Joint 48th IEEE Conference on Decision and Control and
28th Chinese Control Conference
Shanghai, P.R. China, December 16-18, 2009

Computation of Safety Control for Uncertain Piecewise Continuous Systems on a Partial Order

Michael R. Hafner and Domitilla Del Vecchio

Abstract— **In this paper, the safety control problem for a class of hybrid systems with disturbance inputs and imperfect continuous state information is considered. Under the assumption that the system has order preserving dynamics, we provide an algorithmic procedure for computing the control map, which has linear complexity in the number of continuous variables. The structure of the control map with imperfect state information is the same as the one with perfect state information, implying separation between state estimation and control. We illustrate the proposed algorithm on a class of applications characterized by order preserving dynamics.**

I. Introduction

In this paper, we consider the safety control problem for hybrid systems affected by disturbance inputs and imperfect continuous state information. There is a wealth of literature on safety control for hybrid automata assuming perfect state information [8, 10, 13, 15–17]. This control problem is addressed by computing the set of states that lead to an unsafe configuration independently of an input choice, called here the *capture set*. Then, a static feedback is computed that guarantees that the state never enters the capture set. As it appears in these previous works, the algorithms do not scale with the size of the system and are limited to state spaces with small dimension. Furthermore, the proposed algorithms are not guaranteed to terminate [15]. To reduce the computational load, approximate algorithms have been proposed to compute over-approximations of the capture set [9, 17].

These works are only concerned with state feedback, that is, the state of the system is assumed to be available to the controller. In the literature of hybrid systems, dynamic feedback is scarcely addressed. Some works on this problem have recently appeared [5–7, 20]. In particular, [20] proposes a solution to the control problem for rectangular hybrid automata that admit a finite-state abstraction. Dynamic feedback in a special class of hybrid systems with imperfect discrete state information is presented in [5], however safety invariance is not considered. Dynamic control of block triangular order preserving hybrid automata under imperfect continuous state information is considered in [6] for discrete time systems. In [7], these results are extended to continuous time hybrid systems on a partial order and a formal separation principle is stated. However, these results are not applicable when the hybrid system is affected by disturbance inputs.

The authors would like to thank Edwin Romeijn, Peter Scott and Berit Stensones for their helpful suggestions. Del Vecchio and Hafner are with the Systems Laboratory, University of Michigan, Ann Arbor. E-mail: mikehaf@umich.edu

In this paper, we extend the results of [7] to hybrid systems with disturbance inputs. In particular, we exploit the order preserving structure of the system dynamics to show that the capture set (with perfect or imperfect state information) can be determined from two sets. These two sets can in turn be computed with linear complexity algorithms. The dynamic or static control map is then directly constructed from these two sets. The resulting structure of the dynamic control map is the same as the structure of the static control map, in which the state is replaced by its estimate. This implies separation between state estimation and control design for the class of order preserving hybrid systems considered. We apply the developed control algorithm on a collision avoidance problem between two vehicles at a traffic intersection.

This paper is organized as follows. In Section II, we introduce basic definitions and the class of hybrid systems we consider. In Section III, we provide a mathematical statement of the safety control problem. In Section IV, we give the main result of the paper, namely the dynamic feedback control map and separation principle. In Section V, we present a discrete time algorithm for computing the dynamic feedback. In Section VI, we present an example application involving the safety control of two vehicles at an intersection.

II. Preliminaries

A. Notation and Basic Definitions

For the element $x \in \mathbb{R}^n$ and set $A \subset \mathbb{R}^n$, denote the distance from x to A $d(x, A) := \inf_{y \in A} \|x - y\|$. For $A, B \in \mathbb{R}^n$, let $d(A, B) := \inf_{y \in A} d(y, B)$. For the set $A \subset \mathbb{R}^n$, let $B(A, \epsilon) := \{z \in \mathbb{R}^n \mid d(z, A) < \epsilon\}$. Denote the canonical projection $\tau_i : \mathbb{R}^n \to \mathbb{R}$ defined by $\tau_i(x) = x_i$, which naturally extends to sets. Denote the unit sphere $\mathbb{S}^n$ and unit disk $\mathbb{D}^n$, where $\mathbb{S}^n := \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$ and $\mathbb{D}^n := \{x \in \mathbb{R}^{n+1} \mid \|x\| \leq 1\}$. For sets $A, B \subseteq \mathbb{R}^n$ we define the relation $A \lesssim B$ if $\tau_1(A) \cap \tau_1(B)$ is non-empty and for all $x \in A$ and $y \in B$ such that $x_1 = y_1$, we have $x_2 < y_2$.

We denote the space of piecewise continuous functions from $\mathbb{R}_+$ to $A \subset \mathbb{R}$ as $S(A)$. We use the notation $F : A \rightrightarrows B$ to denote a set-valued map from A into B. Denote the unit interval $I := [0, 1]$. We define the Cone at vertex $x \in \mathbb{R}^n$ with respect to $a_1, a_2, \ldots, a_k \in \mathbb{R}^n$ as $\text{Cone}_{\{a_1, a_2, \ldots, a_k\}} x := \{y \in \mathbb{R}^n \mid \langle y - x | a_i \rangle \geq 0 \ \forall \ i \in \{1, 2, \ldots, k\}\}$. For $x \in \mathbb{R}^2$, we use the shorthand notation $\text{Cone}_+(x) := \text{Cone}_{\{\hat{e}_1, \hat{e}_2\}}(x) \subset \mathbb{R}^2$ and $\text{Cone}_-(x) := \text{Cone}_{\{-\hat{e}_1, -\hat{e}_2\}}(x) \subset \mathbb{R}^2$.

Definition 1: A path $\gamma \in C^0(I, \mathbb{R}^2)$ is said to be *order preserving connected* (o.p.c.) if it is simple [14], and for all $x \in \mathbb{R}^2$ $\text{Cone}_+(x) \cap \gamma(I) \neq \emptyset$ implies that $\text{Cone}_+(x) \cap \gamma(I)$ is path connected. A set $D \subseteq \mathbb{R}^2$ is said o.p.c. if for all $x, y \in D$,

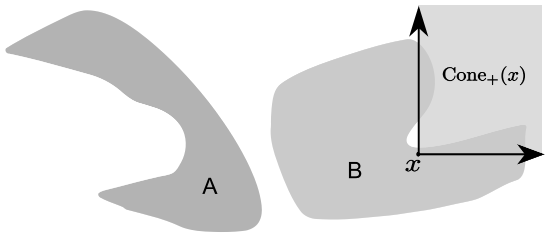


Fig. 1. A is an o.p.c. set while B is not an o.p.c. set.

there exists a $\gamma \in C^0(I, D)$ such that $\gamma(0) = x, \gamma(1) = y$ and γ is o.p.c. (Figure 1).

A partial order is a set P with a relation "$\leq$", which we denote by the pair (P,$\leq$) [4]. Define the partial order $(\mathbb{R}^n, \leq)$ for $w, z \in \mathbb{R}^n$ as $w \leq z$ if and only if $w_i \leq z_i$ for all $i \in \{1, 2, \ldots, n\}$. For $U \subseteq \mathbb{R}$, we define the partial order $(S(U), \leq)$ for $\mathbf{w}, \mathbf{z} \in S(U)$ as $\mathbf{w} \leq \mathbf{z}$ provided $\mathbf{w}(t) \leq \mathbf{z}(t)$ for all $t \in \mathbb{R}_+$. Suppose (P,$\leq_P$) and (Q,$\leq_Q$) are two partially ordered sets. A map $f : P \to Q$ is an order preserving map provided $x \leq_P y$ implies $f(x) \leq_Q f(y)$.

B. Class of Systems Considered

We consider piecewise continuous systems, with imperfect state information. This includes the set of hybrid systems with no continuous state reset and no discrete state dynamics.

Definition 2: A *piecewise continuous system* Σ with imperfect state information is a collection $\Sigma = (X, \mathcal{U}, O, f, h)$, in which (i) $X \subseteq \mathbb{R}^n$ is a set of continuous variables; (ii) U is a set of continuous inputs; (iii) O is a continuous set of outputs; (iv) $f : X \times U \to X$ is a piecewise continuous vector field; (v) $h : O \rightrightarrows X$ is an output map.

For an output measurement $z \in O$, the function $h(z)$ returns the set of all states compatible with the current output. We let $\phi(t, x, \mathbf{u})$ denote the flow of Σ at time $t \in \mathbb{R}_+$, with initial condition $x \in X$ and input $\mathbf{u} \in S(U)$. Denote the i^{th} component of the flow by $\phi_i(t, x, \mathbf{u})$. We assume uniform continuity of the flow with respect to time.

