Forward Invariance-Based Hybrid Control Using Uncertified Controllers

Paul K. Wintz

Ricardo G. Sanfelice

Abstract—For a constrained nonlinear control system, an automated supervisor is proposed that determines switching between a barrier function–certified controller and an uncertified controller. The switching strategy allows for properties of the uncertified controller to be exploited while preserving the forward invariance that is guaranteed by the barrier function for the certified controller. Tunable threshold functions determine regions of the state space where the supervisor switches between controllers. Conditions are given to prevent chattering by establishing a positive minimum time between switches. An example illustrates achieving forward invariance despite using an uncertified MPC controller with delayed computations.

I. INTRODUCTION

Control systems often have operational constraints, such as physical obstacles, legal regulations, or limits on the amount of force or electrical current that a system can safely endure. A popular approach to verify that a system satisfies its constraints is via a barrier function (also called a barrier certificate) [1]–[3]. There are several definitions of barrier functions in the literature [4]. For the definition used in this paper, a barrier function maps the system’s state space to $\mathbb{R}$ and satisfies conditions such that its zero-sublevel set is forward invariant and every point in that set is admissible. The zero-level set is a barrier that the state cannot cross, so if the system starts in the zero-sublevel set, then it is safe.

We consider a continuous-time nonlinear plant with state space $\mathbb{R}^n$ and a set $K \subset \mathbb{R}^n$ that we want to render forward invariant. If, for a controller $\kappa$, the set $K$ is rendered forward invariant and a barrier function of $K$ is known for the closed-loop system, then we say $\kappa$ is barrier-certified. A controller for which a barrier function is unavailable is uncertified.

Although uncertified controllers are not expected to render the set $K$ forward invariant, they can have other desirable properties, such as tracking a reference trajectory, minimizing control effort, or reducing computational demands. As an example, consider model predictive control (MPC). An MPC controller computes the input at discrete sample times by solving a finite-horizon optimization problem. The advantages of MPC are that it computes an approximately optimal control input that satisfies constraints. For nonlinear systems with nonlinear constraints, however, computing an MPC input is computationally expensive, which can lead to delayed updates that cause the system to violate constraints (see Example 2 and [5]). This motivates the development of supervisory control that uses a certified controller as “guard rails”—if the uncertified controller moves the system too close to the unsafe set, an automated supervisor triggers a switch to the certified controller so that the system stays in the safe set.

The Simplex architecture is an approach for switching between an “advanced,” uncertified controller and a “simple,” easy-to-verify controller [6], [7]. In the Simplex architecture, a decision module decides at each time step whether to use the uncertified controller—if it is performing safely—or to fall back to the verified controller. In [8], barrier functions are used with the Simplex architecture to achieve safety for hybrid systems, but this approach requires costly reachability analysis and has only “one way” switching—that is, there are no conditions given for returning to the uncertified controller after switching to the verified controller. The Simplex architecture is also used with a barrier certificate in [9], but there are several limitations to their approach that we overcome in this paper; namely, only rectangular constraints are considered, and the switching criteria depend on the extremal values of the vector field over the entire admissible set, leading to excessive conservatism.

In this paper, we introduce a hybrid control strategy for switching between a barrier-certified controller $\kappa_0$ and an uncertified controller $\kappa_1$ such that the set $K$ is forward invariant for the resulting hybrid closed-loop system; the uncertified controller $\kappa_1$ is preferred over the certified controller $\kappa_0$; and the switching between $\kappa_0$ and $\kappa_1$ does not chatter (the time between all switches is greater than some positive constant). In our switching strategy, user-defined thresholds on the value and the rate-of-change of the barrier function determine where switches occur. The thresholds are defined as functions of the state, so that larger margins can be chosen in regions where the system has faster dynamics. We show that our hybrid control strategy renders $K$ forward invariant, and we provide conditions for establishing a positive minimum time between switches. For a similar supervisory approach applied to asymptotic stability, see our previous work [10].

The remainder of this paper is organized as follows: Section II introduces preliminary concepts and notation, Section III gives the problem setting, Section IV describes our switching scheme and the resulting closed-loop system, Section V contains mathematical results relating to forward invariance, and Section VI discusses how to prevent chattering between the certified and uncertified controllers. Due to space constraints, proofs are abbreviated or omitted.
II. PRELIMINARIES

