}^i_M$.

(iii) For all $\mathbf{u}^i \in \mathcal{C}(\mathcal{U}^i)$, $\mathbf{d}^i \in \mathcal{C}(\mathcal{D}^i)$, initial state $a^i \in S^i$, we have that

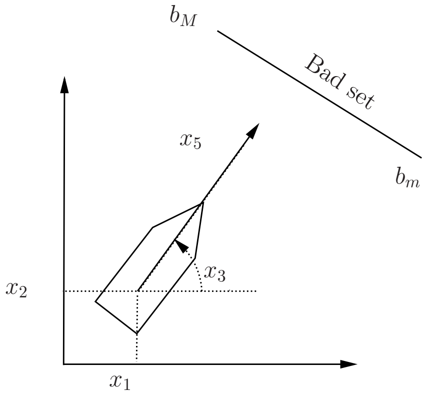
- $y^i(\mathbb{R}_+, a^i_m, \mathbf{d}^i_m, \mathbf{u}^i) \preceq y^i(\mathbb{R}_+, a^i, \mathbf{d}^i, \mathbf{u}^i) \preceq y^i(\mathbb{R}_+, a^i_M, \mathbf{d}^i_M, \mathbf{u}^i)$ if $\mathcal{Y}^i = \mathbb{R}^2$ and
- $y^i(t, a^i_m, \mathbf{d}^i_m, \mathbf{u}^i) \leq y(t, a^i, \mathbf{d}^i, \mathbf{u}^i) \leq y(t, a^i_M, \mathbf{d}^i_M, \mathbf{u}^i)$ if $\mathcal{Y}^i = \mathbb{R}$.

The first item of this assumption requires that the state space $X$ is also equipped with a partial order and that the set $S^i$ has a maximum and a minimum in this partial order. The second item requires that the disturbance space is also equipped with a partial order and that the space of disturbance signals has a minimum and a maximum in the associated partial order. The third item requires that extremal output trajectories obtained with extremal initial conditions in $S^i$ and extremal disturbance signals envelop all possible output trajectories. This property is also weaker than the properties required in earlier works [37], in which it was required that the flow was an order preserving map with respect to all its arguments.

**Theorem 6:** Let $\Sigma$ be an input/output order preserving system with Assumption 1 and let Assumption 3 also hold for $\Sigma$. Let the set $S$ be compact and let $\mathbf{u}$ be an arbitrary control signal. Then $S \cap C_{\mathbf{u}} = \emptyset$ if and only if $\mathbf{B} \succeq y(\mathbb{R}_+, a_M, \mathbf{d}_M, \mathbf{u})$ or $\mathbf{B} \preceq y(\mathbb{R}_+, a_m, \mathbf{d}_m, \mathbf{u})$.

This theorem states that a set $S$ does not intersect $C_{\mathbf{u}}$ if and only if with input $\mathbf{u}$ the output trajectory obtained with maximal disturbance signal and maximal initial condition flows below the bad set or if the output trajectory obtained with minimal disturbance signal and minimal initial condition flows above the bad set. By virtue of Assumption 1, according to which the output flow does not stop, the check of the above theorem can be performed in finite time, that is, in the time required to have the first component of the output trajectory become greater than $\mathbf{B}$. This simple check to determine intersection of $S$ with $C_{\mathbf{u}}$ is all it is required for the implementation of the control strategy.

According to this result, we only need to calculate two extremal finite time trajectories for each of the two extremal control inputs, for $n_r(n_r - 1)/2$ systems. Therefore, the computational demand is of order $n_r^2$, $n_r$ being the dimension of the output space of system $\Sigma$. Note that in the case



(a) Ship coordinate system

| Parameter | value | unit |
|---|---|---|
| $a$ | $1.084$ | 1/min |
| $b$ | $0.62$ | min/rad$^2$ |
| $c$ | $3.553$ | 1/min$^2$ |
| $r_1$ | $-0.0375$ | nm/rad |
| $r_3$ | $0$ | Nm.min$^2$/rad$^3$ |
| $f$ | $0.86$ | 1/min |
| $W$ | $0.067$ | nm/rad$^2$ |

(b) Table I: Parameters of ship model

Fig. 2: (a) Ship coordinate system. The obstacle on the path of the ship is a line segment that connects point $b_m = (8, 5)$ to the point $b_M = (5, 8)$. (b) Parameter values.

in which the current state estimate $\hat{x}$ does not include its supremum or its infimum, the provided checks to determine membership in $\mathcal{W}$ are conservative. The extent of conservatism is directly determined by the distance between the supremum (infimum) and the set $\hat{x}$.

## VI. Application Example I: Ship Maneuvering

As an example to illustrate the application of the proposed algorithm, we consider a system that is input/output order preserving, has imperfect state information and disturbance input. Specifically, we consider the problem of steering a ship from an initial position to a desired target position, where an obstacle must be avoided. The following ship model, taken from [47], is considered:

$$\begin{aligned}
\dot{x}_1 &= x_5 \cos(x_3) - (r_1 x_4 + r_3 x_4^3) \sin(x_3),\\
\dot{x}_2 &= x_5 \sin(x_3) + (r_1 x_4 + r_3 x_4^3) \cos(x_3),\\
\dot{x}_3 &= x_4, \quad \dot{x}_4 = -a x_4 - b x_4^3 + c u_r,\\
\dot{x}_5 &= -f x_5 - W x_4^2 + u_t,
\end{aligned} \tag{33}$$

where $(x_1, x_2)$ is the ship position (in nautical miles (nm)) in the $\mathbb{R}^2$ plane, $x_3$ is the heading angle, $x_4$ is the yaw rate, and $x_5$ is the forward velocity. The two control inputs are: the rudder angle $u_r$ and the propeller thrust $u_t$. Figure 2(a) represents the ship with the coordinates. The model parameters are summarized in Table I (Figure 2(b)). With these parameters, the ship has a maximum speed of 0.25 nm/min = 15 knots for a maximum thrust of 0.215 nm/min$^2$. The maximal rudder angle is $35$ deg, i.e.,

$$|u_r| \leq u_r^m = 0.61 \text{ rad.} \tag{34}$$

With constant propeller thrust $u_t$, and the effect of heading velocity on the speed of the ship being negligible, the speed of the ship is assumed to be constant at $V = 0.25$ nm/min. Therefore, for the forward velocity $x_5$, we have that $x_5(t) = V$ for all $t \geq 0$. Moreover, according to Table I, $r_3 = 0$. Hence, the model is reduced to the following:

$$\dot{x} = \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} V cos(x_3) - (r_1 x_4) sin(x_3) \\ V sin(x_3) + (r_1 x_4) cos(x_3) \\ x_4 \\ -a x_4 - b x_4^3 + c u_r \end{bmatrix}. \tag{35}$$

Without loss of generality, we assume that the ship moves from the origin heading toward a target in the first orthant. The initial heading angle is $x_3 = \pi/4$ and the ship initially is heading toward the target, moving toward the middle of the obstacle. The ship heading angle $x_3$ and heading velocity $x_4$ are initially known with uncertainty of $\delta x_3$ and $\delta x_4$, respectively. The position of the ship is initially known with an uncertainty of $\delta x$. Specifically, $h(z_1, z_2, z_3, z_4) = \{(x_1, x_2, x_3, x_4) \mid x_1 \in [z_1 - \delta x, z_1 + \delta x],\ x_2 \in [z_2 - \delta x, z_2 + \delta x],\ x_3 \in [z_3 - \delta x_3, z_3 + \delta x_3],$ and $x_4 = [z_4 - \delta x_4, z_4 + \delta x_4]\}$, where $[z_1, z_2, z_3, z_4] \in \mathcal{M}$ is the measurement and $\delta x = 0.5$ m, $\delta x_3 = 3.6$ deg and $\delta x_4 = 0.05$ rad/sec. The bad set is $\mathbf{B} = \{\alpha b_m + (1 - \alpha) b_M \mid \alpha \in\ [0, 1]\}$.