We restrict our class of systems $\Sigma = (X, U, O, f, h)$ to order preserving systems. These systems are defined on the partial orders $(\mathbb{R}^n, \leq)$ and $(S(U), \leq)$. Order preserving systems are a subclass of Monotone Control systems, see [1].

Definition 3: We say that Σ is *order preserving* provided there exist constants $u_L, u_H \in \mathbb{R}$ and a constant $\xi > 0$ such that (i) $U = [u_L, u_H] \subset \mathbb{R}$; (ii) The flow $\phi(t, x, \mathbf{u})$ is order preserving with respect to input and initial condition; (iii) $f_1(x, u) \geq \xi$ for all $(x, u) \in X \times U$; (iv) For all $z \in O, h(z) = [\inf h(z), \sup h(z)] \subseteq \mathbb{R}^n$.

Definition 4: For $\Sigma^1 = (X^1, U^1, O^1, f^1, h^1)$ and $\Sigma^2 = (X^2, U^2, O^2, f^2, h^2)$, we define the *parallel composition* $\Sigma = \Sigma^1 \| \Sigma^2 := (X, \mathcal{U}, O, f, h)$, in which $X := X^1 \times X^2$, $U := U^1 \times U^2$, $O := O^1 \times O^2$, $f := (f^1, f^2)$ and $h := (h^1, h^2)$.

For $x = (x^1, x^2) \in X^1 \times X^2$ and $\mathbf{u} = (\mathbf{u}^1, \mathbf{u}^2) \in S(U^1) \times S(U^2)$, we denote the flow of the parallel composition $\Sigma^1 \| \Sigma^2$ as $\phi(t, x, (\mathbf{u}^1, \mathbf{u}^2)) = (\phi^1(t, x, (\mathbf{u}^1, \mathbf{u}^2)), \phi^2(t, x, (\mathbf{u}^1, \mathbf{u}^2)))$ in which $\phi^1(t, x, (\mathbf{u}^1, \mathbf{u}^2)) \in X^1$ and $\phi^2(t, x, (\mathbf{u}^1, \mathbf{u}^2)) \in X^2$. When referring to a component of $\phi(t, x, (\mathbf{u}^1, \mathbf{u}^2))$, we denote $\phi_j^{1,2}(t, x, (\mathbf{u}^1, \mathbf{u}^2)) := (\phi_j^1(t, x, (\mathbf{u}^1, \mathbf{u}^2)), \phi_j^2(t, x, (\mathbf{u}^1, \mathbf{u}^2)))$.

III. Problem formulation

Given the parallel composition $\Sigma = (X, U, O, f, h)$ of two systems (referred to as agents) Σ^1, Σ^2, and a bad set of states $\mathbf{B} \subseteq X$, consider the problem of designing a controller that, based on perfect state measurements, prevents the continuous flow from entering $\mathbf{B}$.

We assume that system Σ^1 can be controlled, that is $\mathbf{u}^1 \in S(U^1)$ can be chosen, while system Σ^2 cannot be controlled, namely, $\mathbf{u}^2 \in S(U^2)$ is a disturbance. In the sequel, we denote $\boldsymbol{\delta} := \mathbf{u}^2$ and $\Delta := U^2$ so that $\boldsymbol{\delta} \in S(\Delta)$. With abuse of notation, denote $\mathbf{u} := \mathbf{u}^1$ and $U := U^1$ so that $\mathbf{u} \in S(U)$. We thus denote the flow of Σ by $\phi(t, x, (\mathbf{u}, \boldsymbol{\delta}))$ with $x \in X$ and $(\mathbf{u}, \boldsymbol{\delta}) \in S(U) \times S(\Delta)$.

First, consider the problem of keeping the flow outside $\mathbf{B}$ using static feedback, that is, we assume perfect state information.

Problem 1: (Static Feedback Safety Control Problem) Given a system $\Sigma^1 \| \Sigma^2$ with $O = X$ and $h = id$, determine

$$W := \left\{ \begin{array}{c} x \in X \mid \exists\ \mathbf{u} \in S(U) \text{ s.t. } \forall\ \boldsymbol{\delta} \in S(\Delta), \\ \text{we have } \phi^(t, x, (\mathbf{u}, \boldsymbol{\delta})) \notin \mathbf{B}\ \forall\ t \in \mathbb{R}_+ \end{array} \right\},$$

and a set-valued map $g : X \rightrightarrows U$ such that for initial conditions $x \in W$, we have $\phi(t, x, (\mathbf{u}, \boldsymbol{\delta})) \notin \mathbf{B}$ for all $\boldsymbol{\delta} \in S(\Delta)$ and $t \in \mathbb{R}_+$ when we choose $\mathbf{u}(\tau) \in g(\phi(\tau, x, (\mathbf{u}, \boldsymbol{\delta})))$, for all $\tau \in \mathbb{R}_+$.

This problem can be interpreted as one of determining a winning strategy for the controlled agent Σ^1, while ensuring that any input chosen by agent Σ^2 does not lead the state into $\mathbf{B}$.

The second problem considered is the dynamic feedback problem. We now assume imperfect information about the state. Let $\hat{x}(t, \hat{x}_0, \mathbf{u}, \mathbf{z})$ denote the set of all possible states at time t given a set of initial conditions $\hat{x}_0 \subset X$ and measurable signals $\mathbf{u}$ and $\mathbf{z}$. More formally,

$$\hat{x}(t, \hat{x}_0, \mathbf{u}, \mathbf{z}) := \{x \in X \mid \exists\ x_0 \in \hat{x}_0 \text{ and } \boldsymbol{\delta} \in S(\Delta) \text{ s.t.}$$
$$\phi(t, x_0, (\mathbf{u}, \boldsymbol{\delta})) = x \text{ and } \ \phi(\tau, x_0, (\mathbf{u}, \boldsymbol{\delta})) \in h(\mathbf{z}(\tau))\ \forall\ \tau \in [0, t]\}.$$

The set $\hat{x}(t, \hat{x}_0, \mathbf{u}, \mathbf{z})$ is called the non-deterministic information state [11] and we will denote it by $\hat{x}(t)$ when $\hat{x}_0$, $\mathbf{u}$ and $\mathbf{z}$ are clear.

Problem 2: (Dynamic Feedback Safety Control Problem) Given a system $\Sigma^1 \| \Sigma^2$, determine

$$\bar{W} := \left\{ \begin{array}{c} A \subset X \mid \exists\ \mathbf{u} \in S(U) \text{ s.t. } \forall\ \mathbf{z} \in S(O) \\ \text{we have } \hat{x}(t, A, \mathbf{u}, \mathbf{z}) \cap \mathbf{B} = \emptyset\ \forall\ t \in \mathbb{R}_+ \end{array} \right\},$$

and a set-valued feedback map $G : 2^X \rightrightarrows U$ such that for initial convex sets $A \subset \bar{W}$, we have $\hat{x}(t, A, \mathbf{u}, \mathbf{z}) \cap \mathbf{B} = \emptyset$ for all $t \in \mathbb{R}_+$ and $\mathbf{z} \in S(O)$ when we choose $\mathbf{u}(\tau) \in G(\hat{x}(\tau, A, \mathbf{u}, , \mathbf{z}))$, for all $\tau \in \mathbb{R}_+$.

IV. Problem Solution

Let $B \subset \mathbb{R}^2$ be a bounded open o.p.c. set and define

$$\mathbf{B} := \{x \in \mathbb{R}^{2n} \mid (x_1^1, x_1^2) \in B\}. \tag{1}$$

This choice is motivated by systems in which x_1^1 and x_1^2 represent displacement and B represents a set of collision configurations. For systems evolving on partial orders, o.p.c. sets provide a natural geometry for capturing the flow.

Rather than directly computing W, we compute the *capture set*, defined as $C := X \backslash W$. Mathematically, it is defined as

$$C = \left\{ \begin{array}{c} x \in X \mid \forall\ \mathbf{u} \in S(U), \exists\ \boldsymbol{\delta} \in S(\Delta), \\ \text{s.t. } \phi(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \cap \mathbf{B} \neq \emptyset \end{array} \right\}.$$

In this paper, we develop a novel way of computing the capture set through the computation of simpler sets. For a given input $\bar{\mathbf{u}} \in S(U)$, we define the *restricted capture set* to be the capture set when the input signal is restricted to $\bar{\mathbf{u}}$. Mathematically, this is expressed as

$$C_{\bar{\mathbf{u}}} = \{x \in X \mid \exists\ \boldsymbol{\delta} \in S(\Delta) \text{ s.t. } \phi(\mathbb{R}_+, x, (\bar{\mathbf{u}}, \boldsymbol{\delta})) \cap \mathbf{B} \neq \emptyset\}.$$

Since Σ^1 and Σ^2 are order preserving, we have that $U = [u_L, u_H]$ and $\Delta = [\delta_L, \delta_H]$. We define the signals $\mathbf{u}_L(t) := u_L$, $\mathbf{u}_H(t) := u_H$, $\boldsymbol{\delta}_L(t) := \delta_L$ and $\boldsymbol{\delta}_H(t) := \delta_H$, which each hold for all $t \in \mathbb{R}_+$. We state the first main result of this paper, a necessary and sufficient condition on convex sets A leading to non-empty intersection of the flow $\phi(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}))$ with $\mathbf{B}$ for every control input $\mathbf{u}$.

