Verification and Runtime Assurance for Dynamical Systems with Uncertainty

Matthew Abate
The Georgia Institute of Technology
Atlanta, Georgia, USA
Matt.Abate@GaTech.edu

Mark Mote
The Georgia Institute of Technology
Atlanta, Georgia, USA
MMote3@GaTech.edu

Eric Feron
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
Eric.Feron@Kaust.edu.sa

Samuel Coogan
The Georgia Institute of Technology
Atlanta, Georgia, USA
Sam.Coogan@GaTech.edu

ABSTRACT

In this work, we show how controlled robustly forward invariant sets for systems with disturbances are efficiently identified via the application of the mixed monotonicity property. A mixed monotone system can be embedded in a related deterministic embedding system with twice as many states but for which the dynamics are monotone; one can then apply the powerful theory of monotone dynamical systems to the embedding system to conclude useful properties of the initial mixed monotone system. Using this technique, we present a method for verifying state-feedback controllers against safety (set invariance) constraints, and our approach involves evaluating a control barrier function type condition that requires the vector field of the embedding system to point into a certain southeast cone. This approach also facilitates the construction of runtime assurance mechanisms for controlled systems with disturbances, and we study system safety in the presence of state uncertainty as well. The results and findings of this work are demonstrated through two numerical examples where we study (i) the verification of a controlled spacecraft system against a safety constraint, and (ii) the formation of a runtime assurance mechanism that functions in the presence of uncertain state measurements.

CCS CONCEPTS

• **Mathematics of computing → Ordinary differential equations**; • **Computing methodologies → Systems theory**;

KEYWORDS

Mixed Monotone Systems, Controller Verification, Runtime Assurance

ACM Reference Format:
Matthew Abate, Mark Mote, Eric Feron, and Samuel Coogan. 2021. Verification and Runtime Assurance for Dynamical Systems with Uncertainty.

HSCC '21, May 19–21, 2021, Nashville, TN, USA

ACM ISBN 978-1-4503-8339-4/21/05…$15.00
https://doi.org/10.1145/3447928.3456656

In *24th ACM International Conference on Hybrid Systems: Computation and Control (HSCC '21), May 19–21, 2021, Nashville, TN, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3447928.3456656

1 INTRODUCTION

Mixed monotone systems are separable, via a decomposition function, into increasing and decreasing components, and this decomposition function enables embedding the system dynamics in a higher-order deterministic *embedding system* with twice as many states but for which the dynamics are monotone. Mixed monotonicity applies to continuous-time dynamical systems [27], discrete-time dynamical systems [13], controlled systems [21], and systems with disturbances [1, 4], and in all cases, the essential tool of mixed monotonicity is the resulting monotone embedding system. It has been shown, for instance, how robust reachable sets for the initial mixed monotone systems are approximated efficiently via a single simulation of the embedding system; see [13, 21] for over-approximating forward reachable sets, [1] for over-approximating backward reachable sets, and [4] for under-approximating forward/backward reachable sets. See also [8, 24] for fundamental results on monotone dynamical systems theory.

While most works, including those discussed previously, analyze the initial mixed monotone system via a *simulation* of the embedding system, it was recently shown in [1] how useful system information is surmised from simply computing the valuation of the vector field of the embedding system at certain choice states. In particular, [1] shows how robustly forward invariant and attractive sets for continuous-time dynamical systems with disturbances are efficiently identified via the computation of an equilibrium for the embedding system, and this procedure is extended to a discrete-time setting in [12]. See also [23] for an algorithm to compute robustly forward invariant sets for discrete-time monotone control systems.

In this work, we consider continuous-time controlled mixed monotone systems with disturbances, and we answer an analogous question to that of [1] by showing how controlled robustly forward invariant sets are identified by studying only the valuation of the vector field of the embedding system, without simulation. Our approach involves a control barrier function type condition, requiring the vector field of the embedding system to point into an appropriate southeast cone in the embedding space. This creates an intuitive procedure for verifying feedback controllers against safety (invariance) constraints, and we show also how feedback

controllers that make control decisions based on uncertain state measurements are verified in a similar way.

A main assumption in our approach is that the system dynamics are mixed monotone with respect to a known decomposition function; large classes of systems have been shown to be mixed monotone with respect to closed-form decomposition functions constructed from, *e.g.*, bounds on the system Jacobian matrix [21] or domain-specific knowledge [14, 25], and in some instances decomposition functions can also be found by solving an optimization problem [4].

When a candidate control policy cannot be verified safe *a priori*, it is desirable to enforce safety online; this approach is referred to in literature as runtime assurance or active set invariance filtering [15–17]. An active set invariance filter decouples the performance goals of the candidate controller from the system safety goals so that the latter is prioritized in application. Thus, when supplied with a, perhaps unverified, candidate control policy, an active set invariance filter will preempt certain candidate control inputs online in a way that ensures system safety; see [6, 10, 18, 26] for application examples.

Numerous mechanisms exist for enforcing invariance constraints at runtime and, notably, control barrier functions are well suited for this task. This is a main idea of [5, 6] where the resulting controller is formulated as a quadratic program for systems without disturbances, and this idea is extended in [7] to the setting with disturbances. In the case with disturbances, the number of constraints in the optimization program can grow exponentially in the dimension of the disturbance space and, notably, [2] presents a control barrier function based active set invariance filter, formed as a quadratic program, for mixed monotone systems with disturbances; this program contains 2^p linear constraints, where p is the dimension of the disturbance space, and a simulation of the embedding system is computed at each time step. Nonetheless, the quadratic program structure allows the filter to be minimally invasive to the candidate controller in the sense that the candidate input is left unmodified in instances where system safety is verifiable online.

In this work too we explore the construction of active set invariance filters for mixed monotone systems, and we show how such mechanisms are formed by applying control barrier function based reasoning to the embedding system. Unlike [2], our approach avoids online simulation of the embedding system and, instead, control inputs are chosen online to guarantee that the vector field of the embedding system obeys certain linear constraints inside a safe subset of the statespace. Moreover, the resulting active set invariance filter is formulated as a quadratic program with q linear constraints, for a polytopic safe set with q faces.

In summary, we provide a foundational theory of how controllers can be designed in the embedding space, so that without simulation of the embedding system, one can verify the existence of robustly forward invariant regions for the initial system. We study two useful applications that arise from this theory: (a) the offline verification of controllers against safety constraints, and (b) the online enforcement of safety constraints. The results and findings of this work are demonstrated through two numerical examples[1].

[1]The code that accompanies these examples, and generates the figures in this work, is publicly available through the GaTech FactsLab GitHub: https://github.com/gtfactslab/Abate_HSCC2021.

2 NOTATION

We denote vector entries via subscript, *i.e.*, x_i for $x \in \mathbb{R}^n$ denotes the i^{th} entry of the n-dimensional vector x, and we denote by $0_n \in \mathbb{R}^n$ the n-dimensional vector fully populated with zeros. Let (x, y) denote the vector concatenation of $x, y \in \mathbb{R}^n$, *i.e.* $(x, y) := [x^T\ y^T]^T \in \mathbb{R}^{2n}$, and let $\leq$ denote the componentwise vector order, *i.e.* $x \leq y$ if and only if $x_i \leq y_i$ for all i. Let $\leq_{\text{SE}}$ denote the *southeast order* on $\mathbb{R}^{2n}$ defined by

$$(x, x') \leq_{\text{SE}} (y, y') \iff x \leq y \text{ and } y' \leq x' \tag{1}$$

where $x, y, x', y' \in \mathbb{R}^n$. Given $x, y \in \mathbb{R}^n$ with $x \leq y$,

$$[x, y] := \left\{ z \in \mathbb{R}^n \mid x \leq z \text{ and } z \leq y \right\} \tag{2}$$

denotes the hyperrectangle defined by the endpoints x and y, and given a nonsingular transformation matrix $T \in \mathbb{R}^{n \times n}$,

$$[x, y]_T := \left\{ z \in \mathbb{R}^n \mid T^{-1} z \in [x, y] \right\} \tag{3}$$

denotes the parallelotope defined by the endpoints x and y and shape matrix T.