### A. *Order preserving property of the ship*

In this section, we first approximate the dynamics (35), by treating $x_4$ in the first two equations of (35) as a disturbance. Then we show that this approximate model is input/output order preserving according to Definition 1.

Considering equation (35), we have that $\dot{x}_4 = -a x_4 - b x_4^3 + c u_r$. Let $x_4^m$ be such that $-a x_4^m - b x_4^{m3} + c u_r^m = 0$. Considering the saturation constraint (34), for $x_4 > x_4^m$ we have that $\dot{x}_4 = -a x_4 - b x_4^3 + c u_r < -a x_4^m - b x_4^{m3} + c u_r^m = 0$. Similarly, for $x_4 < -x_4^m$, we have that $\dot{x}_4 > 0$. Therefore, for all $u_r(\cdot)$, the set $S_1 := \{x \mid |x_4| \leq x_4^m\}$ is an attracting invariant set and for the dynamics (35), we have $|x_4| \leq x_4^m$, where $x_4^m = 0.49$ rad/sec. Since $|x_4| \leq x_4^m$, we consider $x_4$ in the first two equations of (35) as a disturbance input $d$ that is bounded, i.e., $|d| \leq x_4^m$. System

(35) then modifies to the system given by

$$\dot{x} = \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} V cos(x_3) - (r_1 d) sin(x_3) \\ V sin(x_3) + (r_1 d) cos(x_3) \\ x_4 \\ -a x_4 - b x_4^3 + c u_r \end{bmatrix}. \tag{36}$$

Transforming the system output to radial coordinates $(r, \theta)$ given by $r = \sqrt{(x_1^2 + x_2^2)}$ and $\theta = \arctan\left(\frac{x_2}{x_1}\right)$. The dynamics of system (36) in the new coordinates is given by

$$\begin{aligned} \dot{r} &= V\cos(x_3 - \theta) - (r_1 d)\sin(x_3 - \theta), \\ \dot{\theta} &= (V\sin(x_3 - \theta) - (r_1 d)\cos(x_3 - \theta))\frac{1}{r}, \\ \dot{x}_3 &= x_4, \qquad \dot{x}_4 = -a x_4 - b x_4^3 + c u_r. \end{aligned} \tag{37}$$

In these new coordinates, $\Sigma = (X, \mathcal{D}, \mathcal{U}, \mathcal{Y}, f, g)$ where $X = \mathbb{R}_+ \times [-\pi, \pi] \times \mathbb{R}^2$, $\mathcal{U} = \{u_r \in \mathbb{R} \mid |u_r| \leq u_r^m = 0.61\}$, $\mathcal{D} = \{d \in \mathbb{R} \mid |d| \leq x_4^m = 0.49\}$, $\mathcal{Y} = \mathbb{R}_+ \times [-\pi, \pi]$, $f$ is the vector field in (37), $y = (r, \theta)$. We are only interested in the truncated trajectories where $\frac{d}{dt}r > 0$. Because, since the bad set **B** is connected, it is not possible for the trajectories to intersect **B**, while $\frac{d}{dt}r < 0$, with both extremal control inputs (rudder angles) $u_m$ and $u_M$. In other words, if the ship is returning to the origin, it has already avoided collision with the bad set. Confining the trajectories to $\frac{d}{dt}r > 0$, we can show that system (37) is input/output order preserving according to Definition 1 by directly using the algebraic checks of [38].

It is possible to show that also Assumption 3(iii) with $a_m = a_M$ is satisfied, that is, that output trajectories are enveloped by those obtained with maximal and minimal disturbances $d_M = -0.49$ and $d_m = 0.49$. To see this, note that dynamics (36) imply that the velocity vector in the $(x_1, x_2)$ plane is given by $\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = v_V(t) + v_d(t)$, in which $v_V(t) = \begin{bmatrix} V cos(x_3) \\ V sin(x_3) \end{bmatrix}$ and $v_d(t) = \begin{bmatrix} -(r_1 d) sin(x_3) \\ (r_1 d) cos(x_3) \end{bmatrix}$. Since $v_d(t)$ is perpendicular to $v_V(t)$ $(v_d(t)^T v_V(t) = 0)$ and $\|v_d(t)\| = d(t)$, the extremal disturbances generate perpendicular disturbance velocity vectors that result in extremal trajectories that envelop all possible output trajectories. Therefore, for a fixed $x_3$ signal, all trajectories are enveloped by those generated by $d_M$ and $d_m$.

The control strategy is implemented as detailed in the first three algorithms of Section V. To do so, we "inflated" the set **B** by the uncertainty on the output variables and considered a single value for the output $y$ as given by the center of the set of possible outputs. This removed the need for the flow of the system to preserve the ordering with respect to initial conditions.

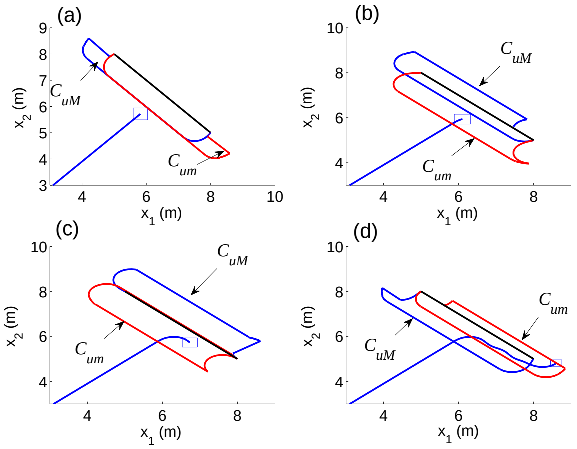


Fig. 3: Ship trajectory and sets $C_{\mathbf{u}_M}$ and $C_{\mathbf{u}_m}$ in the position space corresponding to different heading angles and yaw velocities. The bad set **B** is the black part line. Four different time instants are depicted: (a) shows the time instant where $\hat{x}(t) \cap \partial C_{\mathbf{u}_m} \neq \emptyset$, $\hat{x}(t) \cap \partial C_{\mathbf{u}_M} \neq \emptyset$, $\hat{x}(t) \cap C_{\mathbf{u}_M} = \emptyset$, and $\hat{x}(t) \cap C_{\mathbf{u}_m} = \emptyset$. According to control law (18), either $\mathbf{u}_M$ or $\mathbf{u}_m$ can be applied. We applied $\mathbf{u}_M$. Subplots (b) and (c) show $\hat{x}(t)$ when $\hat{x}(t) \cap \partial C_{\mathbf{u}_M} = \emptyset$, $\hat{x}(t) \cap C_{\mathbf{u}_M} = \emptyset$, and $\hat{x}(t) \cap C_{\mathbf{u}_m} \neq \emptyset$, so that $\mathbf{u}_M$ must be applied. Subplot (d) shows when the set $\hat{x}(t)$ passes the obstacle.