For notation, we use $\mathbb{N} := \{0, 1, 2, \ldots\}$, $\mathbb{R}_{\geq 0} := [0, \infty)$, and $\mathbb{R}_{\leq 0} := (-\infty, 0]$. The Euclidean norm of $v \in \mathbb{R}^n$ is written $|v|$. We write the inner product between $v_1$ and $v_2$ in $\mathbb{R}^n$ as $\langle v_1, v_2 \rangle$. The concatenation of vectors $v_1 \in \mathbb{R}^{n_1}$ and $v_2 \in \mathbb{R}^{n_2}$ is denoted $(v_1, v_2) := [v_1^T, v_2^T]^T \in \mathbb{R}^{n_1+n_2}$. “Continuously differentiable” is abbreviated as $C^1$. For a $C^1$ function $f : \mathbb{R}^n \to \mathbb{R}$, the gradient of $f$ is written $\nabla f$. Given a set $S \subset \mathbb{R}^n$, we write the boundary of $S$ as $\partial S$, the interior as $\text{int}(S) := S \setminus \partial S$ and the closure as $\overline{S} := S \cup \partial S$. A neighborhood of $S$ is any open set $U$ such that $S \subset U$.

A. Hybrid Systems

We consider hybrid systems on $\mathbb{R}^n$ written as

$$\mathcal{H} := \begin{cases} \dot{x} = f(x) & x \in C \\ x^+ = g(x) & x \in D \end{cases}$$  \hspace{1cm} (1)

with state $x \in \mathbb{R}^n$, flow map $f : C \to \mathbb{R}^n$, jump map $g : D \to \mathbb{R}^n$, flow set $C \subset \mathbb{R}^n$, and jump set $D \subset \mathbb{R}^n$. The system $\mathcal{H}$ can be written compactly as $\mathcal{H} = (C, f, D, g)$.

A solution $\phi : E \to \mathbb{R}^n$ to $\mathcal{H}$ is defined on a hybrid time domain $\text{dom} \phi := E \subset \mathbb{R}_{\geq 0} \times \mathbb{N}$, which parameterizes the solution by ordinary time $t \in \mathbb{R}_{\geq 0}$ and discrete time $j \in \mathbb{N}$. More precisely, a hybrid time domain is a subset $E \subset \mathbb{R}_{\geq 0} \times \mathbb{N}$ such that, for every $(T, J) \in E$, there exists a sequence $t_0 = t_1 \leq t_2 \leq \cdots \leq t_{J+1} = T$ such that

$$E \cap ([0, T] \times \{0, 1, \ldots, J\}) = (\{t_0, t_1\} \times \{0\}) \cup ([t_1, t_2] \times \{1\}) \cup \cdots \cup ([t_{J}, t_{J+1}] \times \{J\}).$$

For each $j \in \{1, 2, \ldots, J\}$, the time $t_j$ (defined above) is called a jump time in $\text{dom} \phi$. At each jump time $t_j$ in $\text{dom} \phi$, the solution $\phi$ must satisfy $\phi(t_j, j) \in D$ and

$$\phi(t_j, j+1) = g(\phi(t_j, j)).$$

If $t_{j-1} < t_j$, then $[t_{j-1}, t_j]$ is called an interval of flow and $\phi$ must satisfy $\phi(t, j) \in C$ for all $t \in (t_{j-1}, t_j)$ and

$$\frac{d\phi}{dt}(t, j) = f(\phi(t, j))$$

for almost all $t \in [t_{j-1}, t_j]$. We write $\text{sup}_t \text{dom} \phi := \sup \{t \in \mathbb{R}_{\geq 0} \mid (t, j) \in \text{dom} \phi\}$ and $\text{sup}_j \text{dom} \phi := \sup \{j \in \mathbb{N} \mid (t, j) \in \text{dom} \phi\}$. A solution $\phi$ to $\mathcal{H}$ is said to be complete if the domain of $\phi$ is unbounded (namely, $\text{sup}_t \text{dom} \phi = \infty$, $\text{sup}_j \text{dom} \phi = \infty$, or both) and $\phi$ is said to be maximal if there does not exist a solution $\psi$ to $\mathcal{H}$ such that $\phi$ is a truncation of $\psi$ with $\text{dom} \phi$ a strict subset of $\text{dom} \psi$. For more on hybrid systems, see [11], [12].

Definition 1. A set $K \subset \mathbb{R}^n$ is forward pre-invariant for a hybrid system $\mathcal{H}$ if, for each $x_0 \in K$ and each maximal solution $\phi$ starting from $\phi(0, 0) = x_0$, then $\phi(t, j) \in K$ for all $(t, j) \in \text{dom} \phi$. If, additionally, each maximal solution starting in $K$ is complete, then $K$ is forward invariant. ■

Definition 2 (Barrier Function). Consider a hybrid system $\mathcal{H} = (C, f, D, g)$ in $\mathbb{R}^n$ and a set $K \subset \mathbb{R}^n$. A $C^1$ function $B : \mathbb{R}^n \to \mathbb{R}$ is a barrier function of $K$ for $\mathcal{H}$ if:

(B1) $K = \{ z \in \mathbb{R}^n \mid B(z) \leq 0 \}$.