Theorem 1: Consider $\Sigma^1 \| \Sigma^2$ and a convex set $A \subset X$. Then $A \cap C_{\mathbf{u}_L} \neq \emptyset$ and $A \cap C_{\mathbf{u}_H} \neq \emptyset$ holds if and only if for all $\mathbf{u} \in S(U)$, there exists $\boldsymbol{\delta} \in S(\Delta)$ such that $\phi(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta})) \cap \mathbf{B} \neq \emptyset$.

Before giving the proof, we introduce the following intermediate result, whose proof can be found in the appendix. We assume continuity of the flow with respect to initial conditions.

Lemma 1: Consider $\Sigma^1 \| \Sigma^2$ and a convex set $A \subset X, \mathbf{u} \in S(U)$ *and* $\gamma \in C^0(I, \mathbb{R}^2)$ o.p.c. with $\inf \tau_1(A) < \max \tau_1(\gamma(I))$. Then $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, S(\Delta))) \cap \gamma(I) = \emptyset$ if and only if $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_L)) \gtrsim \gamma(I)$ or $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_H)) \lesssim \gamma(I)$.

Lemma 1 states that the flow ϕ generated from initial conditions A and input $\mathbf{u}$ can avoid an o.p.c. path γ in the (x_1^1, x_1^2) subspace if and only if the disturbance $\boldsymbol{\delta}_L$ takes the trajectory of $\phi_1^{1,2}$ above γ or the disturbance $\boldsymbol{\delta}_H$ takes the trajectory of $\phi_1^{1,2}$ below γ.

Proof: (Theorem 1). ($\Leftarrow$) Follows by choosing the constant input $\mathbf{u}_L$ or $\mathbf{u}_H$.

($\Rightarrow$ Construction) Consider an arbitrary $\mathbf{u} \in S(U)$. Since $A \cap C_{\mathbf{u}_L} \neq \emptyset$ and $A \cap C_{\mathbf{u}_H} \neq \emptyset$, the definition of the restricted capture set implies that there are $x, y \in A, \boldsymbol{\delta}_1, \boldsymbol{\delta}_2 \in S(\Delta)$ and $t_1, t_2 \in \mathbb{R}_+$ such that $\phi(t_1, x, (\mathbf{u}_L, \boldsymbol{\delta}_1)) \in \mathbf{B}$ and $\phi(t_2, y, (\mathbf{u}_H, \boldsymbol{\delta}_2)) \in \mathbf{B}$. Let $\mu, \nu \in B$ where $\mu = \phi_1^{1,2}(t_1, x, (\mathbf{u}_L, \boldsymbol{\delta}_1))$ and $\nu = \phi_1^{1,2}(t_2, y, (\mathbf{u}_H, \boldsymbol{\delta}_2))$. From equation (1), we have that $\mu, \nu \in B$. Since B is an o.p.c. set, there exists an o.p.c. path $\gamma \in C^0(I, B)$ with $\gamma(0) = \mu$ and $\gamma(1) = \nu$.

Condition (ii) of Definition 3 and the decoupling of the dynamics imply $\phi_1^1(t_1, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \geq \mu_1$ and $\phi_1^2(t_1, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \leq \mu_2$. Condition (iii) of Definition 3 and the uniform continuity of the flow with respect to time imply there must be a time $\bar{t} \in [0, t_1]$ such that $\phi_1^1(\bar{t}, x, (\mathbf{u}, \boldsymbol{\delta}_L)) = \mu_1$. At this time $\bar{t}$, condition (ii) of Definition 3 and the decoupling of the dynamics imply $\phi_1^2(\bar{t}, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \leq \phi_1^2(t_1, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \leq \mu_2$. Since $\mu \in \gamma(I)$, we thus have that

$$\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_L)) \not\gtrsim \gamma(I). \tag{2}$$

Similarly, condition (ii) of Definition 3 and the decoupling of the dynamics imply $\phi_1^1(t_2, y, (\mathbf{u}, \boldsymbol{\delta}_H)) \leq \nu_1$ and $\phi_1^2(t_2, y, (\mathbf{u}, \boldsymbol{\delta}_H)) \geq \nu_2$. Condition (iii) of Definition 3 and the uniform continuity of the flow with respect to time imply there must be a time $\bar{t} \geq t_2$ such that $\phi_1^1(\bar{t}, y, (\mathbf{u}, \boldsymbol{\delta}_H)) = \nu_1$. At this time $\bar{t}$, condition (ii) of Definition 3 and the decoupling of the dynamics imply $\phi_1^2(\bar{t}, y, (\mathbf{u}, \boldsymbol{\delta}_H)) \geq \phi_1^2(t_2, y, (\mathbf{u}, \boldsymbol{\delta}_H)) \geq \nu_2$. Since $\nu \in \gamma(I)$, we thus have that

$$\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_H)) \not\lesssim \gamma(I). \tag{3}$$

Note that $\phi_1^1(0, x, (\mathbf{u}, \boldsymbol{\delta})) < \mu_1$ from condition (iii) of Definition 3, implying $\inf \tau_1(A) < \max \tau_1(\gamma(I))$. Therefore, (2) and (3) allow us to invoke Lemma 1, giving $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, S(\Delta))) \cap \gamma(I) \neq \emptyset$. This implies there is $z \in A$ and $\bar{\boldsymbol{\delta}} \in S(\Delta)$ such that $\phi_1^{1,2}(\mathbb{R}_+, z, (\mathbf{u}, \bar{\boldsymbol{\delta}})) \cap B \neq \emptyset$, which leads to $\phi(\mathbb{R}_+, z, (\mathbf{u}, \bar{\boldsymbol{\delta}})) \cap \mathbf{B} \neq \emptyset$. Since this holds for arbitrary $\mathbf{u} \in S(U)$, we have completed the proof. ■

Corollary 1: $C = C_{\mathbf{u}_L} \cap C_{\mathbf{u}_H}$.

Proof: Follows by applying Theorem 1 to $A = \{x\}$. ■

For the above Corollary, it can be shown that it is not necessary to require continuity of the flow with respect to the initial condition.

A. The control map

Define the set-valued map $G : 2^X \rightrightarrows U$ as

$$G(Z) := \begin{cases} u_L & \text{if } Z \cap C_{\mathbf{u}_H} \neq \emptyset \text{ and } Z \cap \partial C_{\mathbf{u}_L} \neq \emptyset \\ & \quad \text{and } Z \cap C_{\mathbf{u}_L} = \emptyset \\ u_H & \text{if } Z \cap C_{\mathbf{u}_L} \neq \emptyset \text{ and } Z \cap \partial C_{\mathbf{u}_H} \neq \emptyset \\ & \quad \text{and } Z \cap C_{\mathbf{u}_H} = \emptyset \\ \{u_H, u_L\} & \text{if } Z \cap \partial C_{\mathbf{u}_H} \neq \emptyset, Z \cap \partial C_{\mathbf{u}_L} \neq \emptyset \\ & \quad \text{and } Z \cap (C_{\mathbf{u}_L} \cup C_{\mathbf{u}_H}) = \emptyset \\ U & \quad \text{otherwise.} \end{cases} \tag{4}$$

We define the closed-loop flow generated with the set-valued map G starting from $A \subset X$ as follows.

Definition 5: For $A \subset X$ compact, let $\Phi_A(t, \mathbf{u}) := \{\phi(t, x, (\mathbf{u}, \boldsymbol{\delta})) \mid x \in A \text{ and } \boldsymbol{\delta} \in S(\Delta)\}$. The closed-loop flow generated by G starting in A is the set-valued map $\Phi_A^{cl} : \mathbb{R}_+ \rightrightarrows X$ defined as $\Phi_A^{cl}(t) := \{\Phi_A(t, \mathbf{u}) \mid \mathbf{u}(\tau) \in G(\Phi_A(\tau, \mathbf{u}))\ \forall \tau \in \mathbb{R}_+\}$.