Figure 3 shows the trajectory of the ship and the position uncertainty as it approaches the bad set, slides on the border of the sets $C_{\mathbf{u}_M}$ and $C_{\mathbf{u}_m}$, and adopts the control signal $\mathbf{u}_M$ until the ship passes the bad set. As it can be seen in Figure 3(c), the state estimate $\hat{x}(t)$ passes fairly close to the bad set, indicating that the approximation of $x_4$ as a bounded disturbance did not introduce substantial conservatism.

## VII. Application Example II: Helicopter Navigation among Obstacles

In this section, we consider the safety control problem for a system that can be described by the parallel composition of input/output order preserving systems. Specifically, we consider an helicopter navigating among buildings in a city and seek to design a supervisor that enforces safe control actions to prevent collisions with buildings.

We consider the helicopter model introduced in [48], which is full state linearizable with respect to velocity and heading angle. The helicopter is modeled as a rigid body subject to external forces and torques originating from the propellers. Let $f^b$ and $\tau^b$ be force and torque with respect to body coordinate frame. Let $\Theta := [\phi\ \theta\ \psi]$, in which Euler angles $\phi$, $\theta$, and $\psi$ are rotation angles about the $X$, $Y$ and $Z$ axis, respectively. Let $R(\Theta) \in SO(3)$ denote the rotation matrix of the body axes relative to the spatial axes $X - Y - Z$. Therefore, $R(\Theta) = e^{\hat{Z}\psi} e^{\hat{Y}\theta} e^{\hat{X}\phi}$ where $\hat{X},\ \hat{Y},\ \hat{Z} \in so(3)$

are skew-symmetric matrices representing rotations $\phi$, $\theta$ and $\psi$ about $X$, $Y$, and $Z$, respectively. Let $P$ and $V^p$ denote the position and velocity, respectively, of the center of mass with respect to a fixed coordinate frame. Let $\omega^b$ denote the body angular velocity in body coordinate frame. According to Euler-Newton equations, the equations of motion are given by

$$\frac{d}{dt}\begin{bmatrix} P \\ V^p \\ \Theta \\ \omega^b \end{bmatrix} = \begin{bmatrix} V^p \\ \frac{1}{m}R(\Theta)f^b \\ \Psi(\Theta)\omega^b \\ I^{-1}(\tau^b - \omega^b \times I\omega^b) \end{bmatrix},$$

where $I$ is the inertial matrix and $\Psi(\Theta) = \begin{bmatrix} 1 & \tan(\theta)\sin(\phi) & \tan(\theta)\cos(\phi) \\ 0 & \cos(\phi) & -\sin(\phi) \\ 0 & \frac{\sin(\phi)}{\cos(\theta)} & \frac{\cos(\phi)}{\cos(\theta)} \end{bmatrix}$. The force and torque in body-fixed coordinates are given by $f^b = \begin{bmatrix} X_M \\ Y_M + Y_T \\ Z_M \end{bmatrix} + R(\Theta)^T \begin{bmatrix} 0 \\ 0 \\ mg \end{bmatrix}$ and $\tau^b = \begin{bmatrix} R_M \\ M_M + M_T \\ N_M \end{bmatrix} + \begin{bmatrix} Y_M h_M + Z_M y_M + Y_T h_T \\ -X_M h_M + Z_M l_M \\ -Y_M l_M - Y_T l_T \end{bmatrix}$, where $X_M$, $Y_M$, and $Z_M$ are forces, $R_M$, $M_M$, and $N_M$ are torques generated by the main rotor and $Y_T$ and $Q_T$ are force and torque generated by the tail rotor, respectively. The forces and torques generated by the main rotor are controlled by $T_M$, $a_{ls}$, and $b_{ls}$, in which $T_M$ is the force generated by the main rotor and $a_{ls}$, and $b_{ls}$ , are the longitudinal and lateral tilt of the tip path plane of the main rotor with respect to the shaft, respectively, while $\{l_M, y_M, h_M, h_T, l_T\}$ are constants. The tail rotor is considered as a source of pure lateral force $Y_T$ and anti-torque $Q_T$, which are controlled by $T_T$. We also have $X_M = -T_M \sin(a_{ls})$, $\quad R_M \simeq \frac{\partial R_M}{\partial b_{ls}} b_{ls} - Q_M \sin(a_{ls})$, $Y_M = T_M \sin(b_{ls})$, $\quad M_M \simeq \frac{\partial M_M}{\partial a_{ls}} a_{ls} + Q_M \sin(b_{ls})$, $Z_M = -T_M \cos(a_{ls})\cos(b_{ls})$, $N_M \simeq -Q_M \cos(a_{ls})\cos(b_{ls})$, and $Y_T = -T_T$. In these equations, $Q_M \simeq C_M^Q T_M^{1.5} + D_M^Q$ and $Q_T \simeq C_T^Q T_T^{1.5} + D_T^Q$, and $\frac{\partial R_M}{\partial b_{ls}}$, $\frac{\partial M_M}{\partial a_{ls}}$, $C_M^Q$, $C_T^Q$, $D_M^Q$ and $D_T^Q$ are constants. For the inputs, we have $|a_{ls}| \leq 0.4363$, $|b_{ls}| \leq 0.3491$, $-20.86 \leq T_M \leq 69.48$, and $-5.26 \leq T_T \leq 5.26$. All other constants are provided in [48]. Figure 4 shows the helicopter body-fixed coordinate frame. As shown in [48], by choosing $[P_1, P_2, P_3, \psi] \in \mathbb{R}^4$ as the output