3 PRELIMINARIES

In this work, we consider dynamical systems with disturbances

$$\dot{x} = F(x, u, w) \tag{4}$$

with state $x \in \mathbb{R}^n$, control input $u \in \mathbb{R}^m$, and disturbance input $w \in \mathcal{W} \subset \mathbb{R}^p$. We assume that $\mathcal{W} := [\underline{w}, \overline{w}]$ is a hyperrectangle, for some $\underline{w} \leq \overline{w}$, and we assume also that the vector field $F : \mathbb{R}^n \times \mathbb{R}^m \times \mathcal{W} \to \mathbb{R}^n$ is locally Lipshitz continuous.

3.1 Mixed Monotone Systems

We begin by recalling fundamental results in mixed monotone systems theory.

Definition 1 (Mixed Monotonicity)**.** Given a locally Lipschitz continuous function $d : \mathbb{R}^m \times \mathbb{R}^n \times \mathcal{W} \times \mathbb{R}^n \times \mathcal{W} \to \mathbb{R}^n$, the system (4) is *mixed monotone with respect to d* if

(1) For all $x \in \mathbb{R}^n$, all $u \in \mathbb{R}^m$ and all $w \in \mathcal{W}$

$$d(u; x, w, x, w) = F(x, u, w).$$

(2) For all $i, j \in \{1, \cdots, n\}$, with $i \neq j$,

$$\frac{\partial d_i}{\partial x_j}(u; x, w, \widehat{x}, \widehat{w}) \geq 0$$

for all $u \in \mathbb{R}^m$ and all ordered $x, \widehat{x} \in \mathbb{R}^n$, and $w, \widehat{w} \in \mathcal{W}$ such that $\frac{\partial d}{\partial x}$ exists.

(3) For all $i, j \in \{1, \cdots, n\}$,

$$\frac{\partial d_i}{\partial \widehat{x}_j}(u; x, w, \widehat{x}, \widehat{w}) \leq 0$$

for all $u \in \mathbb{R}^m$ and all ordered $x, \widehat{x} \in \mathbb{R}^n$, and $w, \widehat{w} \in \mathcal{W}$ such that $\frac{\partial d}{\partial \widehat{x}}$ exists.

(4) For all $i \in \{1, \cdots, n\}$ and all $j \in \{1, \cdots, p\}$,

$$\frac{\partial d_i}{\partial w_j}(u; x, w, \widehat{x}, \widehat{w}) \geq 0 \geq \frac{\partial d_i}{\partial \widehat{w}_j}(u; x, w, \widehat{x}, \widehat{w})$$

for all $u \in \mathbb{R}^m$ and all ordered $x, \widehat{x} \in \mathbb{R}^n$, and $w, \widehat{w} \in \mathcal{W}$ such that $\frac{\partial d}{\partial w}$ and $\frac{\partial d}{\partial \widehat{w}}$ exist. ∎

When (4) is mixed monotone with respect to d, d is a *decomposition function* for (4), and when d is clear from context or not germane to the discussion we simply say that (4) is mixed monotone. Given d,

$$\begin{bmatrix}\dot{x}\\ \dot{\widehat{x}}\end{bmatrix} = E(u;\, x,\, \widehat{x}) := \begin{bmatrix}d(u;\, x,\, \underline{w},\, \widehat{x},\, \overline{w})\\ d(u;\, \widehat{x},\, \overline{w},\, x,\, \underline{w})\end{bmatrix} \tag{5}$$

is the *embedding system relative to d* and E is the *embedding function relative to d* [1].

Remark 1. It was recently shown in [4] that all systems of the form (4) are mixed monotone with a unique *tight* decomposition function that provides a tighter approximation of reachable sets when used with [1, Proposition 1] than any other decomposition function for (4). In practice, it is often difficult to obtain a closed-form expression for the tight decomposition function, and for this reason other decomposition function constructions are often used; see [14, 20, 21, 27] for an algorithm to generate decomposition functions for systems with uniformly bounded Jacobian matrices, and see also [1] for an algorithm to generate decomposition functions for systems defined by polynomial vector fields. ■

When F does not depend on u, we omit the first argument in d and E, so that (4) is mixed monotone with respect to $d(x,\, w,\, \widehat{x},\, \widehat{w})$ and $E(x,\, \widehat{x})$ is the embedding function relative to d.

We relate d and F in the following Proposition.

Proposition 1. *Choose $\underline{x},\, \overline{x} \in \mathbb{R}^n$ such that $\underline{x} \preceq \overline{x}$. For all $x \in [\underline{x},\, \overline{x}]$ such that $x_i = \underline{x}_i$,*

$$F_i(x,\, u,\, w) \geq d_i(u;\, \underline{x},\, \overline{x}) \tag{6}$$

for all $u \in \mathbb{R}^m$ and all $w \in \mathcal{W}$. For all $x \in [\underline{x},\, \overline{x}]$ such that $x_i = \overline{x}_i$,

$$F_i(x,\, u,\, w) \leq d_i(u;\, \overline{x},\, \underline{x}) \tag{7}$$

for all $u \in \mathbb{R}^m$ and all $w \in \mathcal{W}$. ■

Next, we recall how robustly forward invariant regions for uncontrolled systems are identified by studying the vector field of the embedding system. We consider

$$\dot{x} = F(x,\, w) \tag{8}$$

where $x \in \mathbb{R}^n$ and $w \in \mathcal{W}$ retain their definitions from (4) and where $F : \mathbb{R}^n \times \mathcal{W} \to \mathbb{R}^n$ is assumed to be Lipshitz continuous. We denote by $\Phi(t; x,\, \mathbf{w})$ the unique state of (8) reached at time $t \geq 0$ when beginning at state $x \in \mathbb{R}^n$ at time 0 and evolving subject to piecewise continuous input signal $\mathbf{w} : [0,\, t] \to \mathcal{W}$. Additionally, we assume (8) is mixed monotone with respect to $d(x,\, w,\, \widehat{x},\, \widehat{w})$, and we denote by $E(x,\, \widehat{x})$ the embedding function relative to d.

Definition 2. A set $S \subseteq \mathbb{R}^n$ is *robustly forward invariant* for (8) if $\Phi(t;\, x,\, \mathbf{w}) \in S$ for all $x \in S$, all $t \geq 0$ and all piecewise continuous inputs $\mathbf{w} : [0,\, t] \to \mathcal{W}$ whenever $\Phi(t;\, x,\, \mathbf{w})$ exists. ■

Proposition 2. *[1] If there exists a $\underline{x},\, \overline{x} \in \mathbb{R}^n$ with $\underline{x} \preceq \overline{x}$ so that*

$$0_{2n} \preceq_{\mathrm{SE}} E(\underline{x},\, \overline{x}) \tag{9}$$

then $[\underline{x},\, \overline{x}] \subset \mathbb{R}^n$ is robustly forward invariant for (8). ■

3.2 Robust Control Barrier Functions and Active Set Invariance Filtering

We next review active set invariance filtering (ASIF) and the online enforcement of safety constraints for controlled systems with disturbances as in (4). For ease of exposition, we assume in the following that (4) is affine in control so that

$$\dot{x} = F(x,\, u,\, w) = f(x,\, w) + g(x,\, w)u, \tag{10}$$

where $f : \mathbb{R}^n \times \mathcal{W} \to \mathbb{R}^n$ and $g : \mathbb{R}^n \times \mathcal{W} \to \mathbb{R}^{n \times m}$ are continuously differentiable functions. The primary goal of the ASIF is to filter an unverified candidate control law $u^{\mathrm{d}}(x)$ in such a way that is *least invasive* to the candidate signal and guarantees system safety. We assume further that $u^{\mathrm{d}}(x)$ is Lipschitz continuous x.

Safety of (10) is formalized by a set invariance requirement; that is, given a set of allowable states $S \subset \mathbb{R}^n$, the closed-loop system is safe if it renders a S robustly forward invariant. To that end, we assume a safe set S defined as the intersection of the super-zero level set of q continuously differentiable scalar valued functions.