We next show that the feedback map (4) guarantees that the closed-loop flow $\Phi_A^{cl}(t)$ never intersects $\mathbf{B}$ whenever $A \cap C_{\mathbf{u}_L} = \emptyset$ or $A \cap C_{\mathbf{u}_H} = \emptyset$.

Theorem 2: Let $A \subset X$ be compact and convex. If $A \cap C_{\mathbf{u}_L} = \emptyset$ or $A \cap C_{\mathbf{u}_H} = \emptyset$ holds, then $\Phi_A^{cl}(t) \cap \mathbf{B} = \emptyset$ for all $t \in \mathbb{R}_+$.

Proof: Observe that if $\Phi_A^{cl}(t) \cap C_{\mathbf{u}} = \emptyset$ for some $\mathbf{u} \in S(U)$, then necessarily $\Phi_A^{cl}(t) \cap \mathbf{B} = \emptyset$. This follows from the fact that $\mathbf{B} \subset C_{\mathbf{u}}$ for all $\mathbf{u} \in S(U)$. Thus, we show that if the hypothesis is satisfied, necessarily $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_L} = \emptyset$ or $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_H} = \emptyset$ for all $t \in \mathbb{R}_+$.

We proceed by contradiction. Suppose there exists a $t_2 > 0$ such that $\Phi_A(t_2)_{cl} \cap C_{\mathbf{u}_L} \neq \emptyset$ and $\Phi_A^{cl}(t_2) \cap C_{\mathbf{u}_H} \neq \emptyset$. The continuity of the flow with respect to initial conditions and time implies that $\Phi_A^{cl}(t)$ is both upper and lower hemi-continuous, and thus continuous [2]. This, along with $\Phi_A^{cl}(0) \cap C_{\mathbf{u}_H} = \emptyset$ or

$\Phi_A^{cl}(0) \cap C_{\mathbf{u}_L} = \emptyset$, implies there exists an interval $[t_1, t_2] \subset \mathbb{R}_+$ such that one of the following cases occur:

Case(I): $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_H} \neq \emptyset$ for all $t \in [t_1, t_2]$, while $\Phi_A^{cl}(t_1) \cap C_{\mathbf{u}_L} = \emptyset$ and $\Phi_A^{cl}(t_2) \cap C_{\mathbf{u}_L} \neq \emptyset$;

Case(II): $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_L} \neq \emptyset$ for all $t \in [t_1, t_2]$, while $\Phi_A^{cl}(t_1) \cap C_{\mathbf{u}_H} = \emptyset$ and $\Phi_A^{cl}(t_2) \cap C_{\mathbf{u}_H} \neq \emptyset$;

Case(III): $\Phi_A^{cl}(t_1) \cap C_{\mathbf{u}_H} = \emptyset$ and $\Phi_A^{cl}(t_2) \cap C_{\mathbf{u}_L} = \emptyset$ while $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_H} \neq \emptyset$ and $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_L} \neq \emptyset$ for all $t \in (t_1, t_2]$.

Case(I). If the flow is continuous with respect to initial conditions, we can use Theorem 1.4.16 (Maximum Theorem) from [2] to show that $dist(t) := \sup_{x \in \Phi_A^{cl}(t)} d(x, \sim C_{\mathbf{u}_L})$ is a continuous function. Since $\Phi_A^{cl}(t)$ and $\sim C_{\mathbf{u}_L}$ are closed for all t, $dist(t) = 0$ if and only if $\Phi_A^{cl}(t) \subset (\sim C_{\mathbf{u}_L})$, implying $dist(t_2) > 0$ and $dist(t_1) = 0$.

This along with the continuity of $dist(t)$ implies there is a $\bar{t} \in [t_1, t_2]$ such that

$$\bar{t} = \max\{t \in [t_1, t_2) \mid dist(t) = 0\}, \tag{5}$$

because the preimage of a closed set must be closed under a continuous function. By the continuity of $\Phi_A^{cl}(t)$, it follows that $\Phi_A^{cl}(\bar{t}) \cap \partial C_{\mathbf{u}_L} \neq \emptyset$.

At time $\bar{t}$ we also have that $\Phi_A^{cl}(\bar{t}) \cap C_{\mathbf{u}_H} \neq \emptyset$ and $\Phi_A^{cl}(\bar{t}) \cap C_{\mathbf{u}_L} = \emptyset$, implying from the definition of G in (4) that

$$G(\Phi_A^{cl}(\bar{t})) = u_L. \tag{6}$$

From (5), we have $dist(t) \neq 0$ for all $t \in (\bar{t}, t_2]$, implying that $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_L} \neq \emptyset$ for all $t \in (\bar{t}, t_2]$. Since $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_H} \neq \emptyset$ also holds for all $t \in (\bar{t}, t_2]$, $G(\Phi_A^{cl}(t)) = U$ for all $t \in (\bar{t}, t_2]$. Thus, $u_L \in G(\Phi_A^{cl}(t))$ for all $t \in (\bar{t}, t_2]$. Now let $y \in \Phi_A^{cl}(t_2) \cap C_{\mathbf{u}_L}$ and choose $z \in \Phi_A^{cl}(\bar{t})$ such that $\phi(t_2 - \bar{t}, z, (\mathbf{u}_L, \boldsymbol{\delta})) = y$, for some $\boldsymbol{\delta} \in S(\Delta)$. Since $y \in C_{\mathbf{u}_L}$ and $\mathbf{u}_L = u_L$ for all $t \in [\bar{t}, t_2]$, we must have that $z \in C_{\mathbf{u}_L}$ by the definition of $C_{\mathbf{u}_L}$. This leads to a contradiction, since we assume $\Phi_A^{cl}(\bar{t}) \cap C_{\mathbf{u}_L} = \emptyset$. As a consequence, such an interval $[t_1, t_2]$ for which Case(I) holds cannot exit.

For Case(II) and Case (III), a similar argument holds. Therefore $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_L} = \emptyset$ or $\Phi_A^{cl}(t) \cap C_{\mathbf{u}_H} = \emptyset$ must always hold under G for all $t \in \mathbb{R}_+$. Thus, implying that $\Phi_A^{cl}(t) \cap \mathbf{B} = \emptyset$ for all $t \in \mathbb{R}_+$. ∎

We summarize the solutions to Problem 1 and Problem 2 in the two following theorems, respectively.

Theorem 3: (Solution to Problem 1) The set W of Problem 1 is given by $W = X \backslash (C_{\mathbf{u}_L} \cap C_{\mathbf{u}_H})$. A feedback map $g : X \rightrightarrows U$ is given by

$$g(x) := \begin{cases} u_L & \text{if } x \in C_{\mathbf{u}_H} \text{ and } x \in \partial C_{\mathbf{u}_L} \\ u_H & \text{if } x \in C_{\mathbf{u}_L} \text{ and } x \in \partial C_{\mathbf{u}_H} \\ \{u_L, u_H\} & \text{if } x \in \partial C_{\mathbf{u}_L} \text{ and } x \in \partial C_{\mathbf{u}_H} \\ U & \text{otherwise.} \end{cases}$$

Proof: Direct consequence of Corollary 1 and Theorem 2, in which A is a singleton. ∎

Theorem 4: (Solution to Problem 2) A convex set $\hat{x}_0 \subset X$ is in $\bar{W}$ if and only if $\hat{x}_0 \cap C_{\mathbf{u}_L} = \emptyset$ or $\hat{x}_0 \cap C_{\mathbf{u}_H} = \emptyset$. Furthermore, if $\hat{x}_0 \subset \bar{W}$ is also compact, then a dynamic feedback map $G : 2^X \rightrightarrows U$ is given by (4).