(B2) There exists a neighborhood $U$ of $K$ such that

$$\langle \nabla B(x), f(x) \rangle \leq 0 \quad \forall x \in (U \setminus K) \cap C.$$

(B3) For all $x \in K \cap D$,

$$g(x) \in C \cup D \quad \text{and} \quad B(g(x)) \leq 0.$$  \hspace{1cm} ■

For a continuous-time system $z = f(z)$ in $\mathbb{R}^n$, a $C^1$ barrier function $B$ of $K$ is defined as in Definition 2 except without (B3) and with (B2) replaced by the following:

(B2’) There exists a neighborhood $U$ of $K$ such that

$$\langle \nabla B(x), f(x) \rangle \leq 0 \quad \forall x \in U \setminus K.$$  \hspace{1cm} ■

The following corollary uses the existence of a barrier function to establish forward pre-invariance of $K$.

Corollary 1 (Corollary of [3, Theorem 1]). Consider a hybrid system $\mathcal{H} = (C, f, D, g)$ in $\mathbb{R}^n$ with $f$ continuous on $C$. Let $K \subset \mathbb{R}^n$ be closed. If there exists a $C^1$ barrier function $B$ of $K$ for $\mathcal{H}$, then $K$ is forward pre-invariant for $\mathcal{H}$.

Remark 1. The original result in [3] is much more general. It allows for $f$ and $g$ to be set-valued maps, for multiple barrier functions, and it relaxes (B2) by only requiring $\langle \nabla B(x), f(x) \rangle \leq 0$ at each point $x \in (U \setminus K) \cap C$ from which the system can flow while remaining in $C$.

III. PROBLEM SETTING

Consider a continuous-time plant

$$\dot{z} = f_0(z, u)$$  \hspace{1cm} (2)

with state $z \in \mathbb{R}^n$, input $u \in \mathbb{R}^m$, and $f_0 : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$. Suppose we are given a closed set $K \subset \mathbb{R}^n$ to be rendered forward-invariant, and two controllers $\kappa_0, \kappa_1 : \mathbb{R}^n \to \mathbb{R}^n$ such that the vector fields $z \mapsto f_0(z, \kappa_0(z))$ and $z \mapsto f_0(z, \kappa_1(z))$ are continuous. In conjunction with $\kappa_0$, we are also given a $C^1$ barrier function $B : \mathbb{R}^n \to \mathbb{R}$ of $K$ for the closed-loop

$$\dot{z} = f_0(z) := f_0(z, \kappa_0(z)).$$  \hspace{1cm} (3)

The controller $\kappa_1$ is not assumed to render $K$ forward invariant for the closed-loop

$$\dot{z} = f_1(z) := f_0(z, \kappa_1(z)).$$  \hspace{1cm} (4)

Since $B$ guarantees that $K$ is forward invariant for (3), we call $\kappa_0$ a certified controller, whereas $\kappa_1$, which has no such guarantee, is called uncertified.

Given the $C^1$ barrier function $B$ of $K$ for (3), we define

$$\dot{B}_q(z) := \langle \nabla B(z), f_0(z, \kappa_q(z)) \rangle \quad \forall (z, q) \in \mathcal{X},$$  \hspace{1cm} (5)

which is the (hypothetical) rate of change of $t \mapsto B(z(t))$ if $t \mapsto z(t)$ were to evolve according to $\dot{z} = f_0(z)$.

The decision unit that determines when to switch between $\kappa_0$ and $\kappa_1$ is called a supervisor. As shown in Figure 1, an auxiliary logic variable $q \in \{0, 1\}$ is used to select which controller is used. When $q = 0$, the certified controller $\kappa_0$ is used and when $q = 1$, the uncertified controller $\kappa_1$ is used. The supervisor’s switching logic is defined by two switching sets: $Z_{0\to 1}, Z_{1\to 0} \subset \mathbb{R}^n$. The set $Z_{0\to 1}$ specifies where the
supervisor switches from \( q = 0 \) to \( q = 1 \) and the set \( Z_{1 \rightarrow 0} \) specifies where the supervisor switches from \( q = 1 \) to \( q = 0 \). As complements of the switching sets, we define \textit{hold sets} 
\[
Z_0 := \mathbb{R}^n \setminus Z_{0 \rightarrow 1} \quad \text{and} \quad Z_1 := \mathbb{R}^n \setminus Z_{1 \rightarrow 0}
\]
(6) 
that specify where the supervisor holds constant \( q = 0 \) and \( q = 1 \), respectively. In Section IV, we design \( Z_{0 \rightarrow 1} \) and \( Z_{1 \rightarrow 0} \) such that the hybrid closed–loop system with the switched feedback \( u := \kappa_q(z) \) satisfies the following properties:

- The set \( K \) is forward invariant.
- The uncertified controller \( \kappa_1 \) is preferred over the certified controller \( \kappa_0 \).
- The switching between \( \kappa_0 \) and \( \kappa_1 \) does not change.

