Forward Invariance-Based Hybrid Control Using Uncertified Controllers

Paul K. Wintz Ricardo G. Sanfelice

Hybrid Systems Laboratory
University of California, Santa Cruz

December 15, 2023

Introduction – Switched Controllers

Sometimes, a single continuous controller cannot satisfy design requirements.

Switching has been used to...

- Achieve robust global asymptotic stability around obstructions.[1,2]
- Achieve global asymptotic stability by uniting multiple Lyapunov-certified controllers (such as local and global controllers)[3,4,5] or by uniting a Lyapunov-certified controller and an uncertified controller.[6]

[1] Mayhew, Sanfelice, and Teel, "Quaternion-based hybrid control for robust global attitude tracking,", 2011.

[2] Sanfelice, Messina, Tuna, *et al.*, "Robust hybrid controllers for continuous-time systems with applications to obstacle avoidance and regulation to disconnected set of points,", 2006.

[3] Prieur, "Uniting local and global controllers with robustness to vanishing noise,", 2001.

[4] Teel and Kapoor, "Uniting local and global controllers,", 1997.

[5] El-Farra, Mhaskar, and Christofides, "Output feedback control of switched nonlinear systems using multiple Lyapunov functions,", 2005.

[6] Wintz, Sanfelice, and Hespanha, "Global asymptotic stability of nonlinear systems while exploiting properties of uncertified feedback controllers via opportunistic switching,", Atlanta, GA, 2022.

Introduction – Switched Controllers

The *Simplex architecture* is an approach for switching between an "advanced," unverified controller and a "simple," easy-to-verify controller.[7][8]

Barrier functions have been used with the Simplex architecture to guarantee safety for hybrid systems while using an unverified controller.

Existing approaches have drawbacks:

- Requires costly reachability analysis and only defines "one way" switching.[9]
- Only rectangular constraints are considered, and the switching criteria depends on the extremal values of the vector field over the entire admissible set.[10]

[7] Rivera, Danylyszyn, Weinstock, *et al.*, "An architectural description of the Simplex Architecture," Defense Technical Information Center, Fort Belvoir, VA, Tech. Rep., 1996.

[8] Seto, Krogh, Sha, *et al.*, "The Simplex architecture for safe online control system upgrades,", Philadelphia, PA, USA, 1998.

[9] Yang, Islam, Murthy, *et al.*, "A Simplex architecture for hybrid systems using barrier certificates,", Tonetta, Schoitsch, and Bitsch, Eds., ser. Lecture Notes in Computer Science, 2017.

[10] Damare, Roy, Smolka, *et al.*, "A barrier certificate-based Simplex architecture with application to microgrids,", Dang and Stolz, Eds., ser. Lecture Notes in Computer Science, 2022.

Why Use an Uncertified Controller?

An uncertified controller may have "better" properties compared to available certified controllers:

- More energy efficient
- Convergence to a reference
- Less computation

Examples:

- Model predictive control (MPC) that occasionally fails to compute an update due to computational delays.
- Black box controllers (e.g., neural network controllers).

Supervisory Control for Forward Invariance

Consider a nonlinear plant

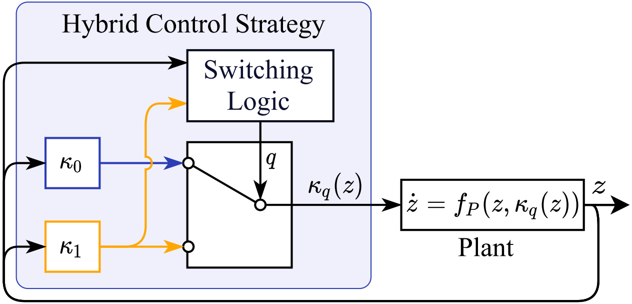
$$\dot{z} = f_{\mathrm{P}}(z, u), \quad z \in \mathbb{R}^n, \; u \in \mathbb{R}^m.$$

Goal: Render $K \subset \mathbb{R}^n$ forward invariant.

Given two continuous controllers:

κ_0: a barrier-certified controller

κ_1: any continuous controller



Design switching logic for $q \in \{0, 1\}$ such that

- K is forward invariant.
- κ_1 is preferred over κ_0.
- The switching does not chatter.