Assumption 1 (Safe Set)**.** We assume that S is represented

$$S = \{x \in \mathbb{R}^n \mid h(x) \geq 0_q\} \tag{11}$$

for continuously differentiable $h_1 \cdots h_q : \mathbb{R}^n \to \mathbb{R}$. ■

An equivalent condition for robust forward invariance of S is provided by Nagumo's theorem [9, 22]. Denote by

$$\dot{x} = F^{\mathrm{d}}(x,\, w) = f(x,\, w) + g(x,\, w)u^{\mathrm{d}}(x), \tag{12}$$

the closed loop dynamics of (10) under the candidate controller $u^{\mathrm{d}}(x)$, and let $L_f h(x,\, w)$ and $L_g h(x,\, w)$ denote the lie derivatives of h along f and g, respectively. Under mild technical conditions ensuring that S is a *practical* set [9], the proposition below holds.

Definition 3 (Class-$\mathcal{K}$)**.** A continuous function $\alpha : \mathbb{R} \to \mathbb{R}$ is class-$\mathcal{K}$ if α is strictly increasing and $\alpha(0) = 0$. we extend this notation to vector valued functions as well, so that $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is class-$\mathcal{K}$ when $\alpha_i(x) = \alpha_i(x_i)$ and α_i is class-$\mathcal{K}$ for all i. ■

Proposition 3. *The set S is robustly forward invariant for* (12) *if there exists a class-$\mathcal{K}$ function $\alpha : \mathbb{R}^q \to \mathbb{R}^q$ such that*

$$L_f h(x,\, w) + L_g h(x,\, w)u^{\mathrm{d}}(x) + \alpha(h(x)) \geq 0_q \tag{13}$$

holds for all $x \in S$ and all $w \in \mathcal{W}$. ■

If the candidate controller u^{d} satisfies (13) for some α then S is robustly forward invariant for (12) and u^{d} is considered safe. In the following, we refer to constraints of the form (13) as *barrier constraints* and such constraints are linear inequalities on the variable u for any $x \in \mathbb{R}^n$ and any $w \in \mathcal{W}$.

Definition 4 (Robust Control Barrier Function)**.** A continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}^q$ is a robust control barrier function for (10) if there exists a class-$\mathcal{K}$ function $\alpha : \mathbb{R}^q \to \mathbb{R}^q$ such that for all $x \in S$ there exists a $u \in \mathbb{R}^m$ satisfying

$$L_f h(x,\, w) + L_g h(x,\, w)u + \alpha(h(x)) \geq 0_q \tag{14}$$

for all $w \in \mathcal{W}$. ■

In [7], the authors propose an ASIF, constructed as a quadratic program where the constraints in this program are given by (14). This filter is given below as CBF-QP.

CBF-QP

$$u^{\mathrm{a}}(x) = \underset{u\in\mathbb{R}^m}{\arg\min} ||u - u^{\mathrm{d}}(x)||_2^2 \tag{15}$$

$$\text{s.t.} \quad L_f h(x,\, w) + L_g h(x,\, w)u + \alpha(h(x)) \geq 0_q \quad \text{for all } w \in \mathcal{W} \tag{16}$$

Proposition 4. *If h is a robust control barrier function for* (10) *and satisfies* (14) *with the class-$\mathcal{K}$ function α, then for all Lipshitz continuous $u^{\mathrm{d}}(x)$ and all continuous signals $w : [0;\, \infty) \to \mathcal{W}$ the CBF-QP is always feasible and the set S is robustly forward invariant for closed loop dynamics of* (10) *under u^{a}.* ■

While the program CBF-QP is always feasible when $h(x)$ is a robust barrier function for (10), note that the program contains an infinite number of linear constraints and, thus, is not always practically implementable. We discuss this concern further in the following sections.

4 PROBLEM SETTING

In this section, we introduce the problem statements of this work, and we discuss the differences between controller verification and runtime assurance. We assume a system of the form (4), and a *safe* set of operating conditions $S \subset \mathbb{R}^n$.

Assumption 2 (Safe Set)**.** Assume a set of safe states given by a hyperrectangle $S := [\underline{s},\, \overline{s}] \subset \mathbb{R}^n$. ■

Traditionally, mixed monotone systems theory has been employed for the analysis of hyperrectangular sets of interest (see *e.g.* Proposition 2), however it was recently shown in [3] how alternative set geometries, *i.e.* polytopic sets, can be analyzed similarly using the tools of mixed monotonicity. Thus, while S is assumed hyperrectangular, the basic results and tools generated in this work are applicable to the more general class of polytopic safe sets, and we demonstrate this assertion through discussion and examples later in the work. Therefore, Assumption 2 is not particularly restrictive on the problem setting.

The goal is to construct a (feedback) controller for (4) that ensures the robust forward invariance of S. One approach to this problem involves *verifying* a candidate controller *a priori*. For example, assume a candidate controller $u^{\mathrm{d}} : \mathbb{R}^n \to \mathbb{R}^m$; denote by

$$\dot{x} = F^{\mathrm{d}}(x,\, w) = F(x,\, u^{\mathrm{d}}(x),\, w) \tag{17}$$

the closed loop dynamics of (4) under $u^{\mathrm{d}}(x)$.

Problem 1 (Controller Verification)**.** Given a feedback controller $u^{\mathrm{d}}(x)$, show that $S = [\underline{s},\, \overline{s}]$ is robustly forward invariant for (17). ■

There are two natural ways to solve Problem 1 using the theory and tools discussed thus far:

(i) One can construct a robust barrier function for the closed loop dynamics (17).
(ii) One can compute a decomposition function d for the closed loop dynamics (17) and show that E satisfies (9), as discussed in Proposition 2.

Solving Problem 1 via method (i) involves computing a class-$\mathcal{K}$ function $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that

$$\frac{\partial h}{\partial x}(x) F^{\mathrm{d}}(x,\, w) \geq -\alpha(h(x)) \tag{18}$$

for all $x \in S$ and for all $w \in \mathcal{W}$, where $h : \mathbb{R}^n \to \mathbb{R}^{2n}$ is given by

$$h(x) := (x - \underline{s},\, \overline{s} - x). \tag{19}$$

In this case, $h(x) \geq 0_{2n}$ implies $x \in S$, and S is robustly forward invariant for (17) by virtue of the fact that $h(x)$ is a robust barrier function for (17). Solving Problem 1 via method (ii) involves computing a decomposition function d for (17) so that (9) holds.

When methods (i) and (ii) fail to solve Problem 1, *i.e.* when u^{d} cannot be verified *a priori*, it is desirable to enforce safety online. This procedure involves filtering u^{d} at runtime to ensure the robust forward invariance of S, as discussed in Problem 2.

Problem 2 (Runtime Assurance)**.** Given a feedback controller $u^{\mathrm{d}}(x)$, design a controller $u^{\mathrm{a}}(x)$ such that S is robustly forward invariant for

$$\dot{x} = F(x,\, u^{\mathrm{a}}(x),\, w) \tag{20}$$

and such that $u^{\mathrm{a}}(x)$ evaluates to $u^{\mathrm{d}}(x)$ whenever possible. ■

A controller that solves Problem 2 is referred to as a *runtime assurance mechanism* or an *active set invariance filter* (ASIF). Several methods exist for solving Problem 2 and we have discussed previously how robust barrier functions are well suited for this task. However, the CBF-QP is not always implementable as the program contains an infinite number of linear constraints. A solution is presented in [2], which also considers mixed monotone systems, where an ASIF is constructed as a quadratic problem with 2^p linear constraints, and where p is the dimension of the disturbance-space. This construction, however, is not suitable for systems with state uncertainty, another limitation we address in this work. In particular, we accommodate uncertainty in state via a set-valued observer as formalized next.

Definition 5 (Uncertain Observer)**.** At time $t \geq 0$ an uncertain observer provides a hyperrectangle $\mathcal{X}(t) := [\underline{x}(t),\, \overline{x}(t)] \subset \mathbb{R}^n$ satisfying $x(t) \in \mathcal{X}(t)$ where $x(t)$ is the current system state. We assume always that $\underline{x}(t)$, $\overline{x}(t)$ vary continuously in t. ■

In the following, we study the verification and construction of feedback controllers which operate based on the uncertain observer output. Such a controller is denoted $u(\mathcal{X}) = u(\underline{x},\, \overline{x})$, where we note that $\underline{x}(t)$, $\overline{x}(t)$ fully characterise the observer output $\mathcal{X}(t)$.