### IV. HYBRID CLOSED–LOOP SYSTEM

We model the closed–loop system with a supervisor for switching between controllers \( \kappa_0 \) and \( \kappa_1 \) as a hybrid system \( \mathcal{H}_{CL} \) with state \( x := (z, q) \) in state space \( \mathcal{X} := \mathbb{R}^n \times \{0, 1\} \), and dynamics given by

\[
\begin{align*}
\dot{z} &= f(z, q) := \begin{bmatrix} f_q(z) \\ 0 \end{bmatrix}, \quad (z, q) \in C := C_0 \cup C_1 \\
\dot{q} &= g(z, q) := \begin{bmatrix} z \\ 1 - q \end{bmatrix}, \quad (z, q) \in D := D_0 \cup D_1
\end{align*}
\]

where
\[
C_0 := Z_0 \times \{0\}, \quad C_1 := Z_1 \times \{1\}, \\
D_0 := Z_{0 \rightarrow 1} \times \{0\}, \quad D_1 := Z_{1 \rightarrow 0} \times \{1\}.
\]

To design \( Z_{0 \rightarrow 1} \) and \( Z_{1 \rightarrow 0} \), we introduce four \textit{threshold functions} \( \delta_0, \delta_1, \theta_0, \theta_1 : \mathbb{R}^n \to \mathbb{R} \geq 0 \) such that
\[
\delta_0(z) < \delta_1(z) \leq 0 \quad \text{and} \quad \theta_0(z) < \theta_1(z) \leq 0 \quad \forall z \in \mathbb{R}^n. \quad (8)
\]

We use the functions \( \delta_0 \) and \( \delta_1 \) as thresholds on \( B \) and the functions \( \theta_0 \) and \( \theta_1 \) as thresholds on \( B_1 \) to determine where switches occur. Thus, we define the switching sets as
\[
\begin{align*}
Z_{0 \rightarrow 1} := \{ z \in \mathbb{R}^n \mid B(z) \leq \delta_0(z) \text{ or } B_1(z) \leq \theta_0(z) \} \\
Z_{1 \rightarrow 0} := \{ z \in \mathbb{R}^n \mid B(z) \geq \delta_1(z), \ B_1(z) \geq \theta_1(z) \}.
\end{align*}
\]

(9) 

The switching sets \( Z_{0 \rightarrow 1} \) and \( Z_{1 \rightarrow 0} \) are shown in Figure 2. Expanding the definitions in (6) of \( Z_0 \) and \( Z_1 \) produces
\[
\begin{align*}
Z_0 &= \{ z \in \mathbb{R}^n \mid B(z) \geq \delta_0(z), \ B_1(z) \geq \theta_0(z) \} \\
Z_1 &= \{ z \in \mathbb{R}^n \mid B(z) \leq \delta_1(z), \ B_1(z) \leq \theta_1(z) \}.
\end{align*}
\]

(10) 

We have \( C \cup D = \mathcal{X} \) because \( Z_0 \cup Z_{0 \rightarrow 1} = Z_1 \cup Z_{1 \rightarrow 0} = \mathbb{R}^n \).

The set \( Z_0 \) is designed such that the supervisor continues to use the certified controller \( \kappa_0 \) so long as the state is close to the boundary of \( K \) (namely, \( B(z) \geq \delta_0(z) \)) and the hypothetical rate of change of \( B \) under \( \kappa_1 \) is too large (\( B_1(z) \geq \theta_0(z) \)). As the complement, \( Z_{0 \rightarrow 1} \) is designed such that the supervisor switches to the uncertified controller \( \kappa_1 \) when the state is either far from \( \partial K \) (i.e., \( B(z) \leq \delta_0(z) \)) or the hypothetical rate that \( B \) would decrease under \( \kappa_1 \) is fast enough (\( B_1(z) \leq \theta_0(z) \)).

For \( q = 1 \), the set \( Z_1 \) is designed such that the supervisor continues to use the uncertified controller \( \kappa_1 \) at each state \( z \in K \) that is far from \( \partial K \) or where the rate that \( B \) would decrease under \( \kappa_1 \) is fast enough. The set \( Z_{1 \rightarrow 0} \) is the closed complement of \( Z_1 \) and is designed to trigger a switch to the certified controller \( \kappa_0 \) whenever the state is too close to \( K \) and is moving toward \( K \) (or, more precisely, not moving away fast enough).

