MIXED MONOTONICITY FOR EFFICIENT REACHABILITY WITH APPLICATIONS TO ROBUST SAFE AUTONOMY

A Dissertation
Presented to
The Academic Faculty

By:

Matthew Christian Licciardi Abate

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in Robotics,
School of Mechanical Engineering

Georgia Institute of Technology

August 2022

MIXED MONOTONICITY FOR EFFICIENT REACHABILITY WITH APPLICATIONS TO ROBUST SAFE AUTONOMY

Approved by:

Dr. Samuel Coogan, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Eric Feron, Advisor
School of Electrical and Computer Engineering
King Abdullah University of Science and Technology

Dr. Mattheiu Bloch
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Panagiotis Tsiotras
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Yorai Wardi
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: July 19, 2022

To Infinity and Beyond!

Buzz Lightyear

ACKNOWLEDGEMENTS

This thesis would not have been possible if not for my exceptional research advisors, Sam Coogan and Eric Feron. They are both impassioned and supportive teachers who consistently encouraged my research and interests, and I have only deep-seated gratitude for their mentorship and friendship over the last five years.

Sam always made himself available to talk about my research interests, which were quite scattered when I began in his lab in 2018. My growth as a researcher was largely due to the fact that he encouraged me to follow these interests while steering my enthusiasm constructively toward practical and meaningful projects. Sam fostered my development as a researcher and significantly improved the quality of my work. I'll remember fondly writing my first paper on mixed monotone systems with him over muffins and yogurt at the Nice airport. That paper later became the catalyst for this entire thesis.

Eric has looked out for my success from our first interaction, which was a full year before I joined his lab. When I joined the DCL, he provided for me a wonderful and inviting research environment, and he introduced me to many of my now closest friends and research collaborators. Eric was a true mentor in my development as a researcher, sparking my interest constantly through regular conversations that touched every area of mathematics. I am deeply grateful for the faith that he put in me, and I would like to thank here also, Max-Daniel Sokollek, who went out of his way to make my introduction to Eric.

I would like to thank my dissertation advisory committee, Matthieu Bloch, who is responsible for the wonderful whiteboard seminars in the DCL; Panos Tsiotras, who provided the hardware and lab equipment used in this thesis' experiments; and Yorai Wardi, who would stop to engage me around the fourth floor of TSRB and excite me with deep theoretical presented eloquently and simply.

I would like to thank the other students in the DCL for being wonderful friends and collaborators throughout this program. I'll remember fondly studying for candidacy exams on the weekends with Mark Mote, in the office, in pajamas, and also doing math on the whiteboards of vacant faculty offices with Ben Mains. I would like to thank Corbin Klett, Kevin Garanger, and Thanakorn Khamvilai, as well as Mark and Ben, for being excellent roommates as well as labmates in Atlanta. I would like to thank Kerianne Hobbs and Max Dutreix who were senior graduate students when I joined the DCL and who both provided a lot of early advice and encouragement. Also, I would like to thank Saber Jafapoor who was able to excite me with new ideas and applications for my research when I was more senior.

I would like to thank my friends from outside of the DCL—George, Ian, Bishop, Derek, Taylor, and Mohammad—as well as those outside of Georgia Tech. In particular, I would like to thank my girlfriend Cecie for her love, support, and constant cheerfulness; my Ph.D. was at times stressful, but Cecie, and her roommate Ellie, would consistently find ways to foster my optimism. I would also like to thank my friends Raph, Henry, John, Tyler, Will, Alex, Shannon, and Harrison.

Finally, I would like to thank my family for their love and support throughout this program: my parents Mark and Pia, as well as my three siblings, Mark, Chatham, and Paula. Thank you all for visiting me often, so far away from home. Last, I would like to acknowledge the role that my grandfather, John, played in my development as a researcher and mathematician; Pop passed away during my second year at Georgia Tech. He had a Ph.D. in electrical engineering, researched dynamical systems, and was a main inspiration for me in my study of mathematics.