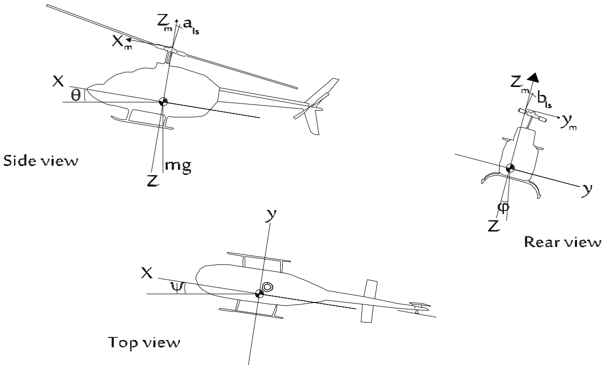


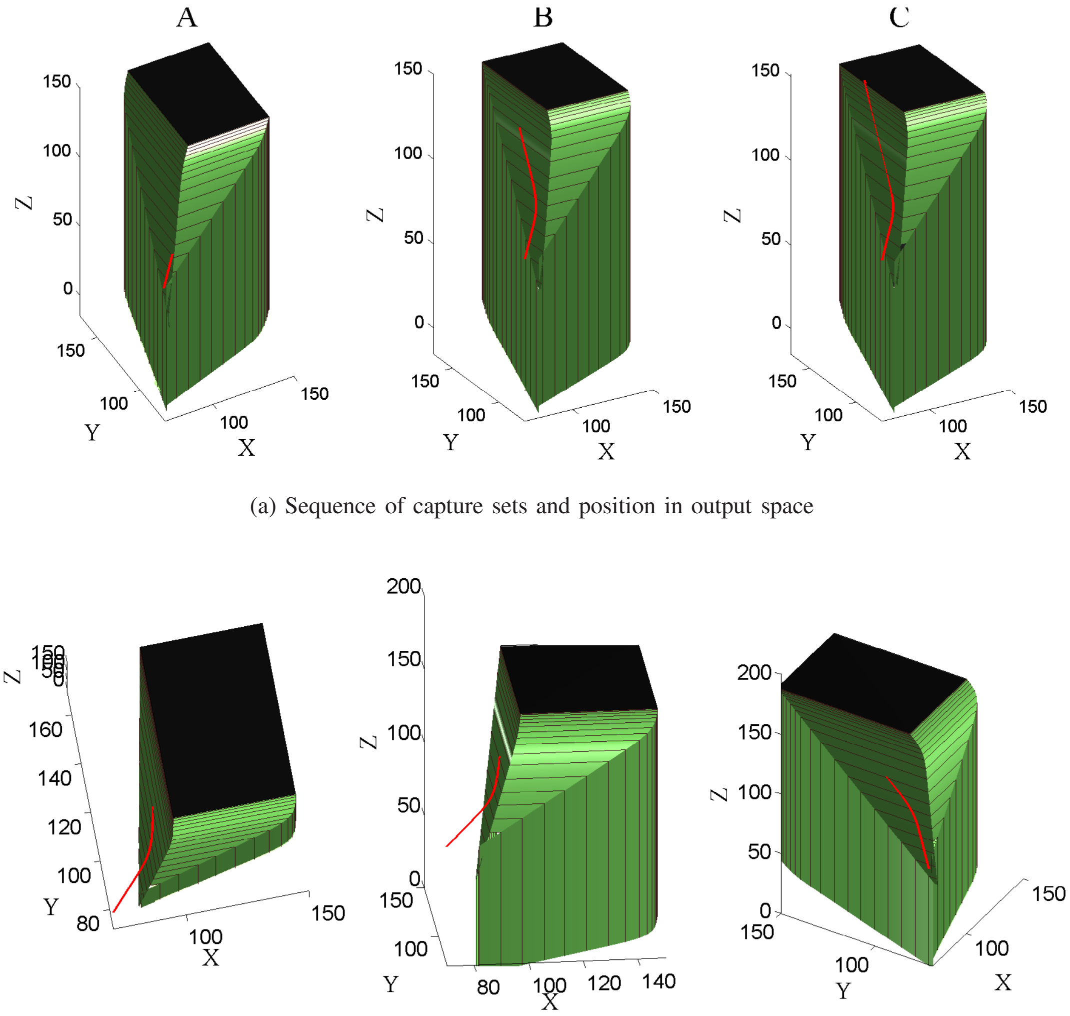
Fig. 4: The body-fixed coordinate frame of the helicopter.

and applying the decoupling algorithm [49], the system takes the form

$$\begin{bmatrix} P_1^{(5)} \\ P_2^{(4)} \\ P_3^{(4)} \\ \cdots \\ \psi^{(3)} \end{bmatrix} = \underbrace{\begin{bmatrix} b^v \\ \\ \\ \cdots \\ b^\psi \end{bmatrix}}_{b} + \underbrace{\begin{bmatrix} A^v \\ \\ \\ \cdots \\ A^\psi \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} \frac{d^2}{dt^3} T_M \\ \frac{d}{dt} T_T \\ \frac{d}{dt} a_{ls} \\ \frac{d}{dt} b_{ls} \end{bmatrix}}_{v},$$

where $b^v \in \mathbb{R}^3$, $A^v \in \mathbb{R}^{3\times 4}$, $b^\psi \in \mathbb{R}$ and $A^\psi :\in \mathbb{R}^{1\times 4}$ are functions of the states $[V^p, \Theta, \omega^b]$. Let $[\nu_1 \ \nu_2 \ \nu_3 \ \nu_\psi]^T = \nu := b + Av$. Since $A$ is invertible for all values of the states $[V^p, \Theta, \omega^b]$ ([48]), if the control inputs $T_M$, $T_T$, $a_{ls}$ and $b_{ls}$ are such that $v = A^{-1}(\nu - b)$, then with respect to the new control input $\nu$ we have four decoupled systems $P_1^{(5)} = \nu_1$, $P_2^{(5)} = \nu_2$, $P_3^{(5)} = \nu_3$, $\psi_\psi^{(3)} = \nu_\psi$.

By setting $\nu_\psi = -a_2\psi^{(2)} - a_1\psi^{(1)} - a_0\psi$, $\psi$ is tracked to $\psi = 0$ so that we can use $\nu_1$, $\nu_2$, $\nu_3$ to control the position. We design closed-loop systems $\Sigma^i : P_i^{(5)} = {V^p}_i^{(4)} = a_0(u^i - {V^p}_i) + a_3{V^p}_i^{(3)} - a_2{V^p}_i^{(2)} - a_1{V^p}_i^{(1)}$, $i = 1, 2, 3$, where the coefficients $a_i$ are chosen such that the polynomial $s^4 + a_3 s^3 + a_2 s^2 + a_1 s + a_0$ has roots with strictly negative real parts, chosen, in particular, equal to $[-1.4, -1.5, -5, -5]$, $u^i$ is the input and $x^i = [P_i, {V^p}_i, {V^p}_i^{(1)}, {V^p}_i^{(2)}, {V^p}_i^{(3)}]$ is the state of subsystem $\Sigma^i$. Hence, we have $\Sigma^i = (X^i, \mathcal{D}^i, \mathcal{U}^i, \mathcal{Y}^i, f^i, g^i)$, $i = 1, 2, 3$, in which $X^i = \mathbb{R}^5$, $\mathcal{D}^i = \emptyset$, $\mathcal{U}^i = \{u^i \in \mathbb{R} \mid u_m^i \leq u^i \leq u_M^i\}$ for some $u_m^i$ and $u_M^i$, $\mathcal{Y}^i = P_i$, $f^i : X^i \times \mathcal{U}^i \to X^i$, with $f^i(x) = [x_2^i,\ x_3^i,\ x_4^i,\ x_5^i,\ a_0 u^i - a_3 x_5^i - a_2 x_4^i - a_1 x_3^i - a_0 x_2^i]$, and the output map is given by $g^i(x^i) = x_1^i$. Systems $\Sigma^i$, $i = 1, 2, 3$ are input/output order preserving. Figure 5(a) shows the trajectory of the helicopter avoiding a building while under the control strategy (28). Note that

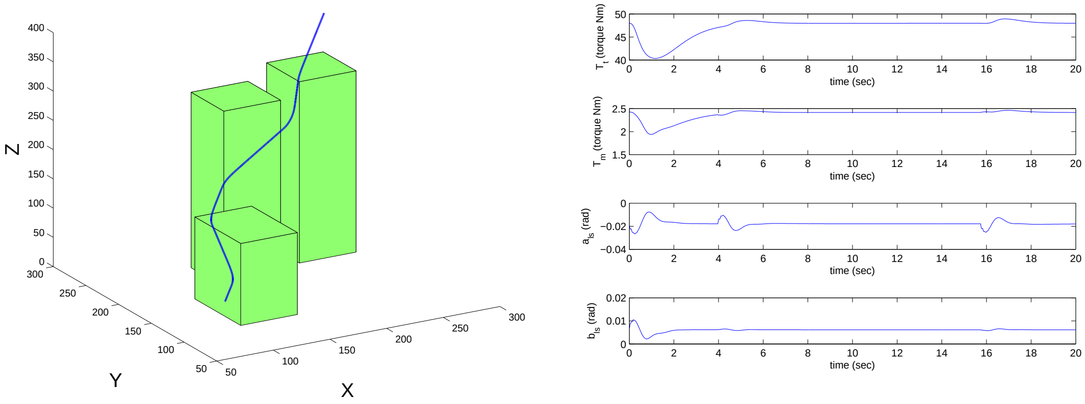


(a) Sequence of capture sets and position in output space

(b) Capture set in output space from different views

Fig. 5: (a) Capture set in position space corresponding to the current values of the velocity and its derivatives at three different time instants. In each subplot, the trajectory up to the current time is depicted in red. (a)-A shows the time instant in which the trajectory hits the boundary of the capture set, (a)-B shows a time at which the vehicle is controlled by the supervisory control and slides along the border of the capture set, (a)-C shows the trajectory that slides on the border of the capture set until it passes the building. (b) shows the capture set in (a)-B viewed from different angles.