Problem 3 (Controller Verification with State Uncertainty)**.** Given a feedback controller $u^{\mathrm{d}}(\mathcal{X})$, show that for all observer signals $\mathcal{X}(t)$, S is robustly forward invariant for (4) when $u^{\mathrm{d}}(\mathcal{X})$ is employed. ■

Problem 4 (Runtime Assurance with State Uncertainty)**.** Given a feedback controller $u^{\mathrm{d}}(\mathcal{X})$, design a controller $u^{\mathrm{a}}(\mathcal{X})$ such that S is robustly forward invariant for

$$\dot{x} = F(x,\, u^{\mathrm{a}}(\mathcal{X}),\, w) \tag{21}$$

for all observer signals $\mathcal{X}(t) := [\underline{x}(t),\, \overline{x}(t)]$, and such that $u^{\mathrm{a}}(\mathcal{X})$ evaluates to $u^{\mathrm{d}}(\mathcal{X})$ whenever possible . ■

Remark 2. Importantly, Problems 3 and 4 do not require $\mathcal{X}(t) \subseteq S$ for all t. Rather, we allow $\mathcal{X}(t)$ to leave S (at least partially). Nonetheless, the proposed control methodology below will still ensure $x(t) \in S$ for all t; that is, even though the observer only guarantees $x(t) \in \mathcal{X}(t)$, the proposed controller guarantees $x(t) \in \mathcal{X}(t) \cap S$, provided that initially $\mathcal{X}(0) \subseteq S$. ■

In the following, we solve Problems 1, 2, 3 and 4, and our solutions rely on mixed monotonicity theory and the tools presented thus far. In particular, Problems 2 and 4 are solved with a controller designed as an optimization problem, in a similar way to the CBF-QP (15)-(16); however, our construction requires only 1 constraint for each face of S and the complexity of the optimization problem is agnostic to the dimension of the disturbance space.

5 CONTROLLER VERIFICATION VIA MIXED MONOTONICITY

In this section, we solve Problems 1 and 3 by applying control barrier function based reasoning to the embedding system (5). As before, we consider a system of the form (4) and a safe set $S = [\underline{s}, \overline{s}]$. We also take the following assumption on our problem setting.

Assumption 3. We assume that (4) is mixed monotone with decomposition function $d(u;\, x,\, w,\, \widehat{x},\, \widehat{w})$, and we denote by $E(u;\, x,\, \widehat{x})$ the embedding function relative to d, as given in (5). ■

5.1 Controller Verification with Full-State Feedback

We begin by addressing Problem 1—the controller verification problem—and we show how traditional barrier based reasoning can be applied to the embedding system to verify a given desired controller $u^{\mathrm{d}}(x)$ renders S robustly forward invariant for (4).

Proposition 5. *Assume a desired controller $u^{\mathrm{d}}(x)$. If there exists a class-$\mathcal{K}$ $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that*

$$-\alpha(\,(x,\, x) - (\underline{s},\, \overline{s})\,) \preceq_{\mathrm{SE}} E(u^{\mathrm{d}}(x);\, x,\, x) \tag{22}$$

for all $x \in S$, then S is robustly forward invariant for (17). ■

Proof. Choose $u^{\mathrm{d}}(x)$ and assume that (22) holds for all $x \in S$. Additionally, choose $x' \in S$ so that $x'_i = \underline{s}_i$, *i.e.* x' is on the i^{th}-bottom-face of S, and let $u' = u^{\mathrm{d}}(x')$. Then

$$\begin{aligned} -\alpha_i(x'_i - \underline{s}_i) &\leq E_i(u';\, x',\, x') \\ &= d_i(u';\, x',\, x') \\ &\leq F_i(x',\, u',\, w) \end{aligned} \tag{23}$$

for all $w \in \mathcal{W}$, where the first inequality in (23) is a result of (22) and the last inequality in (23) is a result of Proposition 1. Moreover, $\alpha_i(x'_i - \underline{s}_i) = 0$ and therefore $F_i(x',\, u(x'),\, w) \geq 0$ for all $w \in \mathcal{W}$ when $x'_i = \underline{s}_i$. Using a similar argument, it can be shown that when $x' \in S$ is chosen so that $x'_i = \overline{s}_i$, we have $F_i(x',\, u(x'),\, w) \leq 0$ for all $w \in \mathcal{W}$. Therefore, S is robustly forward invariant for (17). This completes the proof. □

Proposition 5 provides a basic method for solving Problem 1. This method has two steps:

- Compute a decomposition function d for (4), and form the the corresponding embedding function E via (5).
- Given a desired controller $u^{\mathrm{d}}(x)$, compute a class-$\mathcal{K}$ function $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$, so that (22) holds for all $x \in S$.

When such an α exists, S is robustly forward invariant for (17), and Problem 1 is solved via this approach.

5.2 Controller Verification in the Presence of State Uncertainty

We next address Problem 3 and show how a candidate controller $u^{\mathrm{d}}(\mathcal{X})$ that operates based on the uncertain system measurement $\mathcal{X}(t)$ is verified against safety constraints. As discussed in Remark 2, the goal is not to ensure that $\mathcal{X}(t) \subset S$ for all t; rather, Problem 3 is solved when the current system state x satisfies $x(t) \in S$ for all t. As such any controller $u^{\mathrm{d}}(\mathcal{X})$ that solves Problem 4 can choose to make control decisions based only on $\mathcal{X}(t) \cap S$ and, for this reason, we next introduce the concept of an observer filter, as defined in Definition 6. While such a filter need not be implemented in practice, we introduce this concept to facilitate the following derivations.

Definition 6 (Observer Filter)**.** An observer filter receives the current observer output $\mathcal{X}(t)$ and returns the filtered output $\mathcal{Z}(t) := \mathcal{X}(t) \cap S$. Equivalently, an observer filter receives $\mathcal{X}(t) = [\underline{x}(t),\, \overline{x}(t)]$ and returns $\mathcal{Z}(t) = [\underline{z}(t),\, \overline{z}(t)]$ where

$$\underline{z}_i(t) = \max\{\underline{x}_i(t),\, \underline{s}_i\}, \qquad \overline{z}_i(t) = \min\{\overline{x}_i(t),\, \overline{s}_i\}, \tag{24}$$

for $i \in \{1, \cdots, n\}$. This is a result of the fact that both S and $\mathcal{X}(t)$ are hyperrectangles. ■

As discussed above, it is without loss of generality to assume that a controller that solves Problem 3 makes control decisions after referencing the filtered observer output $\mathcal{Z}(t)$, rather than $\mathcal{X}(t)$. We now have the requisite tools to solve Problem 3.

Theorem 1. *Consider a desired controller $u^{\mathrm{d}} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^m$ with the property that $u^{\mathrm{d}}(\underline{x}, \overline{x}) = u^{\mathrm{d}}(\underline{z}, \overline{z})$ whenever $[\underline{x}, \overline{x}] \cap S \neq \emptyset$ where $\underline{z}$ and $\overline{z}$ are as defined in* (24), i.e., *the control policy acts on filtered observer states. If there exists a class-$\mathcal{K}$ $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that*

$$-\alpha(\,(\underline{z},\, \overline{z}) - (\underline{s},\, \overline{s})\,) \preceq_{\mathrm{SE}} E(u^{\mathrm{d}}(\underline{z},\, \overline{z});\, \underline{z},\, \overline{z}) \tag{25}$$

for all $\underline{z}$, $\overline{z} \in S$ with $\underline{z} \preceq \overline{z}$, then for all observer signals $\mathcal{X}(t)$, S is robustly forward invariant for (4) *when $u^{\mathrm{d}}(\mathcal{X})$ is employed.* ■

Proof. Choose $u^{\mathrm{d}}(\underline{x},\, \overline{x})$ and assume that (25) holds for all $\underline{z}$, $\overline{z} \in \mathbb{R}^n$ satisfying $\underline{s} \preceq \underline{z} \preceq \overline{z} \preceq \overline{s}$. Additionally, choose $x' \in S$ so that $x'_i = \underline{s}_i$, *i.e.* x' is on the i^{th}-bottom-face of S, and choose $\overline{z}'$, $\underline{z}'$ so that $x' \in [\underline{z},\, \overline{z}] \subseteq S$. Lastly, let $u' = u^{\mathrm{d}}(\overline{z}',\, \underline{z}')$.