Thank you all!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Summary

Reachability analysis of control systems plays a crucial role in system verification and controller synthesis. However, many reachability techniques fall short, being only applicable to certain classes of systems or too computationally burdensome for real-time applications. The subject of this thesis is the mixed monotonicity property of dynamical systems which is known to be a general property and which provides a computationally efficient technique for over-approximating reachable sets using hyperrectangles. Specifically, the mixed monotonicity of a dynamical system is tied to the existence of a related decomposition function that separates the system's vector field into cooperative and competitive state interactions. Reachable sets for the mixed monotone system can then be computed simply using a decomposition function and foundational results from monotone dynamical systems theory.

In this thesis, we establish that all continuous-time dynamical systems bearing a locally Lipschitz continuous vector field are mixed monotone and we provide a construction for the unique tight decomposition function of a dynamical system that attains the tightest possible over-approximations of reachable sets. We then provide a suite of new analysis tools for mixed monotone systems that can be applied to attain, for example, over- and under-approximations of both forward- and backward-time reachable sets, and also robustly forward invariant sets. As a final point, we study conservatism in mixed monotone reachable set approximations, and we provide new tools for reducing conservatism using, for example, the decomposition function of a separate dynamical system, formed via a transformation of the initial system's vector field. We conclude with a case study of a five-dimensional spacecraft system and a hardware demonstration of in-the-loop reachability analysis and enforced system safety. Numerous illustrative numerical examples are also provided.

CHAPTER 1

INTRODUCTION

The fields of Physics and Calculus were fathered by the same man to solve the same problem: the man was Sir Isaac Newton and the problem was to *predict* the future motion of the planets. Newton's main insight was that the time-varying properties of an object in the physical world can be modeled using a mathematical tool called the *differential equation*. Systems of differential equations, *i.e.*, dynamical systems, appear as equations of motion and solutions to these equations provide an estimate of future real-world behavior.

While planetary trajectories have well understood dynamical models allowing for accurate predictions [1, 2], many active research areas still focus on predicting future phenomena: for example, traffic [3] and weather patterns [4, 5], on the larger-scale, and robotic behavior [6], on the smaller-scale. For robotic systems, accurate prediction is necessary in safety applications [7, 8], however, unlike with planetary dynamics, often times the physical phenomena effecting a robot's motion are poorly understood. Indeed, a main problem in this approach is in identifying a suitable dynamical model of a system and, when a poor model is employed, the mathematical predictions derived from the model may deviate quickly from true real-world behavior [9]. One method for addressing this limitation is to instead consider a dynamical model that explicitly considers uncertainties and environmental effects within the differential equation. Stochastic [10], hybrid [11, 12] and nondeterministic dynamical models [5] have all been employed for this purpose.

In this thesis, we concern ourselves mainly with continuous-time dynamical systems subject to nondeterministic disturbance inputs. While individual solutions to such systems are computable using simulation of the dynamics, the addition of the disturbance generally prevents robust time-domain analysis using simulation alone. One particular problem of interest involves computing a system's reachable set, which is the set of possible final states of the system, given some set of inital conditions and certain metrics on the class of disturbances under consideration. Generally speaking, it is difficult to compute reachable sets exactly, even in low state dimensions, since they often exhibit complex and nonstandard geometries that are not always easily discernible from the system's vector field [13].

Instead, many efficient algorithms exist for computing *over-approximations* of reachable sets; see [14, Chapter 29] for short a review. Such over-approximations have principal use cases in system verification [15, 16] and safety [8, 17], since they can be used to reason about, for example, whether system trajectories will *always* remain in a safe region of the state space or *eventually* reach an unsafe region. Moreover, over-approximations of reachable sets are generally constructed mathematically to exhibit some special geometry or property, as to make them easy to compute and reason about; see, for example, [18], which deals with elliptical reachable set over-approximations for linear time-varying system. In this thesis, we mainly study the problem of computing a *hyperrectangular* over-approximation of a system's reachable set from an initial set of states that is also a hyperrectangle. Indeed, numerous efficient techniques exist for over-approximating reachable sets using hyperrectangles, many of which scale nicely with the dimensionality of the system [19, 20].