the capture set is 15 dimensional. The figures show the capture set of the building in output space corresponding to the current value of the speed and its derivatives. Figure 5(b) shows the capture set in output space at one specific time from different views. Figure 6(a) shows the helicopter maneuvering among three buildings, each of which is modeled as the product of three intervals. Therefore, we have three rectangle bad sets in the output space of system $\Sigma$. Specifically, we have building1: $[100\ 150] \times [100\ 170] \times [10\ 150]$, building2: $[140\ 190] \times [195\ 245] \times [0\ 300]$,



(a) (b)

Fig. 6: Trajectory of the helicopter maneuvering among three buildings (a) and control signals (b).

and building3: $[217\ 267] \times [213\ 263] \times [0\ 310]$. The helicopter navigates toward its final target while avoiding the buildings. For each of these buildings we have a capture set (not shown), which the control strategy (28) avoids. Note that to guarantee that the helicopter can avoid all of the buildings, the speeds should be kept at sufficiently low values so that the capture sets of the buildings in the position space do not intersect with each other. Figure 6 (b) shows the control efforts. The three bumps in the control signals correspond to safe control being enforced so to avoid entering into the capture set of the first, second, and third building. In all cases, the control effort does not exceed the prescribed bounds.

For simplicity of illustration, perfect state information was assumed in this example since feedback linearization was used on the original model. In the presence of imperfect state information, the calculation of $v$ from $\nu$ will be subject to bounded error. This bounded error can be treated as a bounded disturbance and directly accounted for in the design of the control $\nu$ as we have detailed in the paper. This, however, is beyond the scope of the current example.

## VIII. Conclusion

In this paper, we have considered control under safety specifications for systems with imperfect state information, in which the flow preserves some ordering between the input and the output. Under these order preserving properties, we provided an explicit characterization of the open loop maximal control invariant set (MCIS), or equivalently, of the capture set given a set of bad states to be avoided. Accordingly, we provided an explicit construction of a control strategy that keeps the system state within the MCIS (outside of the capture set) at all times. The algorithms for both determining whether a set of system states belongs to the MCIS and for evaluating the control strategy have a complexity that is at most quadratic with the dimension of the state space. Systems whose flow preserves an ordering between the input and the output are found in a number of application domains from biology to engineering. In this paper, we have illustrated the implementation of the proposed algorithms in two applications, one involving a ship maneuver to avoid an obstacle and the other involving an helicopter navigating in a city while avoiding buildings. In both cases, the system models and parameters were taken from domain-specific literature.

Future work includes extending the techniques proposed in this paper to apply to general systems that are not necessarily input/output order preserving, but that can be approximated by input/output order preserving systems. Also, the problem of making the proposed algorithms robust to input delays and communication delays needs to be addressed. Promising results have been obtained in these directions in the context of vehicle collision avoidance at traffic intersections [44], but a rigorous theoretical framework has yet to be developed. Similarly, we seek to extend our results to when the bad set is not fixed but evolves dynamically as this could be used in a number of applications in transportation systems. This case can be treated by assuming a dynamic model for how the bad set moves and by taking the system into bad set-fixed coordinates.

## IX. Appendix

A cone $\Delta \subset \mathbb{R}^n$ is a set that is closed under multiplication by positive scalars and $0 \in \Delta$. A set $\mathcal{U}$ is partially ordered with respect to "$\leq_\Delta$" if for all $u_1,\ u_2 \in \mathcal{U}$, $u_1 \leq_\Delta u_2$ provided $u_2 - u_1 \in \Delta$. Let $X$ be an ordered Banach space with respect to a cone and let $\|\cdot\|$ be the norm in Banach space $X$. Given Banach space $X$, $x_0 \in X$, and $\epsilon > 0$, $B_\epsilon(x_0) := \{x \in X \mid \|x - x_0\| < \epsilon\}$. Given a Banach space $\mathbb{B}_u$ and $\mathcal{U} \subset \mathbb{B}_u$, $\mathcal{C}(\mathcal{U})$ denotes the set of all piece-wise continuous functions $R : \mathbb{R}_+ \to \mathcal{U}$. For $S \subseteq X$, we let $\inf(S)$ ($\sup(S)$) denote the infimum (supremum) of $S$ with respect to the partial order of $X$. Given a Banach space $\mathbb{B}_u$ and $\mathcal{U} \subset \mathbb{B}_u$, $S(\mathcal{U})$ denotes the set of all measurable functions $R : \mathbb{R}_+ \to \mathcal{U}$. Once $\mathcal{U}$ is partially ordered, $S(\mathcal{U})$ and $\mathcal{C}(\mathcal{U})$ are partially ordered such that for $a, b \in S(\mathcal{U})$ ($a, b \in \mathcal{C}(\mathcal{U})$), $a \geq b$ if and only if $a(t) \geq b(t)$ for all $t \in \mathbb{R}_+$. We equip the sets $\mathcal{C}(\mathcal{U})$ and $S(\mathcal{U})$ with the norm $\|f\|_\infty = \sup_{t \in \mathbb{R}_+} \|f(t)\|$. If $v \in \mathbb{R}^n$, then $v_i$ denotes the i'th element of the vector $v$. For any set $A \subset \mathbb{R}^n$ and $a \in \mathbb{R}$, $A_{\leq(\geq)a} := \{x \in A \mid x_1 \leq (\geq) a\}$. For $x \in \mathbb{R}^n$ and $A \subset \mathbb{R}^n$, $d(x, A) := \inf_{y \in A} \|x - y\|$ denotes the distance of $x$ from $A$. A family of non-empty compact subsets of $\mathbb{R}^n$ is denoted by $Com(\mathbb{R}^n)$. For $X \subset \mathbb{R}^n$, $Cl(X)$ denotes the closure of $X$. For any set $X$, we denote the power set of $X$ by $2^X$ and it is the set of all subsets of $X$. Given two sets $A, B \subset \mathbb{R}^n$, $A \oplus B := \{a + b \mid a \in A \text{ and } b \in B\}$ is the Minkowski sum of the two sets. A mapping $f : \mathbb{R}^n \to Com(\mathbb{R}^n)$ is said upper-hemicontinuous at $x_0 \in \mathbb{R}^n$ if for all $\epsilon > 0$, there exists $\delta > 0$ such that for all $x \in B_\delta(x_0)$ we have that $f(x) \subset f(x_0) \oplus B_\epsilon(0)$. A mapping $f : \mathbb{R}^n \to Com(\mathbb{R}^n)$ is lower-hemicontinuous at $x_0 \in \mathbb{R}^n$ if for all $\epsilon > 0$, there exists $\delta > 0$ such that for all $x \in B_\delta(x_0)$ we have that $f(x_0) \subset f(x) \oplus B_\epsilon(0)$. A mapping is said lower-hemicontinuous (upper-hemicontinuous) if it is lower-hemicontinuous (upper-hemicontinuous) at all points in $\mathbb{R}^n$ [6].