Barrier Function Certificate

Assume a continuously differentiable *barrier function* $B : \mathbb{R}^n \to \mathbb{R}$ that certifies a set $K \subset \mathbb{R}^n$ is forward invariant for the closed–loop system with the certified controller

$$\dot{z} = f_0(z) := f_{\mathrm{P}}(z, \kappa_0(z)).$$

In particular

- $K = \{z \in \mathbb{R}^n \mid B(z) \leq 0\}$.
- There exists a neighborhood U of K such that

$$\dot{B}_0(z) := \langle \nabla B(z),\ f_0(z) \rangle \leq 0 \quad \forall z \in U \setminus K.$$

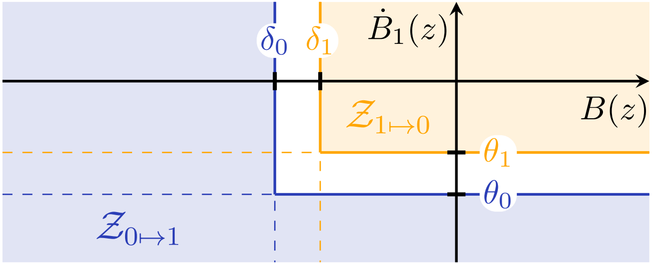
We also define corresponding quantities for the uncertified controller:

$$f_1(z) := f_{\mathrm{P}}(z, \kappa_1(z)) \quad \text{and} \quad \dot{B}_1(z) := \langle \nabla B(z),\ f_1(z) \rangle.$$

Switching Criteria and Hold Criteria

Pick four *threshold functions* $\delta_0,\ \delta_1,\ \theta_0,\ \theta_1 : \mathbb{R}^n \to \mathbb{R}$, such that

$$\delta_0(z) < \delta_1(z) \le 0 \quad \text{and} \quad \theta_0(z) < \theta_1(z) \le 0 \quad \forall z \in \mathbb{R}^n.$$



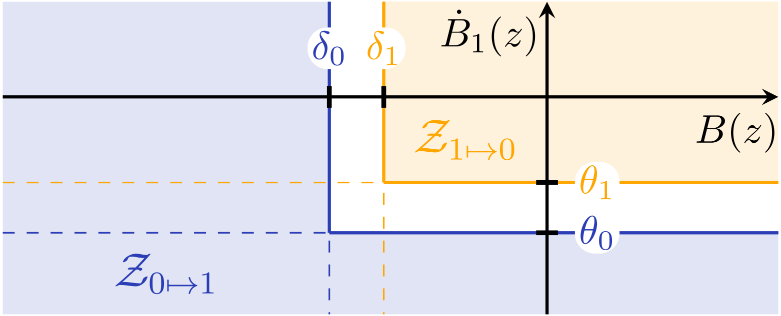
For $q = 1$ (uncertified controller):

- Hold $q = 1$ if $z \in \mathcal{Z}_1$.
- Switch to $q = 0$ if $z \in \mathcal{Z}_{1\mapsto 0}$.

For $q = 0$ (certified controller):

- Hold $q = 0$ if $z \in \mathcal{Z}_0$.
- Switch to $q = 1$ if $z \in \mathcal{Z}_{0\mapsto 1}$.

Switching Criteria and Hold Criteria



$$\mathcal{Z}_{1\mapsto 0} := \{z \in \mathbb{R}^n \mid B(z) \geq \delta_1(z),\ \dot{B}_1(z) \geq \theta_1(z)\}$$

$$\mathcal{Z}_{0\mapsto 1} := \{z \in \mathbb{R}^n \mid B(z) \leq \delta_0(z) \text{ or } \dot{B}_1(z) \leq \theta_0(z)\}.$$

Example: Linear and Affine Feedbacks

Consider the double integrator

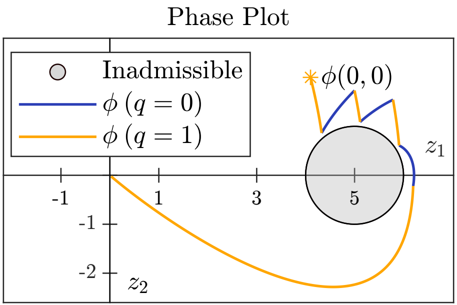
$$\dot{z} = f_{\mathrm{P}}(z,u) := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} z + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u.$$

Admissible set:

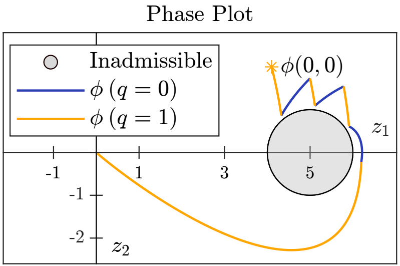
$$K := \left\{ z \in \mathbb{R}^2 \;\middle|\; |z - (5,0)| \geq 1 \right\}.$$