One foundational theory in this area is that of *monotone* dynamical systems. State trajectories of a monotone system exhibit an ordering property [21, 22], and this ordering creates a useful procedure for over-approximating reachable sets using hyperrectangles; in the special instance that a system is monotone, the tightest hyperrectangle containing a reachable set can be computed simply using two simulations of the initial system dynamics. Computing small numbers of system simulations in this way is generally a computationally unintensive task, and the main benefit of employing the monotonicity property for, *e.g.*, reachability analysis, lies in this efficiency. Despite these advantages, it should be noted that monotonicity poses a fairly restrictive assumption on the system's vector field, and more general techniques are needed to solve the reachability analysis problem in the general setting of continuous-time nondeterministic systems.

A related approach, that applies more generally, involves attempting to embed the vector field of an initial nonmonotone system in a higher-dimensional *embedding system* with monotone dynamics. Indeed, this is an old idea—especially in the discrete-time setting, where convergent iteration algorithms were developed as early as 1959 using a similar monotone embedding [23]. Nonetheless, the power of this theory becomes most revealing when placed in the context of monotone dynamical systems, as studied and advanced more recently in [24–28]. The primary focus of these works is in studying the stability of equilibria for dynamical systems without disturbances. This thesis takes a different approach and studies how such a monotone embedding can facilitate efficient reachability analysis for systems with disturbances, as emphasized and advanced more recently in [29]. Moreover, embedding a dynamical system's vector field a higher-dimensional monotone embedding system is the main idea behind the *mixed monotonicity* property of dynamical systems [30].

A dynamical system is mixed monotone if there exists a related *decomposition function* that decomposes the system's vector field into cooperative and competitive state interactions; a result that has been applied in the context of continuous-time systems [25, 27, 28, 31, 32], discrete-time systems [26], and systems with disturbances [29, 33, 34]. In particular, the vector field of an inital n-dimensional mixed monotone system can be embedded in a related $2n$-dimensional embedding system—via the decomposition function—and this embedding system will not contain a disturbance input even in the case where the initial system is nondeterministic. Furthermore, the embedding system is monotone with respect to a particular southeast cone and tools from monotone systems theory can be applied to the embedding system to conclude properties of the original dynamics; in particular, such approaches are useful for efficient reachability analysis [30] and for the explicit identification of robustly forward invariant sets [35, 36]. For the case without disturbances, see also [37, 38] for stability analysis via mixed monotonicity, [26] for reachability analysis, and [39, 40] for formal verification and synthesis.

One canonical reachability analysis tool for mixed monotone systems facilitates computing a hyperrectangular over-approximation of a system's reachable set, from an initial set which is also a hyperrectangle. The initial hyperrectangle is parameterised by a vector in $2n$ coordinates, and a simulation of the embedding system for time horizon t identifies a hyperrectangle containing the systems t-time-unit forward reachable set, where the largest and smallest points in the rectangular approximation are taken to be the first n and last n coordinates of the simulation endpoint. This result has been applied in discrete-time [29, 34] and in continuous-time [33, 34] for the efficient over-approximation of reachable sets using hyperrectangles.

In this thesis, we also study the mixed monotonicity property of dynamical systems and we contribute to its theory in three main ways:

- First, we study the **generality** of the mixed monotonicity property and we show, in particular, that every continuous-time dynamical systems bearing a locally Lipschitz continuous vector field is mixed monotone. We observe that an arbitrary dynamical system will generally be mixed monotone with respect to many different decomposition functions, and that certain decomposition function may provide more or less conservative reachable set over-approximations than others when used with the tools of mixed monotonicity. To that end, we provide a construction for the unique *tight decomposition function* of a system that provides the tightest attainable reachable set approximations, and this construction is applicable to any dynamical system bearing a locally Lipschitz continuous vector field. Our contributions in this area are based mainly on the papers [41, 42].

- Next, we study the **applicability** of the mixed monotonicity property, and we present a suite of new reachability analysis tools for mixed monotone systems. In particular, we provide tools for computing, over- and under-approximations of forward- and backward-time reachable sets for mixed monotone systems, and also tools for computing robustly forward invariant sets. Our contributions in this area are based mainly on the papers [35, 36, 41].