**Lemma 1:** Let $C$ be an open set such that $\hat{x}(t_1, S, \mathbf{u}, \mathbf{z}) \cap C \neq \emptyset$ and $S \cap C = \emptyset$ for some compact set $S \subset X$ and $t_1 \in \mathbb{R}_+$. Then, $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C = \emptyset$, where

$$\bar{t} := \sup\{t \in [0, t_1] \mid \hat{x}(t, S, \mathbf{u}, \mathbf{z}) \cap C = \emptyset\}. \tag{38}$$

*Proof:* We proceed by contradiction argument and assume that $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C \neq \emptyset$. Therefore, there exists $x_0 \in S$ and $\mathbf{d} \in \mathcal{C}(\mathcal{D})$ such that $\phi(\bar{t}, x_0, \mathbf{d}, \mathbf{u}) \in C$. Since $h(\cdot)$ is the measurement map, and for all $\tau \in [0,\ \bar{t}]$, $\phi(\tau, x_0, \mathbf{d}, \mathbf{u}) \in h(\mathbf{z}(\tau))$. From (1), $\phi(\tau, x_0, \mathbf{d}, \mathbf{u}) \in \hat{x}(\tau, S, \mathbf{u}, \mathbf{z})$ for all $\tau \in [0,\ \bar{t}]$. Since $C$ is open and $\phi(\bar{t}, x_0, \mathbf{d}, \mathbf{u}) \in C$, there exists $\epsilon > 0$ such that $B_\epsilon(\phi(\bar{t}, x_0, \mathbf{d}, \mathbf{u})) \subset C$. By continuity of the flow with respect to time, there exists $\delta > 0$ such that for all $\tau \in (\bar{t} - \delta, \bar{t}]$, $\phi(\tau, x_0, \mathbf{d}, \mathbf{u}) \in B_\epsilon(\phi(\bar{t}, x_0, \mathbf{d}, \mathbf{u})) \subset C$. Hence, $\tau \in (\bar{t} - \delta, \bar{t}] \;\Rightarrow\; \hat{x}(\tau, S, \mathbf{u}, \mathbf{z}) \cap C \neq \emptyset$. This contradicts equation (38). Therefore, we must have that $\hat{x}(\bar{t}, S, \mathbf{u}, \mathbf{z}) \cap C = \emptyset$. ■

**Proof of Theorem 6** The output trajectory $y$ partitions the $\mathbb{R}^2$ space into three sets. The trajectory, the set of all points above the trajectory, and the set of all points below it, defined in the following $\gamma^o(x, \mathbf{d}, \mathbf{u}) := \{y(t, x, \mathbf{d}, \mathbf{u}) \mid t \in \mathbb{R}_+\}\gamma^+(x, \mathbf{d}, \mathbf{u}) := \{(y_1(t, x, \mathbf{d}, \mathbf{u}), p) \mid t \in \mathbb{R}_+ \text{ and } p > y_2(t, x, \mathbf{d}, \mathbf{u})\}$, and $\gamma^-(x, \mathbf{d}, \mathbf{u}) := \{(y_1(t, x, \mathbf{d}, \mathbf{u}), p) \mid t \in \mathbb{R}_+ \text{ and } p > y_2(t, x, \mathbf{d}, \mathbf{u})\}$. We know that $\mathbf{B} \succeq y(\mathbb{R}_+, a_M, \mathbf{d}_M, \mathbf{u})$ if and only if $\mathbf{B}_{\geq g_1(a_M)} \subset Cl(\gamma^+(a_M, \mathbf{d}_M, \mathbf{u}))$ and $\mathbf{B} \preceq y(\mathbb{R}_+, a_m, \mathbf{d}_m, \mathbf{u})$ if and only if $\mathbf{B}_{\geq g_1(a_m)} \subset Cl(\gamma^-(a_m, \mathbf{d}_m, \mathbf{u}))$.

A. ($\Leftarrow$) We prove that if $\mathbf{B} \subset Cl(\gamma^+(a_M, \mathbf{d}_M, \mathbf{u}))$ or $\mathbf{B} \subset Cl(\gamma^-(a_m, \mathbf{d}_m, \mathbf{u}))$ then $S \cap C_{\mathbf{u}} = \emptyset$. Assume

$$\mathbf{B} \subset Cl(\gamma^+(a_M, \mathbf{d}_M, \mathbf{u})). \tag{39}$$

According to Assumption 3, for all $a \in S$, and $\mathbf{d} \in \mathcal{C}(\mathcal{D})$, $y(t, a, \mathbf{d}, \mathbf{u}) \in \gamma^-(a_M, \mathbf{d}_M, \mathbf{u})$ for all $t \in \mathbb{R}_+$, $a \in S$, and $\mathbf{d} \in \mathcal{C}(\mathcal{D})$. Therefore, it follows that

$$y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \subset Cl(\gamma^-(a_M, \mathbf{d}_M, \mathbf{u})). \tag{40}$$

Since $\mathbf{B}$ is open, from (39), we have $\mathbf{B} \subset \gamma^+(a_M, \mathbf{d}_M, \mathbf{u})$. Therefore, considering (40), and the fact that $\gamma^+(a_M, \mathbf{d}_M, \mathbf{u}) \cap Cl(\gamma^-(a_M, \mathbf{d}_M, \mathbf{u})) = \emptyset$, we have $\mathbf{B} \cap y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) = \emptyset$. Namely, $S \cap C_{\mathbf{u}} = \emptyset$. With a similar argument, if $\mathbf{B}_{\geq g1(a_m)} \subset Cl(\gamma^-(a_m, \mathbf{d}_m, \mathbf{u})$, then $\mathbf{B} \cap Cl(\gamma^+(a_M, \mathbf{d}_M, \mathbf{u})) = \emptyset$ and therefore $S \cap C_{\mathbf{u}} = \emptyset$.

B.($\Rightarrow$) We prove that if $S \cap C_{\mathbf{u}} = \emptyset$, then $\mathbf{B} \subset Cl(\gamma^+(a_M, \mathbf{d}_M, \mathbf{u}))$ or $\mathbf{B} \subset Cl(\gamma^-(a_m, \mathbf{d}_m, \mathbf{u}))$. Proceeding by contradiction argument, assume there exists $b^1, b^2 \in \mathbf{B}$ such that

$$b^1 \in \gamma^+(a_m, \mathbf{d}_m, \mathbf{u}),\ \ b^2 \in \gamma^-(a_M, \mathbf{d}_M \mathbf{u}). \tag{41}$$

By Assumption 3, we have that $\gamma^o(a_m, \mathbf{d}_m, \mathbf{u}) \subset \gamma^-(a_M, \mathbf{d}_M, \mathbf{u})$. Hence, the trajectories $\gamma^o(a_M, \mathbf{d}_M, \mathbf{u})$ and $\gamma^o(a_m, \mathbf{d}_m, \mathbf{u})$ divide $\mathbb{R}^2_{\geq g1(a_m)}$ into the sets: $S_1 := \gamma^-(a_M, \mathbf{d}_M, \mathbf{u}) \cap \gamma^+(a_m, \mathbf{d}_m, \mathbf{u})$, $S_2 := (\gamma^+(a_M, \mathbf{d}_M, \mathbf{u}) \cup \gamma(a_M, \mathbf{d}_M, \mathbf{u}))_{\geq g1(a_m)}$, and $\bar{S}_2 := (\gamma^-(a_m, \mathbf{d}_m, \mathbf{u}) \cup \gamma(a_m, \mathbf{d}_m, \mathbf{u}))$. Set $S_1$ is the set of all points between the trajectories $\gamma(a_M, \mathbf{d}_M, \mathbf{u})$ and $\gamma(a_m, \mathbf{d}_m, \mathbf{u})$, $S_2$ is the set of all points on and above the trajectory $\gamma^o(a_M, \mathbf{d}_M, \mathbf{u})$, and $\bar{S}_2$ is the set of all points on and below the trajectory $\gamma^o(a_m, \mathbf{d}_m, \mathbf{u})$.