Since $x'_i = \underline{s}_i$ and $x' \in [\underline{z},\, \overline{z}] \subseteq S$, note that $\underline{z}_i = \underline{s}_i$. Note also that

$$\begin{aligned} -\alpha_i(\underline{z}'_i - \underline{s}_i) &\leq E_i(u';\, \underline{z}',\, \overline{z}') \\ &= d_i(u';\, \underline{z}',\, \overline{z}') \\ &\leq F_i(x',\, u',\, w) \end{aligned} \tag{26}$$

for all $w \in \mathcal{W}$, where the first inequality in (26) is a result of (25) and the last inequality in (26) is a result of Proposition 1. Moreover, $\alpha_i(\underline{z}'_i - \underline{s}_i) = 0$ and therefore $F_i(x',\, u(\underline{z}',\, \overline{z}'),\, w) \geq 0$ for all $w \in \mathcal{W}$ when $x'_i = \underline{s}_i$. Using a similar argument, it can be shown that when $x' \in S$ is chosen so that $x'_i = \overline{s}_i$, we have $F_i(x',\, u(\underline{z}',\, \overline{z}'),\, w) \leq 0$ for all $w \in \mathcal{W}$. Therefore, for all observer signals $\mathcal{Z}(t) = [\underline{z}(t),\, \overline{z}(t)]$

S is robustly forward invariant for (4) when $u^{\mathrm{d}}(\underline{z}, \overline{z})$ is employed. This completes the proof. □

The results of Theorem 1 subsume those of Proposition 5 as a special case; that is, when $\mathcal{X}(t) = [x(t), x(t)]$ for all t, *i.e.* state uncertainty is not present, the constraint (25) resolves to (22) and the hypothesis of Theorem 1 is equivalent to that of Proposition 5.

5.3 Extending to General Polytopic Sets

Problems 1 and 3 assume a hyperrectangular safe set of operating conditions S, however, we show in this section how the basic theory posited in Proposition 5 and Theorem 1 extends to more general class of polytopic safe sets, in a similar way.

To that end, we next assume a convex polytope safe set, defined as the intersection of several parallelotopes in $\mathbb{R}^n$.

Assumption 4. We assume a convex polytope safe set $S \subset \mathbb{R}^n$, defined as the intersection of q parallelotopes $\{S^j\}_{j=1}^q$ so that $S := \cap_{j=1}^q S^j$ and $S^j := [\underline{s}^j, \overline{s}^j]_{T_j}$ where $\underline{s}^j \preceq \overline{s}^j$ for all for $j \in \{1, \cdots, q\}$ and $T_j \in \mathbb{R}^{n\times n}$ is a nonsingular transformation matrix. ■

As in Problem 3, we aim to verify that a candidate feedback controller $u^{\mathrm{d}}(\mathcal{X})$ renders S robustly forward invariant for (4), where $u^{\mathrm{d}}(\mathcal{X})$ makes control decisions after referencing the current uncertain observer output $\mathcal{X}(t)$. Here, however, we allow $\mathcal{X}(t)$ to take a nonhyperrectangular geometry, and we assume only that $\mathcal{X}(t)$ is bounded in the intersection of parallelotopes in a way similar to that of S.

Assumption 5. At time $t \geq 0$ the uncertain observer receives the current system state $x(t)$ and returns a set $\mathcal{X}(t) \subset \mathbb{R}^n$ so that $x(t) \in \mathcal{X}(t)$. Moreover, we assume access to q parallelotope signals $\mathcal{X}^1(t), \cdots, \mathcal{X}^q(t)$ so that

$$\mathcal{X}(t) \subseteq \bigcap_{j=1}^{q} \mathcal{X}^j(t), \quad \text{and} \quad \mathcal{X}^j(t) := [\underline{x}^j(t), \overline{x}^j(t)]_{T_j} \tag{27}$$

for all t where $\underline{x}^j(t)$, $\overline{x}^j(t)$ are known and where $T_j \in \mathbb{R}^{n\times n}$ maintains its definition from Assumption 4. Additionally, an observer filter receives the current observer output $\mathcal{X}(t)$ and returns the filtered output $\mathcal{Z}(t) \subset \mathbb{R}^n$, where $\mathcal{Z}(t) = \cap_{j=1}^q \mathcal{Z}^j(t)$ and $\mathcal{Z}^j = \mathcal{X}^j(t) \cap S^j$. Equivalently $\mathcal{Z}^j(t) = [\underline{z}^j, \overline{z}^j]_{T_j}$ where

$$\underline{z}_i^j(t) = \max\{\underline{x}_i^j(t), \underline{s}_i^j\}, \qquad \overline{z}_i^j(t) = \min\{\overline{x}_i^j(t), \overline{s}_i^j\}. \tag{28}$$

■

The fundamental idea in Assumption 5 is that an uncertain observer, in this setting, will return a set of parallelotopes $\{\mathcal{X}^j\}_{j=1}^q$ so that the current system state $x(t)$ is contained in the intersection and $\mathcal{X}^j$ has the same geometry as S^j. The observer filter then operates in a manner similar to that described in Definition 6.

We next show how a candidate controller $u^{\mathrm{d}}(\mathcal{Z})$ is verified to render S robustly forward invariant for (4). For all $j \in \{1, \cdots, q\}$ construct the transformed dynamics

$$\dot{x} = T_j^{-1} F(T_j x, u, w) \tag{29}$$

with state $y \in \mathbb{R}^n$, control input $u \in \mathbb{R}^m$, and disturbance $w \in \mathcal{W}$, and where F and $\mathcal{W}$ maintain their definitions from (4). For each j, let (29) be mixed monotone with respect to $d^j(u; x, w, \widehat{x}, \widehat{w})$ and let $E^j(u; x, \widehat{x})$ denote the embedding function relative to d^j.

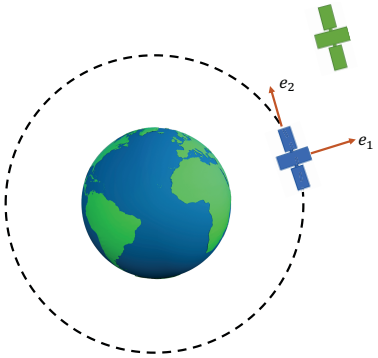


Figure 1: Problem Setting of Section 5.4: the target spacecraft is shown in blue and the chaser spacecraft is shown in green. Unit vectors in the y_1 and y_2 directions are also shown, and are notated e_1 and e_2.

Theorem 2. *Assume a desired controller $u^{\mathrm{d}}(\mathcal{Z})$. If, for each $j \in \{1, \cdots, q\}$, there exists a class-$\mathcal{K}$ $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that*

$$-\alpha(\,(\underline{z}^j, \overline{z}^j) - (\underline{s}^j, \overline{s}^j)\,) \preceq_{\mathrm{SE}} E(u^{\mathrm{d}}(\mathcal{Z}); \underline{z}^j, \overline{z}^j) \tag{30}$$

for all $\mathcal{Z}(t) = \cap_{j=1}^q [\underline{z}^j, \overline{z}^j]_{T_j}$ satisfying $\underline{s}^j \preceq \underline{z}^j \preceq \overline{z}^j \preceq \overline{s}^j$, then S is robustly forward invariant for (17). ■

We omit a formal proof for Theorem 2, as the result follows directly from the general theory posited in Theorem 1 and the results of [3]; the work [3] shows how parallelotope sets are analyzed by applying the tools of mixed monotonicity to the related system (29) formed via a linear transformation of the initial state space.

Theorem 2 shows how a candidate controller $u^{\mathrm{d}}(\mathcal{X})$, which makes control decisions based on the uncertain observer output $\mathcal{X}$, is verified in rendering S robustly forward invariant, where we now allow for a general polytope safe set S and $\mathcal{X}$ is not restricted to any geometry, so long (27) is satisfied.

5.4 Numerical Example

To demonstrate the utility of Proposition 5, we next present a numerical example where we verify a controlled spacecraft system against a safety constraint. This problem setting is taken from [19].