- Finally, we study the **conservatism** inherent in mixed monotone reachable set approximations, and we provide a general theory as to how conservatism enters the reachability approach. Further, we show how it is sometimes possible to apply the tools of mixed monotonicity to a second, *transformed*, dynamical system in order to attain tighter reachable set approximations for the inital system than are attainable directly from its own tight decomposition. Our contributions in this area are based mainly on the papers [42, 43].

Following these discussions and results, at the end of this thesis, we provide two concluding case studies where we demonstrate the use of mixed monotonicity for verifying and enforcing safety properties on complex dynamical systems. In particular, we consider applications to ground robotics [17] and spacecraft systems [44]. We refer the reader also to [45–49], which are by the author, and which deal also with verification and enforced safety of dynamical systems. Further, see [50, 51].

1.1 Contributions

The first main result of this thesis is to show that all continuous-time systems bearing a locally Lipschitz continuous vector field are mixed monotone. We observe, in particular, that an arbitrary dynamical system will usually be mixed monotone with respect to many *different* decomposition functions, however, it may be the case that certain decomposition functions for a system provide less-conservative reachable set approximations than others when used with the tools of mixed monotonicity. These observations motivate the need for new methods of obtaining decomposition functions and reasoning about their *tightness*. Indeed, analogous to searching for Lyapunov functions, constructing closed-form decomposition functions for complex systems can be difficult, and there do not exist universal techniques for doing so.

One classical approach for constructing decomposition functions—that is known to be broadly applicable [31]—involves using single-sided bounds on a system's Jacobian matrices [29, 34, 35]. Such decomposition functions can generally be obtained and evaluated simply, thus aiding in applications where, *e.g.*, decomposition functions need be constructed on-the-fly for high-dimensional nonlinear systems; see [52] for an application of this kind in machine learning. Despite these advantages, Jacobian bounds are generally understood to produce overly-conservative decomposition functions, except in a few, albeit important, special cases, such as when the inital system is linear time-invariant or admits sign-stable Jacobian matrices [53]. See also [54].

Conservatism in mixed monotone reachable set approximations was first studied in [55], in a discrete-time setting, where it was shown that all discrete-time systems are mixed monotone with respect to a unique *tight decomposition function* that can be applied to compute the tightest hyperrectangle containing a system's 1-step reachable set. This tight decomposition function is defined as an optimization problem and evaluating the decomposition function at any point in the embedding space requires explicitly computing or reasoning about the reachable set itself. For this reason, tight decomposition functions in discrete-time do not provide many practical benefits in solving the reachability analysis problem; however, knowing that a decomposition function does exist means that a search directed by, *e.g.*, domain expertise [32], is not generally unreasonable.

This thesis mainly studies continuous-time systems and we present a basic theory of *how* conservatism enters the reachability analysis procedure. Unlike in the discrete-time setting, continuous-time mixed monotonicity cannot generally be applied to compute the tightest hyperrectangle containing a reachable set, except in certain special cases such as when a system is monotone. Nonetheless, we prove an analogous result by providing a construction for a similar *tight decomposition function* that provides the tightest approximations of reachable sets attainable when used with the continuous-time mixed monotonicity tools. Our construction is similarly defined as an optimization problem, however, unlike in the discrete-time setting, computing a tight decomposition function for a continuous-time system does not require computing or reasoning about the system's reachable set explicitly. This distinction makes it so that tight decomposition functions are significantly easier to evaluate in the continuous-time setting and we show through a series of examples how, in certain instances, a tight decomposition function may be attained in closed-form.

After establishing the generality of the mixed monotonicity property, we next present a suite of new reachability analysis tools for a mixed monotone systems, and we study complex system properties beyond simple forward-time reachability. Indeed, we have discussed already how the decomposition function of a mixed monotone system facilitates the efficient over-approximation of reachable sets using hyperrectangles. As second main result in this thesis, we show how this *same* decomposition can be used with broader applicability in systems' analysis.