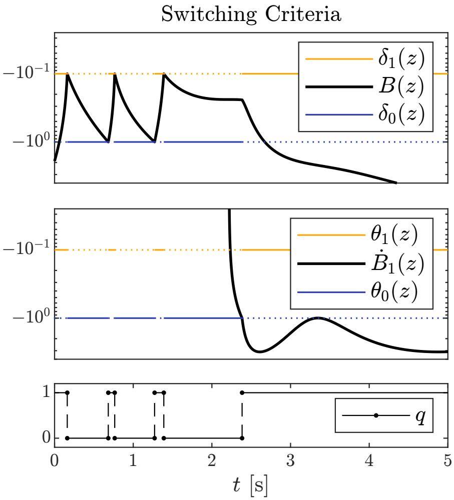
Controllers:

$$\kappa_0(z) = \begin{bmatrix} -1 & 1 \end{bmatrix} (z - c) \qquad \text{(certified)}$$
$$\kappa_1(z) = \begin{bmatrix} -1 & -2 \end{bmatrix} z \qquad \text{(uncertified)}$$

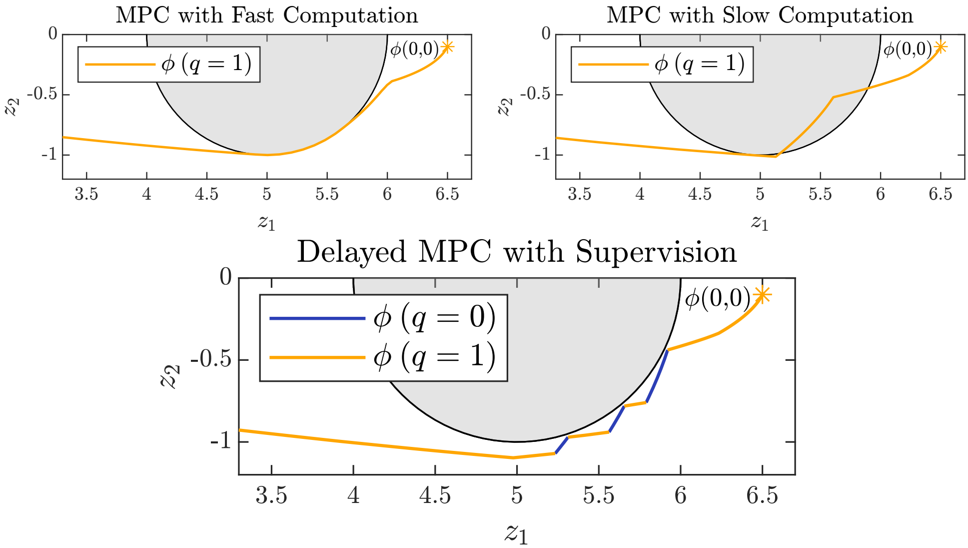


Example: Linear and Affine Feedbacks





Example: MPC with Computational Delays

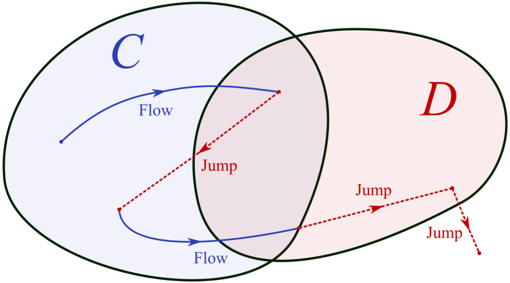


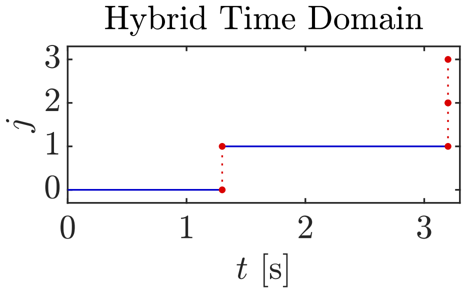
Introduction to Hybrid Dynamical Systems

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

- flow set $C \subset \mathbb{R}^n$
- flow map $f : C \to \mathbb{R}^n$

- jump set $D \subset \mathbb{R}^n$
- jump map $g : D \to \mathbb{R}^n$





Introduction to Hybrid Dynamical Systems

A *solution* ϕ to $\mathcal{H}$ is defined on a hybrid time domain $\operatorname{dom}\phi \subset \mathbb{R}_{\geq 0} \times \mathbb{N}$, which looks something like

$$\operatorname{dom}\phi = ([t_0, t_1] \times \{0\}) \cup ([t_1, t_2] \times \{1\}) \cup \cdots .$$
$$0 = t_0 \leq t_1 \leq t_2 \leq \cdots .$$