We consider two spacecraft in orbit around the earth: (i) a *target* spacecraft, which is in a fixed circular orbit with period τ, and (ii) a *chaser* spacecraft of mass m. In this setting, the dynamics of the chaser spacecraft are given by the Clohessy-Wiltshire-Hill equations, as developed in [11]:

$$\begin{aligned} \ddot{y}_1 &= 3\gamma^2 y_1 + 2\gamma \dot{y}_2 + \tfrac{1}{m} u_1 + w_1 \\ \ddot{y}_2 &= -2\gamma \dot{y}_1 + \tfrac{1}{m} u_2 + w_2 \\ \ddot{y}_3 &= -\gamma^2 y_3 \end{aligned} \tag{31}$$

with state $(y, \dot{y}) \in \mathbb{R}^6$, control input $u \in \mathbb{R}^2$ and disturbance input $w \in [\underline{w}, \overline{w}] \subset \mathbb{R}^2$. In this setting, y_1, y_2, y_3 denote the relative distances between the spacecrafts and $\dot{y}_1$, $\dot{y}_2$, $\dot{y}_3$ denote the respective relative velocities. Additionally, $\gamma = \frac{2\pi}{\tau}$ [11]. This problem setting is depicted graphically in Figure 1.

We consider also $x \in \mathbb{R}^2$, as defined by

$$\begin{aligned} x_1 &:= \dot{y}_1 - \tfrac{\gamma}{2} y_2, \\ x_2 &:= \dot{y}_2 + 2\gamma y_1. \end{aligned} \tag{32}$$

The system (31) is said to be in a *periodic natural motion trajectory* when $x = 0_2$ and, in this case, $y(t)$ will make periodic orbits about the origin, provided $u(t) = w(t) = 0_2$ for all $t \geq 0$; that is, $x = 0_2$ defines a linear subspace in $\mathbb{R}^6$ that is invariant for (31) when $u(t) = w(t) = 0_2$. This invariant subspace is defined by the collection of periodic orbits about $x = 0_2$ and, thus, the norm of x provides a metric of distance to this surface. While the nondeterministic nature of the disturbance input w prevents the system (31) from maintaining a single natural motion trajectory in orbit, it is preferable to minimize x along trajectories of (31), when possible, so that if the ability to actuate the system is ever lost, the system will not drift significantly off course. Thus, it is the goal of this study to verify that a candidate control policy u^{d} ensures $x(t) \in S := [\underline{s}, \overline{s}]$ for all t, and we assume full state feedback so that u^{d} is allowed to make control decisions based on the current system state $x(t)$. Note also that the dynamics governing x are

$$\dot{x} = F(x, u, w) = \begin{bmatrix} \frac{3\gamma}{2} x_2 + \frac{1}{m} u_1 + w_1 \\ \frac{1}{m} u_2 + w_2 \end{bmatrix}. \tag{33}$$

The system (33) is *monotone, i.e.* mixed monotone with respect to $d(u; x, w, \widehat{x}, \widehat{w}) = F(x, u, w)$, and we form the respective embedding function E using (5). We take a candidate controller

$$u^{\mathrm{d}}(x) = \begin{bmatrix} -mx_1 - \frac{3\gamma}{2} mx_2 \\ -mx_2 \end{bmatrix}, \tag{34}$$

and a class-$\mathcal{K}$ function $\alpha_i(x) = x_i$, for $i \in \{1, \cdots, 4\}$. So that the constraint (22) becomes

$$\underline{s} \leq \underline{w} \leq \overline{w} \leq \overline{s}. \tag{35}$$

Thus, it follows from Proposition 5 that u^{d} renders $S = [\underline{s}, \overline{s}]$ robustly forward invariant for (33), in all instances where (35) holds.

6 RUNTIME ASSURANCE VIA MIXED MONOTONICITY

In this section, we solve Problems 2 and 4, by applying control barrier function based reasoning to the embedding system (5). As before, we consider a system of the form (4) and hyperrectangular safe set $S = [\underline{s}, \overline{s}]$. We assume that (4) is mixed monotone with respect to d and E is the embedding function relative to d.

6.1 Runtime Assurance with Full State Feedback

In this section, we solve Problem 2. We begin with a structural assumption on the embedding function E.

Assumption 6. We assume that for all $x \in S$, $E(u; x, x)$ is affine in control so that

$$E(u; x, x) = E^1(x) + E^2(x)u \tag{36}$$

for some $E^1 : \mathbb{R}^n \to \mathbb{R}^n$ and $E^2 : \mathbb{R}^n \to \mathbb{R}^{n \times m}$. ■

Assumption 6 is not particularly restrictive and, in particular, we note that if F from (4) takes the form

$$F(x, u, w) = F^1(x, w) + F^2(x)u, \tag{37}$$

for suitable $F^1 : \mathbb{R}^n \times \mathcal{W} \to \mathbb{R}^n$ and $F^2 : \mathbb{R}^n \to \mathbb{R}^{n \times m}$, then (4) will always have a decomposition function satisfying the hypothesis of Assumption 6; see the tight decomposition function construction [4]. Next, we introduce the concept of embedded-invariance.

Definition 7 (Embedded-Invariance)**.** The set $S \subset \mathbb{R}^n$ is embedded-invariant for (5) if there exists a class-$\mathcal{K}$ $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that for all $x \in S$ there exists a $u \in \mathbb{R}^m$ satisfying

$$-\alpha(\,(x, x) - (\underline{s}, \overline{s})\,) \preceq_{\mathrm{SE}} E^1(x) + E^2(x)u. \tag{38}$$

■

We next show how an ASIF, which renders S forward invariant for (4) and solves Problem 2, is constructed when S is embedded-invariant for E. This ASIF is constructable when there exists $u \in \mathbb{R}^m$ satisfying the constraint (38) for each $x \in S$. Moreover, the resulting ASIF, given below as ECBF-QP, is also defined as a minimally invasive quadratic program.

ECBF-QP

$$u^{\mathrm{a}}(x) = \underset{u \in \mathbb{R}^m}{\arg\min} ||u - u^{\mathrm{d}}(x)||_2^2 \tag{39}$$

$$\text{s.t.} \quad -\alpha(\,(x, x) - (\underline{s}, \overline{s})\,) \preceq_{\mathrm{SE}} E^1(x) + E^2(x)u. \tag{40}$$

Theorem 3. *If S is embedded-invariant for* (4)*, then the ECBF-QP is always feasible, and the controller* (39)-(40) *solves Problem 2; that is, S is robustly forward invariant for the closed loop dynamics of* (4) *under u^{a}, and $u^{\mathrm{a}}(x)$ evaluates to $u^{\mathrm{d}}(x)$ when it is safe to do so.* ■

Proof. From the fact that S is embedded-invariant for (5), there will always exists u satisfying the constraint (40). Moreover, the ECBF-QP is always feasible. When $u^{\mathrm{d}}(x)$ satisfies (38), *i.e.*, applying $u^{\mathrm{d}}(x)$ ensures that trajectories of (4) do not leave S, $u^{\mathrm{a}}(x(t))$ will always evaluate to $u^{\mathrm{d}}(x)$. Thus, the controller (39)-(40) solves Problem 2. This completes the proof. □

6.2 Runtime Assurance in the Presence of State Uncertainty

We next solve Problem 4 and design an ASIF for (4) that provides assurance in the presence of state uncertainty. As before, we assume the presence of an observer filter (Definition 6) in the candidate controller so that $u^{\mathrm{d}}(\mathcal{X}(t)) = u^{\mathrm{d}}(\mathcal{Z}(t))$ for all $t \geq 0$, where $\mathcal{Z}(t) = [\underline{z}(t), \overline{z}(t)]$ is given by (24). Additionally, we take the following structural assumption on the embedding system.

Assumption 7. We assume that for all $x, \widehat{x} \in S$ with $x \preceq \widehat{x}$, $E(u; x, \widehat{x})$ is affine in control so that

$$E(u; x, \widehat{x}) = E^1(x, \widehat{x}) + E^2(x, \widehat{x})u \tag{41}$$

for some $E^1 : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ and $E^2 : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^{n \times m}$. ■

We next introduce the concept of uncertain embedded-invariance (Definition 8).