In particular, we show how the decomposition function of a mixed monotone system enables one to compute also (i) over-approximations of *backward-time reachable sets* for the inital forward-time system, and (ii) *under-approximations* forward-time reachable sets. Our approach in these matters involves constructing a decomposition function for a corresponding set of *backward-time dynamics*, however we show how such a backward-time decomposition function can be immediately identified from a decomposition function for the forward-time dynamics. In this way, one will only ever need to construct a single decomposition function to apply the tools herein. Furthermore, we move beyond finite-time reachability analysis and study also time-invariant system properties using mixed monotonicity. A particular problem of interest involves computing *robustly forward invariant sets* for systems with disturbances; such forward invariant sets have principal use cases in safety for autonomous robotics, since they can be used to reason about system trajectories on an infinite-time horizon [17, 47–49]. To that end, we show how robustly forward invariant sets for mixed monotone systems can be efficiently identified from the *equilibria* of the deterministic embedding system. Indeed, the embedding system of a mixed monotone system can induce stable—or even globally stable—equilibria, and we show also how stability analysis in the embedding space can be used to reason about the attractivity of the invariant sets derived using our approach. As a final tool, we show also how robustly forward invariant sets for mixed monotone systems can be identified from closed periodic orbits in the embedding space.

Finally, we provide a more in-depth analysis of conservatism in mixed monotone reachable set approximations and we present new tools for assessing and reducing conservatism in these approximations. We recall that, given a tight decomposition function for some system, there will not exist another decomposition function for the same system that provides tighter reachable set approximations when used directly with the tools of mixed monotonicity. However, it is true that a tight decomposition function may be only provide conservative reachable set approximations and it is natural to wonder whether conservatism can be reduced using other means. To that end, as a final main result, we show how it is sometimes possible to reduce conservatism in the approximation of reachable sets by considering an *alternative* tight decomposition function corresponding to a transformed set of mixed monotone dynamics.

Reducing conservatism in mixed monotone reachable set approximations via state transformations is a main focus of other works, including [43], which is by the authors, and where it is shown that conservatism can sometimes be reduced by considering mixed monotonicity defined with respect to an alternative partial order on the system's state space. In particular, the authors show how it is sometimes possible to construct a second mixed monotone system, via a *linear transformation* on the statespace of the initial dynamics, and how it is possible to apply the tools of mixed monotonicity to the transformed system in order to attain a *parallelotope* reachable set approximation for the inital (untransformed) dynamics. This approach has also been applied in other works, including [42, 49], in order to attain tighter reachable set approximations using the tools of mixed monotonicity.

In this thesis, we also study how state-transformations can be used to compute higher fidelity reachable set approximations via mixed monotonicity, however, we take a different approach in our analysis. We begin by studying the case where two different mixed monotone systems, with different tight decomposition functions and disturbance spaces, admit the same deterministic embedding system. In this case, the hyperrectangular reachable set approximations will be equal for both systems, for any prediction horizon, even when, *e.g.*, the true reachable set of one system contains that of the other. This analysis aids in the understanding of how conservatism enters the mixed monotone approach and can be used to suggest whether, for some system, the application of mixed monotone systems theory will produce only overly-conservative reachable set approximations. Following this discussion, we next apply our observations and develop tools to reduce excess conservatism in mixed monotone reachable set approximations. Motivated by [43], our approach is to apply the tools of mixed monotonicity to a new dynamical system, constructed via a state transformation on the inital, untransformed, dynamics. Linear transformations, nonlinear transformations, time-varying transformations and state-augmentations are all considered. Furthermore, we provide numerous examples demonstrating the applicability of our approach, to systems such as a 7-dimensional nonlinear spacecraft system and a controlled nonlinear pendulum model.

We provide also, at the end of this thesis, two larger case studies where we apply mixed monotone systems theory in order synthesize safe-by-construction controllers for controlled mixed monotone systems. We present, in particular, two constructions for *run time assurance mechanisms* [56], that enforce system safety online by filtering a performance control input within the control-loop. In our first example, we use mixed monotonicity based reachability methods, together with control barrier functions [57], in order to design a run time assurance architecture for a controlled vehicle platoon model. In our second example, we present the development and testing of a real-world run time assurance mechanism for a torque-controlled spacecraft in free rotational motion. The practicality of the approach is demonstrated in with an application on the Autonomous Spacecraft Testing of Robotic Operations in Space (ASTROS) platform [58], at the Georgia Institute of Technology, and a video of the experiment is available at `https://youtu.be/g1-zMepDm1I`.