In the sequel, we show that for all points $s \in S_1$, there exists an initial state $a \in S$ and a disturbance $\mathbf{d} \in \mathcal{C}(\mathcal{D})$ such that $s \in \gamma^o(a, \mathbf{d}, \mathbf{u})$. Moreover, all trajectories are confined inside $S_1$. Hence, we show in the sequel that if $b^1 \notin Cl(\gamma^-(a_m, \mathbf{d}_m, \mathbf{u}))$ and $b^1 \in \gamma^-(a_M, \mathbf{d}_M, \mathbf{u})$, then $\mathbf{B} \cap S_1 \neq \emptyset$ from which we conclude that $S \cap C_{\mathbf{u}} \neq \emptyset$. Since $\gamma(a_M, \mathbf{d}_M, \mathbf{u}) \subset \gamma^+(a_m, \mathbf{d}_m, \mathbf{u})$, we have that $S_2 \subset \gamma^+(a_m, \mathbf{d}_m, \mathbf{u})$, so that $\gamma^+(a_m, \mathbf{d}_m, \mathbf{u}) = (\gamma^+(a_m, \mathbf{d}_m, \mathbf{u}) \cap \gamma^-(a_M, \mathbf{d}_M, \mathbf{u}))^{S_1} \cup (\gamma^+(a_m, \mathbf{d}_m, \mathbf{u}) \cap \sim \gamma^-(a_M, \mathbf{d}_M, \mathbf{u}))^{S_2} = S_1 \cup S_2$.

With the same argument we have that $\gamma^-(a_M, \mathbf{d}_M \mathbf{u})_{\geq g1(a_m)} = S_1 \cup Cl(S_2)$. From equation (41), we may face two cases: $b^1 \in S_1$ or $b^1 \in S_2$.

Assume $b^1 \in S_1$ and let $W$ be defined as in the proof of Theorem 1. Then, $W(a_m, \mathbf{d}_m; b^1_1, \mathbf{u}) < b^1_2 < W(a_M, \mathbf{d}_M; b^1_1, \mathbf{u})$. Since $W$ is continuous and $\mathcal{C}(\mathcal{D})$, $S$ and $\mathcal{C}(\mathcal{D})$ are connected, there exists $\mathbf{d} \in \mathcal{C}(\mathcal{D})$ and $a \in S$, such that $W(a, \mathbf{d}; b^1_1, \mathbf{u}) = b^1_2$. That is, $b^1 \in y(\mathbb{R}_+, a, \mathbf{d}, \mathbf{u}) \subset y(\mathbb{R}_+, S, \mathbf{d}, \mathbf{u})$ and consequently $\mathbf{B} \cap y(\mathbb{R}_+, S, \mathcal{C}(\mathcal{D}), \mathbf{u}) \neq \emptyset$. Hence, $S \cap C_{\mathbf{u}} \neq \emptyset$.

If $b^1 \in S_2$ then, since $\mathbf{B}$ is open, $\mathbf{B} \cap \gamma^+(a_M, \mathbf{d}_M, \mathbf{u}) \neq \emptyset$. Also, according to (41), $\mathbf{B} \cap \gamma^-(a_M, \mathbf{d}_M, \mathbf{u}) \neq \emptyset$. Since $\mathbf{B}$ is connected, the union of the two open sets $\gamma^+(a_M, \mathbf{d}_M, \mathbf{u})$ and $\gamma^-(a_M, \mathbf{d}_M, \mathbf{u})$ does not covers $\mathbf{B}$. Hence, $\mathbf{B} \cap y(\mathbb{R}_+, a_M, \mathbf{d}_M, \mathbf{u}) \neq \emptyset$. Hence, $\mathbf{B} \cap C_{\mathbf{u}} \neq \emptyset$ which is a contradiction.

■

# References

[1] H. S. Witsenhausen, “A minmax control problem for sampled linear systems,” *IEEE Transactions on Automatic on Automatic Control*, 13(1):5:21, 1968.

[2] D. P. Bertsekas and I. B. Rhodes, “On the minmax reachability of target sets and target tubes,” *Automatica*, 7(2):233-247, 1971.

[3] J. D. Glover and F. C. Schweppe, “Control of linear dynamic systems with set constrained disturbances,” *IEEE Transactions on Automatic on Automatic Control*, 16(5):411-423, 1971.

[4] D. P. Bertsekas, “Infinite-time Reachability of state-space regions by using feedback control,” *IEEE Transactions on Automatic on Automatic Control*, 17(5):604-613, 1972.

[5] F. Blanchini, “Set invariance in control”, *Automatica*, 35(11):1747-1767, 1999.

[6] J. Aubin, “Viability Theory”, Birkhäuser, 1991.

[7] C. Tomlin, G. J. Pappas, and S. Sastry, “Conflict resolution for air traffic management: A study in multiagent hybrid systems”, *IEEE Trans. on Automatic Control*, 43(4):509-521, 1998.

[8] J. Lygeros, C. J. Tomlin, and S. Sastry. “Controllers for reachability specifications for hybrid systems”, *Automatica*, 35(3):349-370, 1999.

[9] C. Tomlin, J. Lygeros, S. Sastry, “Synthesizing controllers for nonlinear hybrid systems”, In Hybrid systems: Computation and control, Lecture Notes in Computer Science, 1386, pp. 360-373, Springer, 1998.

[10] C. J. Tomlin, J. Lygeros, and S. Sastry, “A game theoretic approach to controller design for hybrid systems”, *Proceedings of the IEEE*, 88(7):949-970, 2000.

[11] I. Mitchell and C. J. Tomlin, “Level Set Methods for Computation in Hybrid Systems”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 1790, pp. 310-323, Springer, 2000.

[12] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, “Computational techniques for the verification of hybrid systems”, *Proceedings of the IEEE*, 91(7):986-1001, 2003.

[13] A. Chutinam and B. Krogh, “Verification of polyhedral-invariant hybrid automata using polygonal pipe approximations”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 1569, pp. 76-90, Springer, 1999.

[14] S. Rakovic, E. C. Kerrigan, D. Q. Mayne, and J. Lygeros, “Reachability analysis of discrete-time systems with disturbances”, *IEEE transactions on Automatic Control*, 51(4):546-561, 2006.

[15] M. Althoff, C. Le Guernic and B. H. Krogh, “Reachable Set Computation for Uncertain Time-Varying Linear Systems,” In Hybrid Systems: Computation and Control, pp. 93-102, 2011.

[16] C. Le Guernic, “Reachability Analysis of Hybrid Systems with Linear Continuous Dynamics”, Univerité Joseph Fourier, 2009.

[17] A. Kurzhanski, P. Varaiya, “Ellipsoidal techniques for reachability analysis”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 1790, pp. 203-213, Springer, 2000.