Definition 8 (Uncertain Embedded-Invariance)**.** The set S is uncertain embedded-invariant for (5) if there exists a class-$\mathcal{K}$ $\alpha : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ so that for all $\underline{z}, \overline{z} \in S$ with $\underline{z} \preceq \overline{z}$ there exists a $u \in \mathbb{R}^m$ satisfying

$$-\alpha(\ (\underline{z}, \overline{z}) - (\underline{s}, \overline{s})\ ) \preceq_{\text{SE}} E^1(\underline{z}, \overline{z}) + E^2(\underline{z}, \overline{z})u. \tag{42}$$

■

We next propose a construction for an ASIF that renders S forward invariant for (4) and solves Problem 4 when S is embedded-invariant for E. Moreover, the resulting ASIF, given below as UECBF-QP, is defined as a minimally invasive quadratic program.

UECBF-QP

$$u^{\text{a}}(\underline{z}, \overline{z}) = \underset{u \in \mathbb{R}^m}{\arg\min} ||u - u^{\text{d}}(\underline{z}, \overline{z})||_2^2 \tag{43}$$

$$\text{s.t.} \quad -\alpha(\ (\underline{z}, \overline{z}) - (\underline{s}, \overline{s})\ ) \preceq_{\text{SE}} E^1(\underline{z}, \overline{z}) + E^2(\underline{z}, \overline{z})u. \tag{44}$$

Theorem 4. *If S is embedded-invariant for* (4)*, then the UECBF-QP is always feasible, and the controller* (43)*–*(44) *solves Problem 4; that is, $u^{\text{a}}(\underline{z}, \overline{z})$ evaluates to $u^{\text{d}}(\underline{z}, \overline{z})$ whenever possible and S is robustly forward invariant for $\dot{x} = F(x, u^{\text{a}}(\underline{z}, \overline{z}), w)$ for all observer signals $\mathcal{Z}(t) = [\underline{z}(t), \overline{z}(t)]$ satisfying $x(t) \in \mathcal{Z}(t) \subseteq S$ for all t.* ■

6.3 Numerical Example

To demonstrate the utility of Theorem 4, we study a polynomial system and form an ASIF to ensure the forward invariance of a polytope subset of the statespace. We consider the system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x, u, w) = \begin{bmatrix} -x_1 - x_1^3 + x_2 + u_1 + w^3 \\ -x_2 - x_2^3 - x_1 + u_2 - w \end{bmatrix} \tag{45}$$

with state $x \in \mathbb{R}^2$, control input $u \in \mathbb{R}^2$ and scalar disturbance $w \in \mathcal{W}$, for hyperrectangular $\mathcal{W} = [\underline{w}, \overline{w}]$ with $\overline{w} = -\underline{w} = 1/2$.

The goal of this study is to design an ASIF for (45) that enforces the robust forward invariance of a safe set S in the presence of state uncertainty. We choose an octagon safe set $S \subset \mathbb{R}^2$, described as the intersection of parallelotopes $S = [\underline{s}, \overline{s}] \cap [\underline{s}, \overline{s}]_T$ where $\overline{s} = -\underline{s} = (1, 1)$ and where

$$T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \tag{46}$$

and control decisions are made via an uncertain observer, which provides a circular subset $\mathcal{X}(t)$ so that $x(t) \in \mathcal{X}(t)$ for all t. Additionally, an observer filter $\mathcal{Z}(t) = \mathcal{Z}^1(t) \cap \mathcal{Z}^2(t)$ is employed, which provides two parallelotope over-approximations of $\mathcal{X}(t) \cap S$. This problem setting is depicted graphically in Figure 2.

We next go about designing an ASIF for (45) by applying the procedure detailed in Section 6.2. The system (45) is mixed monotone with respect to

$$d(u; x, w, \widehat{x}, \widehat{w}) = \begin{bmatrix} -x_1 - x_1^3 + x_2 + u_1 + w^3 \\ -x_2 - x_2^3 - \widehat{x}_1 + u_2 - \widehat{w} \end{bmatrix} \tag{47}$$

and we denote by E the embedding function relative to d as prescribed in (5). Using an analogous procedure, a decomposition function d_T for (29) is also formed , and we denote by E_T the embedding function relative to d_T. Both E and E_T satisfy Assumption 7, and we numerically verify that S is uncertain embedded invariant for both E and E_T with the class-$\mathcal{K}$ function $\alpha_i(x) = 5000x_i^3$ for $i \in \{1, \cdots, 2n\}$. Thus we form an ASIF for (45), using (43)-(44), where the constraint (44) is understood to hold for both E and E_T.

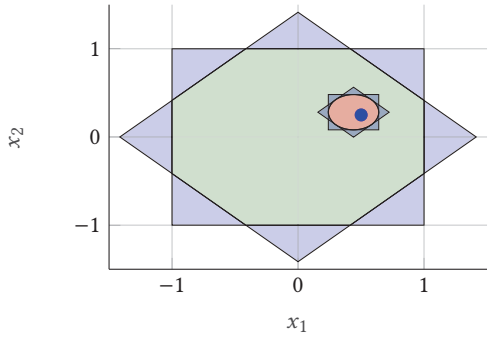


Figure 2: Problem setting of Section 6.3. The octagon safe set S is shown in green, and $[\underline{s}, \overline{s}]$ and $[\underline{s}, \overline{s}]_T$ are shown in blue. For a state $x(t)$, shown in blue, the observation $\mathcal{X}(t)$ is shown in red, and the filtered observation, which is comprised of two parallelotopes, is shown in blue.

A demonstration of the ASIF formed in this study is shown in Figure 3, where we take an initial state $x(0) = 0_2$ and simulate the closed loop system behavior under u^{a} on the time interval $[0, 3/4]$. A random disturbance input $w(t) \in \mathcal{W}$ is chosen, and we choose also a candidate control policy

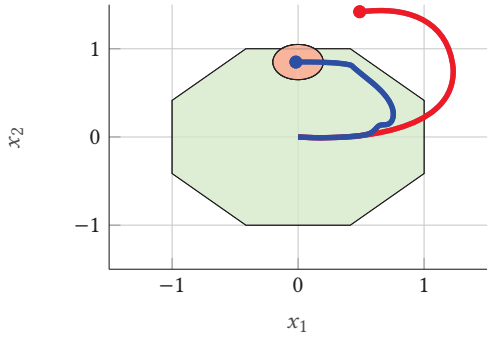
$$u^{\text{d}}(t) = \begin{bmatrix} 6\cos(\pi t) \\ 6\sin(\pi t) \end{bmatrix} \tag{48}$$

where we note that the theory and tools discussed above, which apply to state-feedback controllers $u^{\text{d}}(\mathcal{X})$, can accommodate an explicit time-dependent control policy equivalently. As shown in Figure 3a the observed set $\mathcal{X}(t)$ leaves S partially along trajectories of (45) when u^{a} is employed; however, S is robustly forward invariant for (45) as a result of Theorem 4 and we find $x(t) \in S$ for all $t \in [0, 3/4]$. This study was conducted using MATLAB 2020a, which ran on a 2017 MacBook Pro. The simulation used a discretized timestep of 0.005 seconds and, at each timestep, the optimization problem (40)-(44) was solved using Quadprog.m. The average solver time reported in this study was 0.0029 seconds per optimisation.

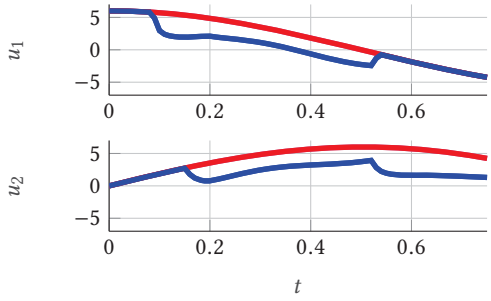
6.4 Discussion

The UECBF-QP controller, which allows for state uncertainty, is defined in (43)-(44) as an optimization problem with a quadratic cost function and $2n$ linear constraints. This is in contrast to the CBF-QP controller (15)-(16), which can retain an infinite number of linear constraints without structural assumptions on the vector field and the disturbance input w. Note also that the general theory posited in Sections 6.1–6.2 for the construction of ASIFs for systems as in (4) can be extended to the case of general polytopic safe sets by applying similar reasoning to that presented in Section 5.3; in this instance, the resulting ASIF will contain q constraints for a polytopic safe set with q faces.