**Example 1.** To illustrate the design of \( \mathcal{H}_{CL} \), consider the double integrator plant

\[
\dot{z} = f(z, u) := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} z + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u. \tag{11}
\]

Suppose we want the system to avoid a disk with radius 1, centered on the \( z_1 \)-axis at \( c := (5, 0) \in \mathbb{R}^2 \). The admissible set, which we want to render forward invariant, is

\[
K := \{ z \in \mathbb{R}^2 \mid |z - c| \geq 1 \}.
\]

Let \( \kappa_0(z) := [-1 \ 1](z - c) \) and \( B(z) := \frac{1}{2}(1 - |z - c|^2) \). Because \( B_0(z) = -z_2^2 \leq 0 \), the set \( K \) is certified to be forward invariant for \( \dot{z} = f_0(z) \).

For the uncertified controller, let \( \kappa_1(z) := [-1 \ -2]z \), which renders the origin of system (11) globally exponentially stable, but violates constraints. The set \( K \) is not forward invariant for \( \dot{z} = f_1(z) \) because \( B_1 \) is positive at \((5, 1) \in \partial K \).

We select constant threshold functions, which we write (with abuse of notation) as \( \theta_0 := -1, \theta_1 := -0.1, \delta_0 := -1, \) and \( \delta_1 := -0.1 \). Figure 3 shows a solution to \( \mathcal{H}_{CL} \) and the corresponding switching criteria are shown in Figure 4. \(^1\) These plots show that the system is controlled by the uncertified controller \( \kappa_1 \) until it becomes too close to the obstacle and switches to the certified controller \( \kappa_0 \). The closed–loop system \( \mathcal{H}_{CL} \) satisfies the assumptions of Theorem 2 given in Section V, so the set \( K \) is forward invariant for \( \mathcal{H}_{CL} \).

**Example 2.** Consider the system given in Example 1 with the uncertified controller \( \kappa_1 \) replaced by an MPC controller. If each periodic MPC computation finishes immediately, then the trajectory grazes the boundary of the unsafe set but does not enter it. MPC computations can be slow, however, in the

\(^1\)Simulations are computed in MATLAB with the HyEQ Toolbox [13].
presence of nonlinear or non-convex constraints. In Figure 5, we see that adding small, random delays to the update times for the MPC input causes the solution to violate the constraint.

Using our supervisory control strategy, \( H_{\text{cl}} \) respects the constraint by switching to the certified controller, as shown in Figure 6.

V. FORWARD INVARIANCE OF \( K \)

Our first result, Theorem 1, states that \( K \) is forward pre-invariant for \( H_{\text{cl}} \), meaning that each solution to \( H_{\text{cl}} \) remains in \( K \) for as long as the solution exists. Under stronger assumptions, Theorem 2 asserts that \( K \) is forward invariant by establishing that every maximal solution \( \phi \) is complete (sup \( \text{dom} \, \phi = \infty \) or sup \( \text{dom} \, \phi = \infty \) or both) and, if \( \phi \) is bounded, then sup \( \text{dom} \, \phi = \infty \).

**Theorem 1** (Forward Pre-Invariance). Suppose \( B \) is a \( C^1 \) barrier function of \( K \) for \( z = f_0(z) \); the vector fields \( f_0 \) and \( f_1 \) are continuous; and the threshold functions \( \delta_0, \delta_1, \theta_0, \) and \( \theta_1 \) satisfy the inequalities in \((8)\). Then, \( K' := K \times \{0, 1\} \) is forward pre-invariant for \( H_{\text{cl}} \) in \((7)\).

**Proof Sketch.** Let \( B'(z, q) := B(z) \) for all \((z, q) \in X\). The proof proceeds by first showing that \( B' \) is a barrier function of \( K' \) for \( H_{\text{cl}} \), and is completed by applying Corollary 1.

The only point of difficulty is showing that \( B' \) satisfies (B2). Because \( B \) is a barrier function of \( K \) for \( z = f_0(z) \), we can take from (B2) a neighborhood \( U \) of \( K \) where \( B_0(z) \leq 0 \). The set \( U' := U \times \{0, 1\} \) is a neighborhood of \( K' \) relative to \( X \), so we want to show \( \langle \nabla B'(z, q), f(z, q) \rangle \leq 0 \) for all \((z, q) \in (U' \setminus K') \cap C\). Every element \((z, q)\) of \((U' \setminus K') \cap C\) satisfies one of two disjoint cases:

- If \( q = 0 \) and \( z \in (U \setminus K) \cap Z_0 \), then, by (B2),
  \[ \langle \nabla B'(z, 0), f_0(z) \rangle = B_0(z) \leq 0. \]

- If \( q = 1 \) and \( z \in (U \setminus K) \cap Z_1 \), then by the design of \( Z_1 \), either \( B(z) \leq \delta_1(z) \leq 0 \) or \( B_1(z) \leq \theta_1(z) \leq 0 \). Because \( z \not\in K \), we must have \( B(z) \geq \delta_1(z) \). Thus, every \( z \) in \((U \setminus K) \cap Z_1 \) satisfies \( B_1(z) \leq \theta_1(z) \), so
  \[ \langle \nabla B'(z, 1), f_1(z) \rangle = B_1(z) \leq \theta_1(z) \leq 0. \]

Therefore, (B2) is satisfied.

In the following result, we assert (under appropriate assumptions) that each bounded solution to the closed-loop system \( H_{\text{cl}} \) does not exhibit arbitrarily short intervals of time between jumps. This result, combined with a proof that all maximal solutions are complete (in Theorem 2, below), allows us to conclude that maximal solutions exist for all time \( t \geq 0 \).

**Lemma 1.** Suppose \( B : \mathbb{R}^n \to \mathbb{R} \) is \( C^1 \); the vector fields \( f_0 \) and \( f_1 \) are continuous; and the threshold functions \( \delta_0, \delta_1, \theta_0, \) and \( \theta_1 \) are continuous and satisfy the inequalities in \((8)\). For each solution \( \phi \) to \( H_{\text{cl}} \) in \((7)\), if \( \phi \) is bounded, then there exists \( \gamma > 0 \) such that \( t_{j+1} - t_j \geq \gamma \) for every pair of jump times \( t_j \) and \( t_{j+1} \) in \( \text{dom} \, \phi \).

**Proof Sketch.** To establish a positive lower bound on the time between jumps, we show that \( D \) and \( g(D) \) are disjoint, and apply \([12, \text{Proposition 2.34}]\)—using the fact that \( f \) and \( g \) are continuous and \( C \) and \( D \) are closed. The sets \( Z_{0 \rightarrow 1} \) and \( Z_{0 \rightarrow 1} \) are disjoint because for every \( z \in Z_{0 \rightarrow 1} \), we have that \( B(z) \geq \delta_1(z) \geq 0 \) and \( B_1(z) \geq \theta_1(z) > 0 \), so \( z \not\in Z_{0 \rightarrow 1} \). Thus, since the function \( g \) maps \( z \) to \( q \) and \( z \) to \( 1 - q \), the sets \( D := (Z_{0 \rightarrow 1} \times \{0\}) \cup (Z_{1 \rightarrow 0} \times \{1\}) \) and \( g(D) := (Z_{0 \rightarrow 1} \times \{1\}) \cup (Z_{1 \rightarrow 0} \times \{0\}) \) are also disjoint.

To ensure solutions to \( H_{\text{cl}} \) exist for all \( t \geq 0 \), we require that all solutions to \( \tilde{z} = f_0(z) \) and \( \tilde{z} = f_1(z) \) do not exhibit “finite escape times.” We say that \( z : [0, T) \to \mathbb{R}^n \) with \( t_0 < T \) has a finite escape time \( T \) if \( \lim_{t \uparrow T} |z(t)| = \infty \).

**Theorem 2** (Forward Invariance). Suppose \( B \) is a \( C^1 \) barrier function of \( K \) for \( z = f_0(z) \); the vector fields \( f_0 \) and \( f_1 \) are continuous; the threshold functions \( \delta_0, \delta_1, \theta_0, \) and \( \theta_1 \) are continuous and satisfy the inequalities in \((8)\); and for each \( q \in \{0, 1\} \), no solution to
\[ \dot{z} = f_q(z) \quad z \in Z_q \]
has a finite escape time. Then, \( K' := K \times \{0, 1\} \) is forward invariant for \( H_{\text{cl}} \) and every maximal solution \( \phi \) to \( H_{\text{cl}} \) is complete. Furthermore, if \( \phi \) is bounded, then sup \( \text{dom} \, \phi = \infty \).
Remark. Therefore, for all solutions to $H$ established a uniform lower bound on the time between jumps may converge to zero, as shown in Example 3, below. To rate of the processor used to run the supervisor. Furthermore, the solution, rather than being a uniform lower bound that applies in Example 2. Computational delays cause the constraint to be violated.