We write

$$\sup\nolimits_t \operatorname{dom}\phi := \sup\{\, t \mid (t, j) \in \operatorname{dom}\phi\}$$
$$\sup\nolimits_j \operatorname{dom}\phi := \sup\{\, j \mid (t, j) \in \operatorname{dom}\phi\}.$$

A solution ϕ to $\mathcal{H}$ is said to be *complete* if

$$\sup\nolimits_t \operatorname{dom}\phi + \sup\nolimits_j \operatorname{dom}\phi = \infty.$$

A solution ϕ is said to be *maximal* if it cannot be extended into a longer solution.

Hybrid Model of Closed-Loop System

The hybrid model for our closed-loop switched system is

$$\mathcal{H}_{\mathrm{CL}}\colon \begin{cases} \begin{bmatrix} \dot{z} \\ \dot{q} \end{bmatrix} = f(z,q) := \begin{bmatrix} f_q(z) \\ 0 \end{bmatrix} & (z,q) \in C := C_0 \cup C_1 \\ \begin{bmatrix} z^+ \\ q^+ \end{bmatrix} = g(z,q) := \begin{bmatrix} z \\ 1-q \end{bmatrix} & (z,q) \in D := D_0 \cup D_1, \end{cases} \tag{1}$$

where

$$\begin{aligned} C_0 &:= \mathcal{Z}_0 \times \{0\}, & C_1 &:= \mathcal{Z}_1 \times \{1\}, \\ D_0 &:= \mathcal{Z}_{0\mapsto 1} \times \{0\}, & D_1 &:= \mathcal{Z}_{1\mapsto 0} \times \{1\}. \end{aligned}$$

Result: Forward Invariance

Theorem 1 (Forward Invariance)

Suppose that

- B *is a* $\mathcal{C}^1$ *barrier function of* K *for* $\dot{z} = f_0(z)$.
- f_0 *and* f_1 *are continuous.*
- δ_0, δ_1, θ_0, *and* θ_1 *are continuous and satisfy*

$$\delta_0(z) < \delta_1(z) \leq 0 \quad \text{and} \quad \theta_0(z) < \theta_1(z) \leq 0 \quad \forall z \in \mathbb{R}^n.$$

- *For each* $q \in \{0, 1\}$, *no solution to* $\dot{z} = f_q(z),\ z \in \mathcal{Z}_q$ *has a finite escape time.*

Then:

- $K' := K \times \{0, 1\}$ *is forward invariant for* $\mathcal{H}_{\mathrm{CL}}$.

Furthermore, if ϕ *is bounded, then* $\sup_t \operatorname{dom} \phi = \infty$.

Proof Sketch.

Let

$$B'(z,q) := B(z) \quad \forall (z,q) \in \mathbb{R}^n \times \{0,1\}.$$

The function B' is a barrier function of K' for $\mathcal{H}_{\mathrm{CL}}$, so K' is forward pre-invariant.

To show that all maximal solutions are complete, we show that

- $C \cup D$ is the entire space $\mathbb{R}^n$.
- At every point in $C \setminus D$, flows are viable, so solutions can always either flow or jump.

D and $g(D)$ are closed and disjoint, so that for every bounded solution ϕ, there exists $\gamma > 0$ such that the time between jumps is greater than γ.

$\implies$ If ϕ is maximal and bounded, then $\sup_t \operatorname{dom} \phi = \infty$. $\square$

Result: Forward Invariance Without Chattering

Theorem 2 (Forward Invariance Without Chattering)

Suppose that

- B *is a* $\mathcal{C}^1$ *barrier function of* K *for* $\dot{z} = f_0(z)$.
- f_0 *and* f_1 *are globally Lipschitz continuous with Lipschitz constants* L_0 *and* L_1.
- δ_0, δ_1, θ_0, *and* θ_1 *are continuous and satisfy the threshold function inequalities.*
- *There exists* $\tau > 0$ *such that for all* $z^0 \in \mathcal{Z}_{0\mapsto 1}$ *and* $z^1 \in \mathcal{Z}_{1\mapsto 0}$,

$$|z^0 - z^1| \geq \tau \max\{|f_0(z^0)| \exp(L_0\tau),\ |f_1(z^1)| \exp(L_1\tau)\}.$$

Then,

- τ *is a lower bound on the time between jumps for all solutions to* $\mathcal{H}_{\mathrm{CL}}$.
- *Every maximal solution* ϕ *to* $\mathcal{H}_{\mathrm{CL}}$ *is complete and* $\sup_t \operatorname{dom} \phi = \infty$.