Proof: By Theorem 1, there exists a $\mathbf{u} \in S(U)$ such that $\phi(t, A, (\mathbf{u}, \boldsymbol{\delta})) \cap \mathbf{B} = \emptyset$ for all $\boldsymbol{\delta} \in S(\Delta)$ and $t \in \mathbb{R}_+$ if and only if $A \cap C_{\mathbf{u}_L} = \emptyset$ or $A \cap C_{\mathbf{u}_H} = \emptyset$. Letting $A = \hat{x}_0$ and assuming $\mathbf{z}$ is the worst-case observation signal that does not restrict the flow $\phi(t, A, (\mathbf{u}, \boldsymbol{\delta}))$ further, we have that $\hat{x}(t, \hat{x}_0, \mathbf{u}, \mathbf{z}) = \phi(t, A, (\mathbf{u}, \boldsymbol{\delta}))$ for all $t \in \mathbb{R}_+$. Therefore, there is an input $\mathbf{u} \in S(U)$ such that $\hat{x}(\mathbb{R}_+, \hat{x}_0, \mathbf{u}, \mathbf{z}) \cap \mathbf{B} = \emptyset$ for all $\boldsymbol{\delta} \in S(\Delta)$ and $t \in \mathbb{R}_+$ if and only if $\hat{x}_0 \cap C_{\mathbf{u}_L} = \emptyset$ or $\hat{x}_0 \cap C_{\mathbf{u}_H} = \emptyset$. Theorem 2 shows that feedback map G given by (4) maintains $\Phi_{\hat{x}_0}^{cl}(t)$ not intersecting $\mathbf{B}$ for all $t \in \mathbb{R}_+$ and thus $\hat{x}(t, \hat{x}_0, \mathbf{u}, \mathbf{z})$ with $\mathbf{u}(\tau) \in G(\hat{x}(\tau, \hat{x}_0, \mathbf{uz}))$ $\forall \tau \in \mathbb{R}_+$ does not intersect $\mathbf{B}$ for all $t \in \mathbb{R}_+$. ∎

Since the static feedback map g is equivalent to the dynamic feedback map G with set inclusion replaced by membership, a separation principle holds for $\Sigma^1 \| \Sigma^2$ between state estimation and control.

V. Algorithms Implementation

By virtue of Theorems 3 and 4, the static and dynamic control Problems 1 and 2 can be solved by computing the sets $C_{\mathbf{u}_L}$ and $C_{\mathbf{u}_H}$. These sets can be in turn computed by linear complexity algorithms. With the idea of digital implementation, we illustrate our algorithm in discrete time. We assume that f_1^i does not depend on x_1^i for $i \in \{1, 2\}$. This structure is found, for example, in systems consisting of chains of integrators. These can be in turn be realized after the feedback linearization of a nonlinear system (when such a transformation exists).

Let $\bar{x}^i := (x_2^i, \ldots, x_n^i)$, $\bar{f}^i := (f_1^i, \ldots, x_n^i)$ and define the discretized system (using the forward Euler approximation) with step size $\Delta T > 0$ and index n

$$\begin{aligned} x_1^i[n+1] &= x_1^i[n] + F_1^i(\bar{x}^i[n], \mathbf{u}^i[n]), \\ \bar{x}^i[n+1] &= \bar{x}^i[n] + \bar{F}^i(\bar{x}^i[n], \mathbf{u}^i[n]), \end{aligned}$$

in which $F_1^i(\bar{x}^i[n], \mathbf{u}^i[n]) := \Delta T f_1^i(\bar{x}^i[n], \mathbf{u}^i[n])$ and $\bar{F}^i(\bar{x}^i[n], \mathbf{u}^i[n]) := \Delta T \bar{f}^i(\bar{x}^i[n], \mathbf{u}^i[n])$ are order preserving in both arguments. For a given bad set $\mathbf{B}$ with $\tau_{1,n+1}(\mathbf{B})$ bounded, we construct an over-approximation of $\mathbf{B}$ using intervals. Let $L^1 = \inf \tau_1(\mathbf{B})$, $U^1 = \sup \tau_1(\mathbf{B})$, $L^2 = \inf \tau_{n+1}(\mathbf{B})$, and $U^2 = \sup \tau_{n+1}(\mathbf{B})$. Thus we must have $B \subset [L^1, U^1] \times [L^2, U^2]$. Thus, we have $\mathbf{B} \subset \tilde{\mathbf{B}} := [L^1, U^1] \times \mathbb{R}^{n-1} \times [L^2, U^2] \times \mathbb{R}^{n-1}$. Note that if B is a box, then $\mathbf{B} = \tilde{\mathbf{B}}$ and our computation exactly determines the restricted capture sets $C_{\mathbf{u}_L}$ and $C_{\mathbf{u}_H}$.

We next propose the algorithm used to compute the restricted capture sets. Set $\bar{F}^{i,0}(\bar{x}^i[n], \mathbf{u}^i[n]) := 0$, $\bar{F}^{i,1}(\bar{x}^i[n], \mathbf{u}^i[n]) := \bar{x}^i[n], \mathbf{u}^i[n]$ and recursively define $\bar{F}^{i,k+1}(\bar{x}^i[n], \mathbf{u}^i[n]) := \bar{F}^i(\bar{F}^{i,k}(\bar{x}^i[n], \mathbf{u}^i[n]), \mathbf{u}^i[n])$ for $k \in \mathbb{N}$. With the goal of computing $C_{\mathbf{u}_L}$ and $C_{\mathbf{u}_H}$, we consider the initial conditions $\bar{x}^1, \bar{x}^2 \in \mathbb{R}^{n-1}$, and define

$$\begin{aligned} L^{1,k}(\bar{x}^1[n], u) &:= L^1 - \textstyle\sum_{j=0}^{k-1} F_1^1(\bar{x}^1[n] + \bar{F}^{1,j}(\bar{x}^1[n], u), u) \\ U^{1,k}(\bar{x}^1[n], u) &:= U^1 - \textstyle\sum_{j=0}^{k-1} F_1^1(\bar{x}^1[n] + \bar{F}^{1,j}(\bar{x}^1[n], u), u), \\ L^{2,k}(\bar{x}^2[n], u) &:= L^1 - \textstyle\sum_{j=0}^{k-1} F_1^2(\bar{x}^2[n] + \bar{F}^{2,j}(\bar{x}^2[n], \delta_H), \delta_H) \\ U^{2,k}(\bar{x}^2[n], u) &:= U^2 - \textstyle\sum_{j=0}^{k-1} F_1^2(\bar{x}^2[n] + \bar{F}^{2,j}(\bar{x}^2[n], \delta_L), \delta_L). \end{aligned}$$

For $\mathbf{u}(t) = u \in U$ for all $t \in \mathbb{R}_+$, one can check that

$$C_{\mathbf{u}} = \left\{ \begin{array}{c} x \in X \mid \exists k \geq 0 \text{ such that} \\ L^{i,k}(\bar{x}^i, u) < x_1^i < U^{i,k}(\bar{x}^i, u) \ \forall\ i \in \{1, 2\} \end{array} \right\}.$$

Since the dynamics of the system are order preserving with respect to the state, we construct a state estimator that keeps track of only the lower and upper bounds of the information state. Let $\vee\hat{x}^i := \sup \hat{x}^i$ and $\wedge\hat{x}^i := \inf \hat{x}^i$ denote the upper and lower bounds respectively of the set of possible current states $\hat{x}^i$. Let $\mathbf{z}^i$ be an output measurement of for the i^{th} agent, let $h^i(z^i[n]) = [\inf h^i(z^i[n]), \sup h^i(z^i[n])]$ and let $z^i_+ := z^i[n+1]$. Then a state estimator that updates $\vee\hat{x}$ and $\wedge\hat{x}$ is given by

$$\begin{aligned}
\vee\hat{x}^1[n+1] &= \vee\hat{x}^1[n] + \inf\{F^1_1(\vee\hat{x}^1[n], \mathbf{u}[n]), \sup h^1(z^1_+)\},\\
\wedge\hat{x}^1[n+1] &= \wedge\hat{x}^1[n] + \sup\{F^1_1(\wedge\hat{x}^1[n], \mathbf{u}[n]), \inf h^1(z^1_+)\},\\
\vee\hat{x}^2[n+1] &= \vee\hat{x}^2[n] + \inf\{F^2_1(\vee\hat{x}^2[n], \delta_L), \sup h^2(z^2_+)\},\\
\wedge\hat{x}^2[n+1] &= \wedge\hat{x}^2[n] + \sup\{F^2_1(\wedge\hat{x}^2[n], \delta_H), \inf h^2(z^2_+)\}.
\end{aligned}$$

At every time step n, one needs to check whether $[\vee\hat{x}[n], \wedge\hat{x}[n]]$ intersects $C_{\mathbf{u}_L}$ or $C_{\mathbf{u}_H}$. From assumption (ii) in Definition 3, we know that $\bar{F}^i(\bar{x}^i[n], u^i)$ is order preserving in the argument $\bar{x}^i[n]$, thus the functions $L^{1,k}(\bar{x}^1[n], u)$ are order reversing in the argument $\bar{x}^1$. Let $L^k(\hat{x}[n], u_L) := (L^{1,k}(\hat{x}^1[n], u_L), L^{2,k}(\hat{x}^2[n], u_L))$ and $U^k(\hat{x}[n], u_L) := (U^{1,k}(\hat{x}^1[n], u_L), U^{2,k}(\hat{x}^2[n], u_L))$. Therefore, a sufficient condition guaranteeing that for some $i \in \{1,2\}$, we have $[\vee x[n], \wedge x[n]] \cap (\bigcup_k [L^k(\hat{x}[n], u_L), U^k(\hat{x}[n], u_L)]) = \emptyset$, is that for all $k \in \mathbb{N}$, there exists $i \in \{1,2\}$ such that

$$[\vee x^i[n], \wedge x^i[n]] \cap [L^{i,k}(\vee\hat{x}^i[n], u_L), U^{i,k}(\wedge\hat{x}^i[n], u_L)] = \emptyset. \quad (7)$$

Condition (ii) of Definition 3 implies that the sequences $\{L^{i,k}(\hat{x}^i[n], u)\}_{k\in\mathbb{N}}$ and $\{U^{i,k}(\hat{x}^i[n], u)\}_{k\in\mathbb{N}}$ are strictly monotonically decreasing to $-\infty$. Therefore, condition (7) need only be checked for all $k \in \mathbb{N}$ such that $\wedge\hat{x} \geq U^k(\hat{x}^i[n], u)$. This guarantees *termination* of the dynamic algorithm that computes the control map.