1.2 Preview of Thesis

This thesis is written in six chapters as detailed more thoroughly bellow:

Chapter 2 serves as a preliminary tutorial on the theory of mixed monotone dynamical systems; see Figure 1.1. We begin with a discussion on the reachability analysis problem for dynamical systems in Section 2.1, and we present the monotonicity property of dynamical systems in Section 2.2. Monotonicity is shown to produce an efficient procedure for over-approximating the reachable set of a dynamical system using a hyperrectangle, however, the conditions on monotonicity are fairly restrictive and later, in Section 2.4, we introduce the mixed monotonicity property which applies more generally. Before this study, we present a discussion on the southeast order, in Section 2.3, which is crucial in the understanding of mixed monotonicity. Numerous examples are provided throughout to guide the reader in understanding mixed monotonicity and the tools on which the theory is built. In particular, a mixed monotone system will be mixed monotone with respect to a related *decomposition function* that separates the system dynamics into cooperative and competitive state interactions and, in Section 2.5 of this thesis, we present a brief discussion on the application of mixed monotonicity and on the construction of decomposition functions. Finally,

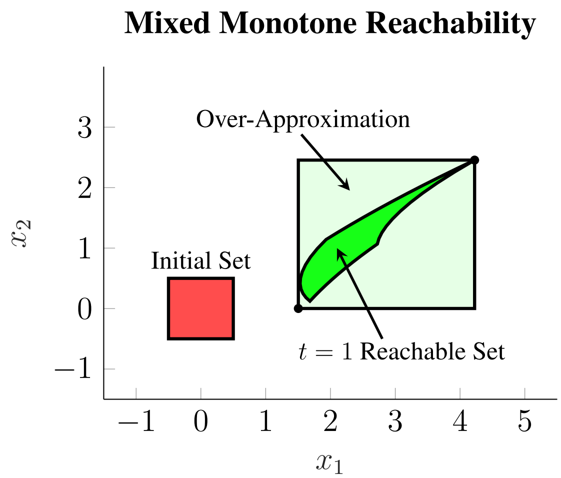


Figure 1.1: Chapter 2 serves as a preliminary tutorial on the theory of mixed monotone dynamical systems. A dynamical system is mixed monotone when there exists a related decomposition function that separates a systems dynamics into cooperative and competitive state interactions, and this decomposition function can then be used to compute a hyperrectangular over-approximation of a system's reachable set.

we present a few related notions and tools, in Section 2.6, for over-approximating the reachable set of a system using hyperrectangles.

In Chapter 3 we present a more formal theory on *how* decomposition functions are constructed for mixed monotone systems and, in doing so, we reveal the generality of the mixed monotonicity property; see Figure 1.2. We begin, in Section 3.1, by introducing the *kinematic unicycle model* dynamics which will become a primary case study in the chapter; throughout, we present several different methods for decomposing the unicycle dynamics, and we compare each of the decomposition functions obtained in terms of their conservatism and and their computational complexity. As a first technique, we show in Section 3.2 how decomposition functions can sometimes be constructed from single-sided bounds on the system's Jacobian matrices. An important observation made in this section is that, generally speaking, many different decomposition functions for the same system can be produced using Jacobian-bounds, and this observation motivates the need for new techniques of obtaining and reasoning about decomposition functions. To address this point, we provide, in Section 3.3, a basic theory of how conservatism enters the reachability analysis procedure for mixed monotone systems. Then, following this theory, we show in Section 3.4 that all