Proof Sketch of Theorem 2.

- Forward pre-invariance is proven using the same barrier function as in Theorem 1.
- Solutions to $\dot{z} = f_0(z)$ and $\dot{z} = f_1(z)$ cannot escape to infinity in finite time because f_0 and f_1 are globally Lipschitz.
- Let $z^0 \in \mathcal{Z}_{0\mapsto 1}$ and $z^1 \in \mathcal{Z}_{1\mapsto 0}$. To prove τ is a lower bound on the time between jumps, we show
  - The (unique) solution to $\dot{z} = f_0(z)$ starting at z^0 satisfies

    $$|z^0 - z^1| \geq \tau |f_0(z^0)| \exp(L_0 \tau) \geq |z(t) - z^0| \quad \forall t \in [0, \tau].$$

    Thus, in time τ, a solution to $\mathcal{H}_{\mathrm{CL}}$ cannot move from $(z^0, 1) \in g(D_0)$ to $(z^1, 1) \in D_1$.
  - The (unique) solution to $\dot{z} = f_1(z)$ starting at z^1 satisfies

    $$|z^0 - z^1| \geq \tau |f_1(z^1)| \exp(L_1 \tau) \geq |z(t) - z^1| \quad \forall t \in [0, \tau].$$

    Thus, in time τ, a solution to $\mathcal{H}_{\mathrm{CL}}$ cannot move from $(z^1, 0) \in g(D_1)$ to $(z^0, 0) \in D_0$.
  - The time to move from $g(D)$ to D is at least τ. $\square$

Example: Lower Bound on Switching Times

Consider the plant

$$\dot{z} = f_{\mathrm{P}}(z, u) := \begin{bmatrix} z_1 \\ u \end{bmatrix}$$

with $z = (z_1, z_2) \in \mathbb{R}^2$ and $u \in \mathbb{R}$.

Admissible Set: Lower Half Plane of $\mathbb{R}^2$

Controllers: $\kappa_0(z) := -|z_1|$

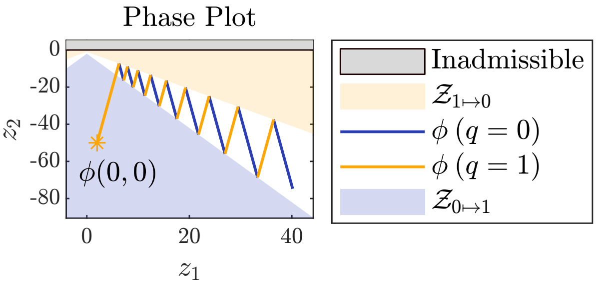
$\kappa_1(z) := +|z_1|$

Barrier Function: $B(z) := z_2$.

Thresholds: $\delta_0(z) := -2 - 2|z_1|$

$\delta_1(z) := -1 - |z_1|$.

Satisfies Theorem 1 $\implies$ K is forward invariant.



Solutions are unbounded $\implies$ Theorem 1 does not guarantee solutions existence for all $t > 0$.

Example: Lower Bound on Switching Times

We find that for $\tau := 0.25$,

$$|z^0 - z^1| \geq \frac{|z_1^0| + 1}{\sqrt{5}} > \tau |f_0(z^0)| \exp(L_0 \tau),$$
$$|z^0 - z^1| \geq \frac{|z_1^1| + 1}{\sqrt{2}} > \tau |f_1(z^1)| \exp(L_1 \tau).$$

Satisfies Theorem 2 $\implies \begin{cases} \text{The time between jumps is at least } \tau = 0.25. \\ \text{Every maximal solution exists for all } t \geq 0. \end{cases}$

Conclusion

Summary

- Designed a hybrid control algorithm that switches between a barrier-certified controller that renders a desired set forward invariant and a 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 to be safely used without constructing barrier functions.

Future work

- Weaken assumption on f_1 to allow for discontinuous vector field.
- Consider systems with disturbances.
- Develop better methods for picking the threshold functions.

Questions?

This research was supported by the following grants:

NSF	CNS-2039054 and CNS-2111688;
AFOSR	FA9550-19-1-0169, FA9550-20-1-0238, FA9550-23-1-0145, and FA9550-23-1-0313;
AFRL	FA8651-22-1-0017 and FA8651-23-1-0004;
ARO	W911NF-20-1-0253;
DOD	W911NF-23-1-0158.

Slides will be available at `paulwintz.com/publications/`.