VI. Simulation Results

We illustrate the application of the algorithms outlined in Section V on a system that is naturally order preserving. We consider the problem of maintaining a safety specification for two vehicles merging at a traffic intersection (Figure 3). The controlled agent has imperfect knowledge of the entire state, a condition present when sensors are assumed to only provide information subject to bounded error (due to GPS measurements, for example). For practical reasons, both agents are forced to maintain a strictly positive bounded forward velocity, which is accomplished by modifying the second order model from [18] to include a fixed invariant, yielding the piecewise continuous system depicted in Figure 2.

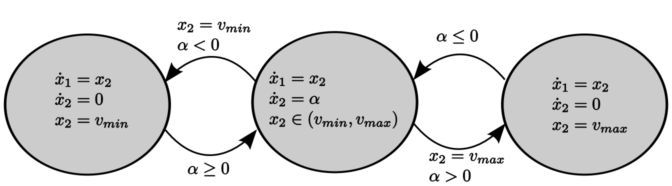


Fig. 2. Hybrid system modeling the dynamics of each agent. In the diagram, we denote $\alpha := au + b + cx_2^2$.

One can verify that each agent satisfies all conditions of Definition 3. We implement the algorithms of Section V symbolically to compute the restricted capture sets $C_{\mathbf{u}_L}$ and $C_{\mathbf{u}_H}$. Figure 4 shows the execution of the closed-loop system.

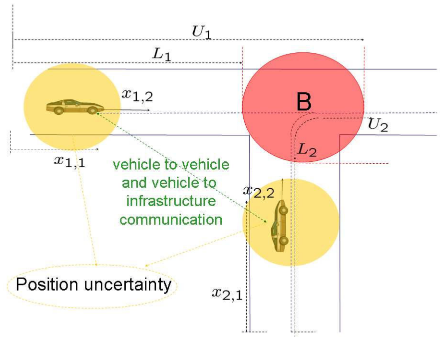


Fig. 3. Example of vehicles converging at an intersection. The bad set **B** represents all configurations where the vehicles overlap at the intersection.

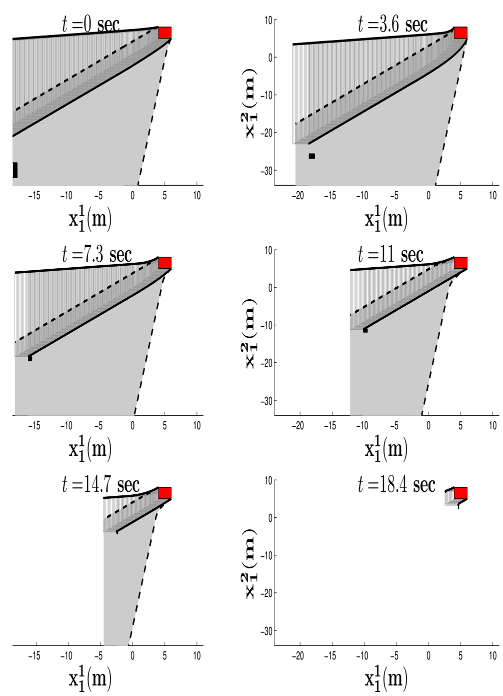


Fig. 4. The above plots depict snapshots of the dynamic evolution of the closed-loop system. The system considered has $a^i = 1$, $b^i = -.5$ and $c^i = -.1$ for $i \in \{1,2\}$, with $v_{min} = .25\ m/sec$ and $v_{max} = 2\ m/sec$. We choose $\Delta T = .1$ sec, $\mathbf{B} = [4,6] \times \mathbb{R} \times [5,8] \times \mathbb{R}$, $U = \Delta = I$, $x_0 = (-20, .5, -30, .5)$, $\hat{x}_0 = [-22, -18] \times [.3, .7] \times [-32, -28] \times [.3, .7]$. The measurements z are generated randomly with a uniform probability distribution in the interval $[x(t) - (5, .5, 5, .5), x(t) + (5, .5, 5, .5)]$ so that $h(z) = [z - (5, .5, 5, .5), z + (5, .5, 5, .5)]$. The black box represents the projection of $\hat{x}(t)$ onto the (x_1^1, x_1^2) plane. The red box represents the projection of **B** onto the (x_1^1, x_1^2) plane, the slice of $C_{\mathbf{u}_L}$ corresponding to the current velocities is shown in light grey with a solid outline and the slice of $C_{\mathbf{u}_H}$ corresponding to the current velocities is shown in dark grey with a dashed outline.

VII. Conclusion and Future Work

In this paper, we have considered the problem of safety control for a class of hybrid systems with imperfect state information, disturbances, and order preserving dynamics. By exploiting the order preserving dynamics, we provided static and dynamic feedback maps that can be computed by linear complexity algorithms. The resulting control maps

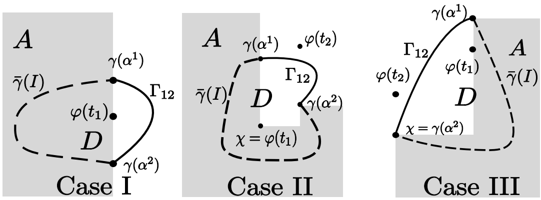


Fig. 5. Three Cases.

for the static and dynamic control problem have the same structure. This highlights a separation principle between state estimation and control for the class of systems studied in this work.

Future work includes extending the algorithms to more general hybrid systems with continuous state reset and discrete state dynamics [19].

VIII. Appendix: Proof of Lemma 1

Before giving the proof of Lemma 1, we need the following intermediate results.

Proposition 1: Consider $\Sigma^1 \| \Sigma^2$, $x = (x^1, x^2) \in X, \mathbf{u} \in S(U), \boldsymbol{\delta} \in S(\Delta)$ and $\gamma \in C^0(I, \mathbb{R}^2)$ o.p.c. where $x_1^1 \leq \max \tau_1(\gamma(I))$. Then, we have that $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \gtrsim \gamma(I)$ or $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \lesssim \gamma(I)$ if and only if $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \cap \gamma(I) = \emptyset$.

Proof: ($\Rightarrow$) Follows from the definition of the $\lesssim$ relation.

($\Leftarrow$) Suppose $\{\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \gtrsim \gamma(I)$ or $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \lesssim \gamma(I)\}$ does not hold. The hypothesis $\phi_1^1(0, x, (\mathbf{u}, \boldsymbol{\delta})) \leq \sup \tau_1(\gamma(I))$ and condition (iii) of Definition 3 imply that there exist $\alpha^1, \alpha^2 \in I$ and $t_1, t_2 \in \mathbb{R}_+$ such that $\phi_1^{1,2}(t_1, x, (\mathbf{u}, \boldsymbol{\delta})) \lesssim \gamma(\alpha^1)$ and $\phi_1^{1,2}(t_2, x, (\mathbf{u}, \boldsymbol{\delta})) \gtrsim \gamma(\alpha^2)$. For simplifying notation, let $\varphi(t) := \phi_1^{1,2}(t, x, (\mathbf{u}, \boldsymbol{\delta}))$. Without loss of generality, assume $\alpha^1 \leq \alpha^2$, define $\chi := (\min\left\{\gamma_1(\alpha^1), \gamma_1(\alpha^2)\right\}, \min\left\{\phi_1^2(t_1, x, \mathbf{u}, \boldsymbol{\delta}), \gamma_2(\alpha^2)\right\})$, and $\Gamma_{12} := \gamma([\alpha^1, \alpha^2])$. By the construction of χ, we have that $\gamma(\alpha^1), \gamma(\alpha^2) \in \mathrm{Cone}_+(\chi)$, which implies that $\Gamma_{12} \subset \mathrm{Cone}_+(\chi)$ by the definition of o.p.c.