[18] A. Girard, “Reachability of uncertain linear systems using zonotopes”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 3414, Springer, pp. 291-305, 2005.

[19] A. Girard, C. Le Guernic, O. Maler, “Efficient computation of reachable sets of linear time-invariant systems with inputs”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 3927, Springer, pp. 257-271, 2006.

[20] G. Laferriere, G. J. Pappas, and S. Yovine, “A new class of decidable hybrid systems”, In Hybrid Systems : Computation and Control, Lecture Notes in Computer Science, 1569. pp. 137-151. Springer, 1999.

[21] G. Laferriere, G. J. Pappas, and S. Yovine, “Symbolic reachability computation for families of linear vector fields”, *J. Symb. Comput.*, 32(3):231-253, 2001.

[22] R. Ghosh and C. Tomlin, “Symbolic reachable set computation of piecewise affine hybrid automata and its application to biological modeling: Delta-notch protein signalling,” *IET Syst. Biol.*, 1(1):170-183, 2004.

[23] A. Tiwari, “Termination of Linear Programs”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 3114, pp. 70-82, Springer, 2004.

[24] H. Anai and V. Weispfenning, “Reach set computation using real quantifier elimination”, In Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, 2034, pp. 63-76, Springer, 2001.

[25] A. Dolzmann and T. Sturm, “REDLOG: Computer algebra meets computer logic”, Universitä Passau, Fakultät Für Mathematik und Informatik, Passau, Germany, Tech. Rep. MIP-9603, 1996.

[26] G. Collins and H. Hong, “Partial cylindrical algebraic decomposition for quantifier elimination”, *J. Symb. Comput., 12:299-328*, 1991.

[27] E. Frazzoli, M. A. Dahleh, and E. Feron, “Real-Time Motion Planning for Agile Autonomous Vehicles”, *AIAA Journal of Guidance, Control, and Dynamics*, 25:116-129, 2002.

[28] E. Frazzoli, M. A. Dahleh, and E. Feron, “Maneuver-Based Motion Planning for Nonlinear Systems with Symmetries” *IEEE Trans. on Robotics*, 21(6):1077-1091, 2005.

[29] Z. Sun, Y. Liu, and X. Xie, “Global Stabilization for a Class of High-Order Time-Delay Nonlinear Systems”, *International Journal of Innovative Computing, Information and Control*, 7(12):7119-7130, 2011.

[30] L. Yao and H-K. Wen, “Design of Observer Based Adaptive PID Controller for Nonlinear Systems”, *International Journal of Innovative Computing, Information and Control*, 9(2):667-677, 2013.

[31] R. B. Messaoud, N. Zanzouri, and M. Ksouri, “Local Feedback Unknown Input Observer for Nonlinear Systems”, *International Journal of Innovative Computing, Information and Control*, 8(2):1145-1154, 2012.

[32] L. Zhang, P. Shi, and M. Liu, “Stability and Stabilization of Switched Linear Systems With Mode-Dependent Average Dwell Time”, *IEEE Trans. on Aut. Control*, 57(7):1809-1815, 2012.

[33] R. Verma and D. Del Vecchio, “Safety Control of Hidden Mode Hybrid Systems”, *IEEE Trans. on Aut. Control*, 57(1):62 - 77, 2012.

[34] R. Verma and D. Del Vecchio, “Semiautonomous Multivehicle Safety”, *Robotics & Automation Magazine*, 18 (3), 44-54, 2011.

[35] D. Del Vecchio, “Observer-based control of block triangular discrete time hybrid automata on a partial order”, *International Journal of Robust and Nonlinear Control*, 19(14):1581-1602, 2009.

[36] D. Del Vecchio, M. Malisoff, and R. Verma, “A separation principle for a class of hybrid automata on a partial order”, *Proc. of American Control Conference*, 2009.

[37] M. R. Hafner and D. Del Vecchio, “Computational Tools for the Safety Control of a Class of Piecewise Continuous Systems with Imperfect Information on a Partial Order ”, *SIAM J. on Control and Optimization*, 9(6):2463-2493, 2011.

[38] D. Angeli and E. D. Sontag, “Monotone Control Systems”, *IEEE Trans. on Automatic Control*, 48(10):1684-1698, 2003.

[39] R. Ghaemi and D. Del Vecchio, “Safety control of piece-wise continuous order preserving systems ”, *Proc. IEEE Conference on Decision and Control*, 2011.

[40] D. Bertsekas, “Dynamic Programming and Suboptimal Control: A Survey from ADP to MPC”, *European Journal of Control*, 11:310-334, 2005.

[41] D. Angeli and E.D. Sontag, “Interconnections of monotone systems with steady-state characteristics”, Optimal control, stabilization and non-smooth analysis. Lecture Notes in Control and Information Science, Springer, 301:135-154, 2004.

[42] D. Angeli and E.D. Sontag, “Oscillations in I/O monotone systems”, *IEEE Trans. on Circuits and Systems*, 55:166-176, 2008.

[43] R. Raffard, S. Waslander, A. Bayen, and C. Tomlin, “A cooperative distributed approach to multi-agent Eulerian network control: Application to air traffic management”, *AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2005.

[44] M. Hafner, D. Cunningham, L. Caminiti, and D. Del Vecchio, “Cooperative Collision Avoidance at Intersections: Algorithms and Experiments”, *IEEE Trans. on Intelligent Transportation Systems*, 14(3):1162-1175, 2013.

[45] B. A. Davey and H. A. Priesteley. “Introduction to lattices and order”, Cambridge: Cambridge University Press, 2002.

[46] S. Lavalle. “Planning Algorithms”, Cambridge University Press, 2006.

[47] M. H. Casado, A. Fernandez, and J. Iglesias, “Optimization of the course in the ships movement by input-output linearization”, *Proc. of IFAC Conference on Control Application and Marine Systems*, 2001.

[48] T. J. Koo and S. Sastry, “Output tracking control design of a helicopter model based on approximate linearization”, *Proc. of IEEE Conference on Decision and Control*, 1998.

[49] J. Descusse and C. Moog, “Dynamic decoupling for right invertible nonlinear systems”, *Systems and Control Letters*, 8:345-9, 1987.

**Reza Ghaemi** received the B.S. and M.S. degrees from the University of Tehran, Iran, and the Ph. D. degree in Electrical Engineering from the University of Michigan, Ann Arbor in 1998, 2001, and 2009, respectively. From 2001 to 2004, he conducted research on control and monitoring of power electronic systems at the Power Research Institute, Tehran, Iran. During 2010-2012 he was a post-doctoral researcher at MIT. He is now Lead Engineer at General Electrics. His research interests include optimal control theory and model predictive control.

**Domitilla Del Vecchio** received the Ph. D. degree in Control and Dynamical Systems from the California Institute of Technology, Pasadena, and the Laurea degree in Electrical Engineering from the University of Rome at Tor Vergata in 2005 and 1999, respectively. From 2006 to 2010, she was an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Michigan, Ann Arbor. In 2010, she joined the Department of Mechanical Engineering at the Massachusetts Institute of Technology (MIT), where she is currently an Associate Professor. Her research interests include analysis and control of nonlinear and hybrid dynamical systems with application to biomolecular networks and transportation networks.

D. Del Vecchio is a recipient of the Donald P. Eckman Award from the American Automatic Control Council (2010), the NSF Career Award (2007), the American Control Conference Best Student Paper Award (2004), and the Bank of Italy Fellowship (2000).