Proof Sketch. By Theorem 1, the set $K'$ is forward pre-invariant for $H_{\text{CL}}$. With the given assumptions, [12, Proposition 2.34] can be used to show that every maximal solution is complete. In particular, $\partial C$ is a subset of $D$ and solutions to $\dot{x} = f(x)$ can flow from every $x \in \text{int} C$. Combined with the fact that $C \cup D = X$, we have that solutions can flow or jump at every point in the state space. By assumption, solutions to $\dot{x} = f(x)$ cannot have a finite escape time with $x \in C$, so all maximal solutions are complete. Since every maximal solution $\phi$ to $H_{\text{CL}}$ is complete, we have that $\sup_\tau \text{dom} \phi = \infty$ or $\sup_\tau \text{dom} \phi = \infty$. By Lemma 1, if $\phi$ is bounded, then there exists $\gamma > 0$ such that every interval of flow has a length of at least $\gamma$, so $\sup_\tau \text{dom} \phi = \infty$ implies $\sup_\tau \text{dom} \phi = \infty$. Therefore, $\sup_\tau \text{dom} \phi = \infty$ for every bounded maximal solution $\phi$ to $H_{\text{CL}}$.

The “no finite escape time” assumption in Theorem 2 is satisfied if, for each $q \in \{0, 1\}$, the vector field $f_q$ is globally Lipschitz continuous or the set $Z_q$ is bounded.

Remark 2. Under the assumptions of Theorem 2, $H_{\text{CL}}$ is well-posed because it satisfies the hybrid basic conditions in [11, Assumption 6.5]. Solutions to a well-posed hybrid system (having a sense) continuous dependence on initial conditions, although the sense of continuity is weaker (upper semi-continuous instead of continuous) than it is for well-posed continuous-time systems [11, Chapter 6].

VI. UNBOUNDED SOLUTIONS WITHOUT CHATTERING

There are several practical difficulties with Lemma 1 and Theorem 2 that we address in this section. Notably, the lower bound $\gamma > 0$ in Lemma 1 depends on the choice of solution, rather than being a uniform lower bound that applies to all solutions. This can cause problems if—as an extreme example—$\gamma$ for a particular solution is shorter than the clock rate of the processor used to run the supervisor. Furthermore, if a solution is unbounded, then the time between switches may converge to zero, as shown in Example 3, below. To address these problems, Theorem 3 provides conditions for establishing a uniform lower bound on the time between jumps for all solutions to $H_{\text{CL}}$ (including unbounded solutions).

Example 3. One can construct $H_{\text{CL}}$ with $z \in \mathbb{R}^2$ and with

$$f_0(z) = (z_1, -1), \quad Z_{0 \to 1} := \{(z_1, z_2) \mid z_2 \leq 0\},$$

$$f_1(z) = (z_1, 1), \quad Z_{1 \to 0} := \{(z_1, z_2) \mid z_2 \geq \exp(-z_1^2)\},$$

such that $H_{\text{CL}}$ satisfies the assumptions of Theorem 2. Consider a maximal and complete solution $\phi$ that starts in the right-half plane. The $z_1$-component of $\phi$ grows exponentially, approaching $+\infty$ as $t + j \to \infty$, so $\phi$ is unbounded. Meanwhile, the $z_2$-component of $\phi$ bounces between $Z_{0 \to 1}$ and $Z_{1 \to 0}$ as the distance between them approaches zero—causing the time between switches to also approach zero. ■

To rule out arbitrarily fast switching, the following result asserts a minimum time between all switches and thereby establishes that maximal solutions to $H_{\text{CL}}$ exist for all $t \geq 0$.

Theorem 3. Suppose that $B$ is a $C^1$ barrier function of $K$ for $\dot{z} = f_0(z)$; the vector fields $f_0$ and $f_1$ are globally Lipschitz continuous with Lipschitz constants $L_0$ and $L_1$; the threshold functions $\delta_0, \delta_1, \theta_0$, and $\theta_1$ are continuous and satisfy the inequalities in (8); and there exists $\tau > 0$ such that for all $z^0 \in Z_{0 \to 1}$ and $z^1 \in Z_{1 \to 0}$, the following hold:

$$|z^0 - z^1| \geq \tau |f_0(z^0)| \exp(L_0 \tau),$$

$$|z^0 - z^1| \geq \tau |f_1(z^1)| \exp(L_1 \tau).$$

Then, for every solution $\phi$ to $H_{\text{CL}}$ in (7), and each pair of jump times $t_j$ and $t_{j+1}$ in $\text{dom} \phi$, we have that $t_{j+1} - t_j \geq \tau$. Furthermore, if $\phi$ is a maximal solution, then $\sup_\tau \text{dom} \phi = \infty$.