We now consider the three possible cases: (Case I) $t_1 = t_2$, (Case II) $t_1 < t_2$, and (Case III) $t_1 > t_2$.

(Case II) Suppose $t_1 < t_2$. This along with condition (ii) of Definition 3 implies that $\gamma_1(\alpha^1) < \gamma_1(\alpha^2)$. We assume that $\varphi(t_1) \lesssim \gamma(I)$ and $\varphi(t_2) \gtrsim \gamma(I)$, otherwise we would be back to (Case I). Define the sets $S_1 := \mathrm{Cone}_{\{\hat{e}_1, -\hat{e}_2\}}(\gamma(\alpha^2))$ and $S_2 := \mathrm{Cone}_+(\chi)$. Define $A := \mathring{S}_1 \cup (\sim S_2)$ and $\tilde{A} := A \cup \gamma(\alpha^1) \cup \gamma(\alpha^2)$. Since γ is an o.p.c. path, $\Gamma_{12} \subset \mathrm{Cone}_+(\chi)$ and $\Gamma_{12} \cap S_1 = \emptyset$, we must have that $\Gamma_{12} \cap A = \emptyset$. The set $\tilde{A}$ is path connected, implying the existence of $\bar{\gamma} \in C^0(I, \tilde{A})$ with $\bar{\gamma}(0) = \gamma(\alpha^1)$, $\bar{\gamma}(1) = \gamma(\alpha^2)$ and $\bar{\gamma}$ simple. Since $A \cap \Gamma_{12} = \emptyset$, $\bar{\gamma}(I) \cup \Gamma_{12}$ can be re-parameterized with a simple closed curve (see Figure 5). This curve, by the Jordan Curve Theorem, forms a bounded set D, where $\varphi(t_1) \in D$ by construction. Condition (ii) and (iii) of Definition 3 along with the decoupling of the dynamics imply that $\varphi([t_1, \infty]) \cap A = \emptyset$ and $\varphi([t_1, \infty]) \cap \partial D \neq \emptyset$. Since $\bar{\gamma} \subset A$, we have that $\varphi([t_1, \infty]) \cap \Gamma_{12} \neq \emptyset$. Therefore, $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \cap \gamma(I) \neq \emptyset$.

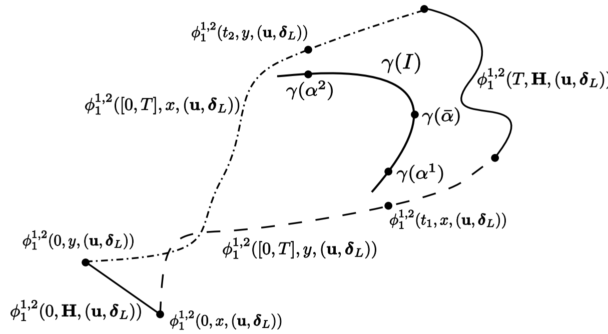


Fig. 6. Geometry of $\phi_1^1(t, x, (\mathbf{u}, \boldsymbol{\delta}_L))$ and $\phi_1^1(t, y, (\mathbf{u}, \boldsymbol{\delta}_L))$.

The arguments for Case I and Case III follow in a similar manner, see Figure 5.

Therefore, we have shown for each case $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta})) \cap \gamma(I) \neq \emptyset$, completing the proof. ∎

Proposition 1 states that the flow ϕ generated from the initial condition x and input $\mathbf{u}$ and disturbance $\boldsymbol{\delta}$ can avoid an o.p.c. path γ in the (x_1^1, x_1^2) subspace if and only if the trajectory of $\phi_1^{1,2}$ lies above γ or if the trajectory of $\phi_1^{1,2}$ lies below γ. Another intermediate result is needed before stating the proof of Lemma 1.

Proposition 2: Consider $\Sigma^1 \| \Sigma^2$, $x = (x^1, x^2) \in X, \mathbf{u} \in S(U)$ and $\gamma \in C^0(I, \mathbb{R}^2)$ o.p.c. with $x_1^1 \leq \max \tau_1(\gamma(I))$. If $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, S(\Delta))) \cap \gamma(I) = \emptyset$, then either $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \gtrsim \gamma(I)$ or $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta}_H)) \lesssim \gamma(I)$.

Proof: Follows directly from the order preserving property with respect to input and the decoupling of the dynamics. ∎

Proposition 2 states that the flow ϕ generated from the initial condition x and input $\mathbf{u}$ can avoid an o.p.c. path γ in the (x_1^1, x_1^2) subspace if and only if the trajectory of $\phi_1^{1,2}$ lies above γ or if the trajectory of $\phi_1^{1,2}$ lies below γ.

Proof: (*Lemma 1*) ($\Leftarrow$) Follows from the definition of the $\lesssim$ relation.

($\Rightarrow$) Suppose $\{\phi_1(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_L)) \gtrsim \gamma(I)$ or $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, \boldsymbol{\delta}_H)) \lesssim \gamma(I)\}$ does not hold. Then there must exist $x, y \in A$, $\alpha^1, \alpha^2 \in I$, and $t_1, t_2 > 0$ such that $\phi_1^{1,2}(t_1, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \lesssim \gamma(\alpha^1)$ and $\phi_1^{1,2}(t_2, y, (\mathbf{u}, \boldsymbol{\delta}_H)) \gtrsim \gamma(\alpha^2)$. We assume that $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \lesssim \gamma(I)$, otherwise Proposition 1 implies that $\phi_1^{1,2}(\mathbb{R}_+, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \cap \gamma(I) \neq \emptyset$. Likewise, we assume that $\phi_1^{1,2}(\mathbb{R}_+, y, (\mathbf{u}, \boldsymbol{\delta}_L)) \gtrsim \gamma(I)$. Figure 6 shows the resulting geometry of the flow. Let $\bar{\alpha} \in I$ be such that $\tau_1(\gamma(I)) \leq \tau_1(\gamma(\bar{\alpha}))$. Condition (iii) of Definition 3 along with (a) leads to $\phi_1^1(0, x, (\mathbf{u}, \boldsymbol{\delta}_L)) < \phi_1^1(t_1, x, (\mathbf{u}, \boldsymbol{\delta}_L)) \leq \gamma_1(\bar{\alpha})$ and $\phi_1^1(0, y, (\mathbf{u}, \boldsymbol{\delta}_L)) < \phi_1^1(t_2, y, (\mathbf{u}, \boldsymbol{\delta}_L)) \leq \gamma_1(\bar{\alpha})$. Consider $H := \mathrm{co}(\{x, y\}) \subset A$, since convexity is preserved under projection [3], condition (iii) of Definition 3 implies there is $T > 0$ such that

$$\phi_1^1(0, H, (\mathbf{u}, \boldsymbol{\delta}_L)) < \{\gamma_1(\bar{\alpha})\} < \phi_1^1(T, H, (\mathbf{u}, \boldsymbol{\delta}_L)). \quad (8)$$

We seek to show that $\gamma(\bar{\alpha}) \in \phi_1([0, T], H, (\mathbf{u}, \boldsymbol{\delta}_L))$. Define $K := [0, T] \times H \subset \mathbb{R}_+ \times \mathbb{R}^{2n}$ and let $\Theta : K \to \mathbb{R}^2$ be the map defined by $\Theta(t, z) := \phi_1^{1,2}(t, z, (\mathbf{u}, \boldsymbol{\delta}_L))$ for $(t, z) \in K$. We proceed by breaking this proof into three steps: (i) Construct

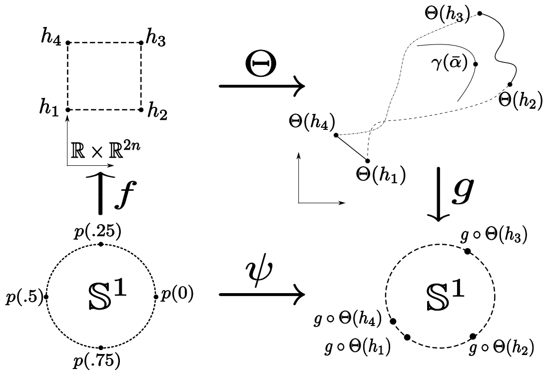
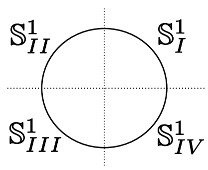


Fig. 7. The Mapping ψ.

$$\begin{tikzcd} I \arrow[r, "\tilde{\psi}"] \arrow[d, "p"'] & \mathbb{R} \arrow[d, "p"] \\ \mathbb{S}^1 \arrow[r, "\psi"] & \mathbb{S}^1 \end{tikzcd}$$

(a) Commuting Diagram



(b) Four Quadrants

Fig. 8. Tools used to find deg ψ.

from Θ a map $\psi : \mathbb{S}^1 \to \mathbb{S}^1$; (ii) Show that the degree of ψ is nonzero; (iii) Show that the degree of ψ being nonzero implies that $\gamma(\bar{\alpha}) \in \Theta(K)$.