Last, it is instructive also to discuss the purpose of the class-$\mathcal{K}$ function α in the programs presented in this work. We have discussed previously how in the CBF-QP controller (15)–(16), α



(a) Trajectories resulting from the application of u^a and u^d. The assured trajectory, resulting from the application of u^a is shown in blue, and the nominal trajectory, resulting from the application of u^d is shown in red. Note that the observation $\mathcal{X}(t)$ leaves S partially along trajectories of (45) when u^a is employed; nonetheless, $x(t) \in S$ for all $t \in [0,\ 3/4]$.



(b) Visualisation of the control input signals on the time interval $[0,\ t]$. The candidate input u^d, given by (48), is shown in red. The ASIF input is shown in blue.

Figure 3: Numerical demonstration. A simulation of the system (45) is conducted on the time interval $[0,\ 3/4]$, where the system begins with an initial state $x(0) = 0_2$.

is a strengthening term that relaxes the constraint (16) when the current system state $x(t)$ is far from the boundary of S. In contrast, the ASIF constraints for ECBF-QP and UECBF-QP instead require the valuation of the vector field of the embedding system to be pointing in an appropriate cone. For instance, when $\alpha(x) = 0_{2n}$ the constraint (40) requires $0_{2n} \preceq_{\mathrm{SE}} E(x,\ x)u$, *i.e.* the requirement is that $E(x,\ x)u$ points into the southeast cone. When alternative class-$\mathcal{K}$ functions α are chosen, this requirement relaxes so that u is allowed to steer $E(x,\ x)u$ into a less restrictive cone, provided $x(t)$ is not on the boundary of S.

7 CONCLUSION

In this work, we consider controlled mixed monotone systems with disturbances, and we show how controlled robustly forward invariant sets are identified by studying only the valuation of the vector field of the embedding system, without simulation. This approach provides a basic theory as to how controllers can be designed in the embedding space, and allows one to verify the existence of robustly forward invariant regions for the initial system. We study two useful applications that arise from this observation: (a) the offline verification of controllers against safety constraints, and (b) the online enforcement of safety constraints. The results and findings of this work are demonstrated through two numerical examples. The fast computation times reported in the examples here are expected to scale well to other systems; additional examples and experiments building on the theoretical foundations of this paper are the subject of ongoing work.

8 ACKNOWLEDGEMENTS

This work was supported by the Air Force Office of Scientific Research under grant FA9550-19-1-0015 and by the National Science Foundation under grant #1749357.

REFERENCES

[1] M. Abate and S. Coogan. 2020. Computing Robustly Forward Invariant Sets for Mixed-Monotone Systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*. 4553–4559. https://doi.org/10.1109/CDC42340.2020.9304461

[2] M. Abate and S. Coogan. 2020. Enforcing Safety at Runtime for Systems with Disturbances. In *2020 59th IEEE Conference on Decision and Control (CDC)*. 2038–2043. https://doi.org/10.1109/CDC42340.2020.9304203

[3] M. Abate and S. Coogan. 2021. Improving the Fidelity of Mixed-Monotone Reachable Set Approximations via State Transformations. In *2021 American Control Conference (ACC)*. IEEE. To appear. Preprint available: https://arxiv.org/abs/2010.01065.

[4] M. Abate, M. Dutreix, and S. Coogan. 2021. Tight Decomposition Functions for Continuous-Time Mixed-Monotone Systems With Disturbances. *IEEE Control Systems Letters* 5, 1 (2021), 139–144.

[5] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada. 2019. Control Barrier Functions: Theory and Applications. In *2019 18th European Control Conference (ECC)*. 3420–3431.

[6] A. D. Ames, J. W. Grizzle, and P. Tabuada. 2014. Control barrier function based quadratic programs with application to adaptive cruise control. In *53rd IEEE Conference on Decision and Control*. 6271–6278.

[7] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada. 2017. Control Barrier Function Based Quadratic Programs for Safety Critical Systems. *IEEE Trans. Automat. Control* 62, 8 (Aug 2017), 3861–3876.

[8] D. Angeli and E. D. Sontag. 2003. Monotone control systems. *IEEE Trans. Automat. Control* 48, 10 (Oct 2003), 1684–1698.

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

[10] Urs Borrmann, Li Wang, Aaron D Ames, and Magnus Egerstedt. 2015. Control barrier certificates for safe swarm behavior. *IFAC-PapersOnLine* 48, 27 (2015), 68–73.

[11] WH Clohessy and RS Wiltshire. 1960. Terminal guidance system for satellite rendezvous. *Journal of the Aerospace Sciences* 27, 9 (1960), 653–658.

[12] S. Coogan. 2020. Mixed Monotonicity for Reachability and Safety in Dynamical Systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*. 5074–5085. https://doi.org/10.1109/CDC42340.2020.9304391

[13] Samuel Coogan and Murat Arcak. 2016. Stability of Traffic Flow Networks with a Polytree Topology. *Automatica* 66, C (April 2016), 246–253. https://doi.org/10.1016/j.automatica.2015.12.015

[14] S. Coogan, M. Arcak, and A. A. Kurzhanskiy. 2016. Mixed monotonicity of partial first-in-first-out traffic flow models. In *2016 IEEE 55th Conference on Decision and Control (CDC)*. 7611–7616.

[15] T. Gurriet, M. Mote, A. D. Ames, and E. Feron. 2018. An Online Approach to Active Set Invariance. In *2018 IEEE Conference on Decision and Control (CDC)*. 3592–3599. https://doi.org/10.1109/CDC.2018.8619139

[16] T. Gurriet, M. Mote, A. Singletary, E. Feron, and A. D. Ames. 2019. A Scalable Controlled Set Invariance Framework with Practical Safety Guarantees. In *2019 IEEE 58th Conference on Decision and Control (CDC)*. 2046–2053.

[17] T. Gurriet, M. Mote, A. Singletary, P. Nilsson, E. Feron, and A. D. Ames. 2020. A Scalable Safety Critical Control Framework for Nonlinear Systems. *IEEE Access* 8 (2020), 187249–187275.

[18] Thomas Gurriet, Andrew Singletary, Jacob Reher, Laurent Ciarletta, Eric Feron, and Aaron Ames. 2018. Towards a framework for realizable safety critical control through active set invariance. In *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 98–106.

[19] C. Jewison and R. S. Erwin. 2016. A spacecraft benchmark problem for hybrid control and estimation. In *2016 IEEE 55th Conference on Decision and Control*

(CDC). 3300–3305. https://doi.org/10.1109/CDC.2016.7798765

[20] P. Meyer and D. V. Dimarogonas. 2019. Hierarchical Decomposition of LTL Synthesis Problem for Nonlinear Control Systems. *IEEE Trans. Automat. Control* 64, 11 (Nov 2019), 4676–4683. https://doi.org/10.1109/TAC.2019.2902643

[21] Pierre-Jean Meyer, Alex Devonport, and Murat Arcak. 2019. TIRA: Toolbox for Interval Reachability Analysis. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '19)*. Association for Computing Machinery, 224–229. https://doi.org/10.1145/3302504.3311808 An extended version of this work appears on ArXiv https://arxiv.org/abs/1902.05204.

[22] Mitio Nagumo. 1942. Über die lage der integralkurven gewöhnlicher differentialgleichungen. *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series* 24 (1942), 551–559.

[23] A. Saoud, E. Ivanova, and A. Girard. 2019. Efficient Synthesis for Monotone Transition Systems and Directed Safety Specifications*. In *2019 IEEE 58th Conference on Decision and Control (CDC)*. 6255–6260.

[24] H.L. Smith. 2008. *Monotone Dynamical Systems: An Introduction to the Theory of Competitive and Cooperative Systems.* American Mathematical Society.

[25] Hal L Smith. 2006. The discrete dynamics of monotonically decomposable maps. *Journal of Mathematical Biology* 53, 4 (2006), 747.

[26] Li Wang, Aaron D Ames, and Magnus Egerstedt. 2017. Safe certificate-based maneuvers for teams of quadrotors using differential flatness. In *2017 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 3293–3298.

[27] L. Yang, O. Mickelin, and N. Ozay. 2019. On Sufficient Conditions for Mixed Monotonicity. *IEEE Trans. Automat. Control* 64, 12 (Dec 2019), 5080–5085.