Example 4. Consider the plant

$$\dot{z} = f_\varepsilon(z, u) := \begin{bmatrix} z_1 \\ u \end{bmatrix}, \quad z = (z_1, z_2) \in \mathbb{R}^2, \quad u \in \mathbb{R}$$

with admissible set $K := \{z \in \mathbb{R}^2 \mid z_2 \leq 0\}$, certified controller $\kappa_0(z) := -|z_1|$, barrier function $B(z) := z_2$, uncertified controller $\kappa_1(z) := |z_1|$, and threshold functions $\delta_0(z) := -2 - 2|z_1|$ and $\delta_1(z) := -1 - |z_1|$. The threshold functions $\theta_0$ and $\theta_1$ have no effect because $B_1(z) = |z_1| \geq 0$. Thus, the switching sets are

$$Z_{0 \to 1} = \{(z_1, z_2) \in \mathbb{R}^n \mid z_2 \leq -2 - 2|z_1|\},$$

$$Z_{1 \to 0} = \{(z_1, z_2) \in \mathbb{R}^n \mid z_2 \geq -1 - |z_1|\}.$$

By Theorem 2, $K$ is forward invariant for $H_{\text{CL}}$. We can apply Theorem 3 to show that solutions exist for all $t \geq 0$ and the time between every pair of jumps is longer than $\tau := 0.25$. The vector fields $f_0$ and $f_1$ are globally Lipschitz continuous with Lipschitz constants $L_0 = L_1 = 1$. Take any points $z^0 := (z^0_1, z^0_2) \in Z_{0 \to 1}$ and $z^1 := (z^1_1, z^1_2) \in Z_{1 \to 0}$. Using the geometry of $Z_{0 \to 1}$ and $Z_{1 \to 0}$, and the fact that
Therefore, (12) and (13) are satisfied, so Theorem 3 asserts controllers, such as neural networks and MPC, to be safely uncertified controller. Our approach allows for advanced guarantees forward invariance while preferentially using the uncertified controller. That start in farther than the system can travel in time are chosen such that the distance from $\kappa$ invariance for $T$ sample time the supervisor. If the supervisor only checks the switching $\kappa$ invariant for $T$.

To broaden the applicability of our results, future work includes relaxing the assumption in Theorem 2 that $f_1$ is continuous so that our results can be applied with an arbitrary uncertified controller $\kappa_1$. In a similar vein, future work may include considering hybrid plants affected by disturbances, as in [2], and allowing for more general forward invariant sets by using multiple barrier functions, as in [3]. Improved methods for designing the threshold functions to limit the rate of switching and to safely handle discrete sampling in the supervisor are also of interest.

Fig. 7: A solution $\phi$ to $\mathcal{H}_{ci}$ in Example 4.

$\tau \exp(L_0 \tau) = \tau \exp(L_1 \tau) = 0.25 \exp(0.25) < \frac{1}{2}$, we find

$$|z^0 - z^1| \geq \frac{|z_1| + 1}{\sqrt{5}} > \frac{1}{3} |z_1| > \tau |f_0(z)| \exp(L_0 \tau),$$

$$|z^0 - z^1| \geq \frac{|z_1| + 1}{\sqrt{2}} > \frac{1}{3} |z_1| > \tau |f_1(z^1)| \exp(L_1 \tau).$$

Therefore, (12) and (13) are satisfied, so Theorem 3 asserts that every solution to $\mathcal{H}_{ci}$ exists for all time $t \geq 0$. A solution to $\mathcal{H}_{ci}$ is shown in Figure 7 and the corresponding switching criteria are shown in Figure 8.

Fig. 8: Switching criteria for $\phi$ in Figure 7 from Example 4.

It is important to note the effects of discrete sampling in the supervisor. If the supervisor only checks the switching conditions periodically (instead of continuously) with some sample time $T_s > 0$, then the set $K$ is not, in general, forward invariant for $\mathcal{H}_{ci}$. In particular, for Example 4, solutions that start with $\phi(0,0)$ in $\partial K \times \{1\}$ will leave $K$ due to the supervisor applying $\kappa_1$ over the interval $[0,T_s]$, before the first update. If, however, the threshold functions $\delta_0$ and $\theta_0$ are chosen such that the distance from $\mathcal{Z}_{0\to1}$ to $\mathbb{R}^n \setminus K$ is farther than the system can travel in time $T_s$, then solutions that start in $\mathcal{Z}_{0\to1}$ will never leave $K$.

VII. CONCLUSION

We designed a supervisory hybrid control algorithm that switches between a given barrier-certified controller that renders a desired set forward invariant and an uncertified controller that may not. The resulting hybrid control strategy guarantees forward invariance while preferentially using the uncertified controller. Our approach allows for advanced controllers, such as neural networks and MPC, to be safely used while avoiding the difficult task of constructing barrier functions for them.

REFERENCE