(i) Denote the four corners of $\partial K : h_1 = (0,x)$, $h_2 = (T,x)$, $h_3 = (T,y)$, $h_4 = (0,y)$. Define the sets $A_1 := \mathrm{co}(\{h_1,h_2\}) \cup \mathrm{co}(\{h_2,h_3\})$ and $A_2 := \mathrm{co}(\{h_3,h_4\}) \cup \mathrm{co}(\{h_4,h_1\})$. Consider the standard covering map of $\mathbb{S}^1$ $p : \mathbb{R} \to \mathbb{S}^1$, in which $p(z) := (cos(2\pi z), sin(2\pi z))$. Define the homeomorphism $f : \mathbb{D}^1 \to K$, such that $f(p(0)) = h_1$, $f(p(.25)) = h_2$, $f(p(.5)) = h_3$, and $f(p(.75)) = h_4$. Since Θ is a continuous function, we have that $\Theta(\partial K)$ defines a closed curve. Assume that $\gamma(\bar{\alpha}) \notin \Theta(\partial K)$ and let $g : \mathbb{R}^2\backslash\gamma(\bar{\alpha}) \to \mathbb{S}^1$ be the continuous map defined by

$$g(z) := \frac{z - \gamma(\bar{\alpha})}{\|z - \gamma(\bar{\alpha})\|},\ \forall z \in \mathbb{R}^2\backslash\gamma(\bar{\alpha}). \tag{9}$$

Define $\psi \in C^0(\mathbb{S}^1, \mathbb{S}^1)$ as $\psi(x) := (g \circ \Phi \circ f)(x)$ for all $x \in \mathbb{S}^1$ (see Figure 7).

(ii) To compute the degree of ψ, we consider the lift $\tilde{\psi} : I \to \mathbb{R}$ where $p \circ \tilde{\psi} = \psi \circ p$ (see Figure 8(a)). The degree of ψ is defined as deg $\psi := \tilde{\psi}(1) - \tilde{\psi}(0)$ (see [12] for details). We introduce the sets $\mathbb{S}^1_I := p([0,.25]), \mathbb{S}^1_{II} := p([.25,.5]), \mathbb{S}^1_{III} := p([.5,.75]), \mathbb{S}^1_{IV} := p([.75,1])$ (see Figure 8(b)). Let $\mu_1 := \tilde{\psi}(0)$ and note that $p(\mu_1) = \psi(p(0)) = g(\Theta(h_1))$, which must be in $\mathbb{S}^1_{III}$, since $\Theta(h_1) < \gamma(\bar{\alpha})$. Let $\mu_2 = \tilde{\psi}(.5)$ and note that $p(\mu_2) = \psi(p(.5)) = g(\Theta(h_3))$. From (8) and condition (iii) of Definition 3, we have that $\gamma(\bar{\alpha}) < \Theta(h_3)$. This inequality along with the definition of g imply that $g(\Theta(h_3)) \in \mathbb{S}^1_I$. As a consequence, we have $p(\mu_2) \in \mathbb{S}^1_I$, implying that $\mu_1 \neq \mu_2$.

Finally, let $\tilde{\psi}(1) = \mu_3$. We can show without much difficulty that $\mu_1 < \mu_2 < \mu_3$. As a consequence, deg $\psi = \tilde{\psi}(1) - \tilde{\psi}(0) = \mu_3 - \mu_1 \neq 0$.

(iii) Now suppose we extend the map ψ to $\bar{\psi} \in C^0(\mathbb{D}^1, \mathbb{S}^1)$, where $\bar{\psi}(x) := (g \circ \Theta \circ f)(x)$ for all $x \in \mathbb{D}^1$. By Lemma 3.5.7 in [12], if a continuous function $h : \mathbb{S}^1 \to \mathbb{S}^1$ extends to a continuous function $H : \mathbb{D}^1 \to \mathbb{S}^1$, then deg h must be zero. However, we found the degree of ψ to be non-zero, implying that ψ cannot extend to $\bar{\psi}$. Since $\Theta(f(\mathbb{D}^1))$ is well defined, we must have that $g(\Theta(f(\mathbb{D}^1)))$ is undefined. Since $g(z)$ is defined for all $z \in \mathbb{R}^2\backslash\gamma(\bar{\alpha})$, we must have that $\gamma(\bar{\alpha}) \in \Theta(f(\mathbb{D}))$. This implies that $\gamma(\bar{\alpha}) \in \Theta(K) = \phi_1([0,T], H, (\mathbf{u}, \boldsymbol{\delta}_L)) \subset \phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, S(\Delta)))$. Therefore, $\phi_1^{1,2}(\mathbb{R}_+, A, (\mathbf{u}, S(\Delta))) \cap \gamma(I) \neq \emptyset$

■

References

[1] D. Angeli and E. D. Sontag. Monotone control systems. *IEEE Transactions on Automatic Control*, 48:1684–1698, 2003.

[2] J. Aubin and H. Frankowska. *Set-Valued Analysis*. Systems and Control: Foundations and Applications. Birkhäuser, Boston, 1990.

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

[4] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, Cambridge, UK, 2002.

[5] D. Del Vecchio. A partial order approach to discrete dynamic feedback in a class of hybrid systems. In *Hybrid Systems: Computation and Control,* Lecture Notes in Computer Science, vol. 4416, A. Bemporad, A. Bicchi, and G. Buttazzo (Eds.), Springer Verlag, pages 159–173, Pisa, Italy, 2007.

[6] D. Del Vecchio. Observer-based control of block triangular discrete time hybrid automata on a partial order. *International Journal of Robust and Nonlinear Control*, 2008.

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

[8] O. Maler E. Asarin and A.Pnueli. Symbolic controller synthesis for discrete and timed systems. In *Hybrid Systems II,* Lecture Notes in Computer Science, vol. 999, P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry (Eds.), Springer Verlag, pages 1–20, 1995.

[9] T. A. Henzinger, P. H. Ho, and H. Wong-Toi. A user guide to HyTech. In *TACAS 95: Tools and Algorithms for the construction and analysis of systems,* Lecture Notes in Computer Science, vol. 1019, E. Brinksma, W. Cleaveland, K. Larsen, T. Margaria, and B. Steffen (Eds.), Springer-Verlag, pages 41–71, 1995.

[10] A. B. Kurzhanski and P. Varaiya. Ellipsoidal techniques for hybrid dynamics: the reachability problem. In *New Directions and Applications in Control Theory,* Lecture Notes in Control and Information Sciences, vol 321, W.P. Dayawansa, A. Lindquist, and Y. Zhou (Eds.), pages 193–205, 2005.

[11] S. M. LaValle. *Planning Algorithms*. Cambridge University Press, 2006.

[12] T. Lawson. *Topology: A Geometric Approach*. Oxford, 2003.

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

[14] J. R. Munkres. *Topology*. Prentice Hall, second edition, 2000.

[15] O. Shakernia, G. J. Pappas, and S. Sastry. Semi-decidable synthesis for triangular hybrid systems. In *Hybrid Systems: Computation and Control,* Lecture Notes in Computer Science, vol. 2034, M. D. Di Benedetto and A. Sangiovanni-Vincentelli (Eds.), Springer Verlag, 2001.

[16] 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.

[17] 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.

[18] R. Verma, D. Del Vecchio, and H. Fathy. Development of a scaled vehicle with longitudinal dynamics of a HMMWV for an its testbed. *IEEE/ASME Transactions on Mechatronics*, 13(1):46–57, 2008.

[19] R. Verma and D. Del Vecchio. Continuous control of hybrid automata with imperfect mode information assuming separation between state estimation and control. *Proc. of Conference on Decicion and Control*, 2009 (To Appear).

[20] M. De Wulf, L. Doyen, and J.-F. Raskin. A lattice theory for solving games of imperfect information. *Hybrid Systems: Computation and Control,* Lecture Notes in Computer Science, vol. 3927, J. Hespanha and A. Tiwari (Eds.), Springer-Verlag, pages 153–168, 2006.