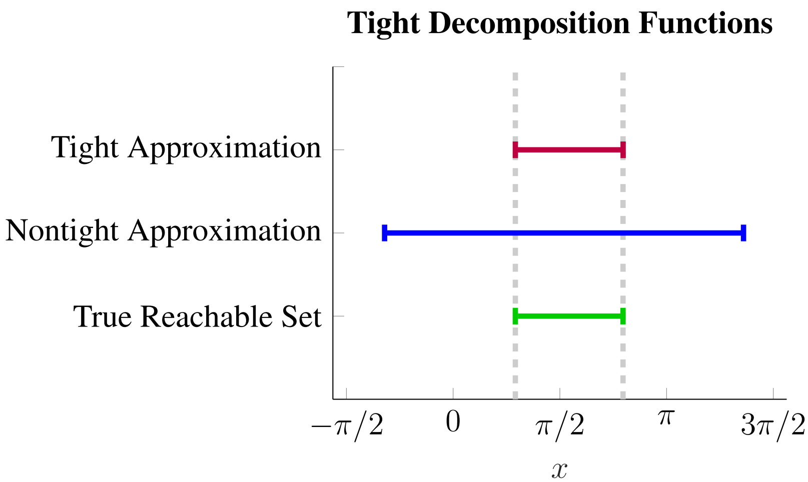


Figure 1.2: In Chapter 3 we show that all continuous-time dynamical systems bearing a locally Lipschitz continuous vector field are mixed monotone, and we present several techniques for constructing decomposition functions. Certain decomposition functions may provide more or less conservative reachable set approximations than others when used with the tools of mixed monotonicity. To that end, we present a construction for the unique *tight decomposition function* that provides the tightest attainable reachable set approximations.

continuous-time dynamical system, possibly subject to a disturbance input, are mixed monotone and we provide an explicit construction for the unique *tight decomposition function* that provides the tightest attainable approximations of reachable sets. Our construction is presented, initially, as a nonconvex optimization problem evaluated over a hyperrectangular set of states. However, we show through numerous examples how tight decomposition functions can sometimes be computed in closed-form and, in Section 3.5, we present a basic method for obtaining closed-form representations. A concluding case study is presented in Section 3.6 where we apply our results to compute a tight decomposition function for a 4-dimensional nonlinear bicycle model.

Next, in Chapter 4, we present a suite of new analysis tools for a mixed monotone systems, and we study complex system properties beyond simple forward-time reachability; see Figure 1.3. The first part of Chapter 4, Section 4.1, deals with extending the reachability analysis techniques introduced previously in Chapter 2. From the initial dynamics of a mixed monotone system, we construct a backward-time dynamical model in Section 4.1.1 and we show how forward-time reachability on the backward-time model allows for over-approximating backward-time reachable sets for the inital forward-time dynamics. This backward-time model is also employed in Section 4.1.2

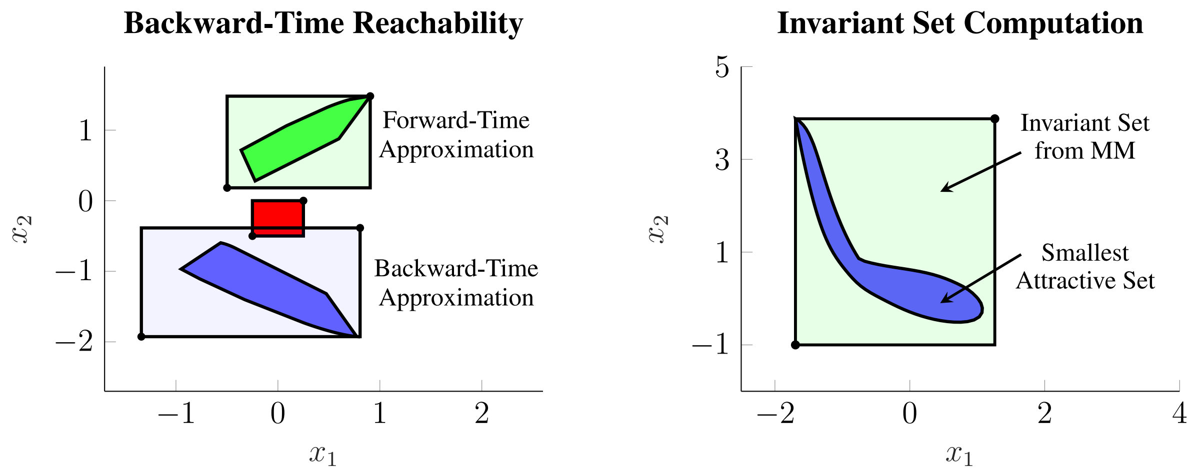


Figure 1.3: In Chapter 4 we present tools for computing over- and under-approximations of forward- and backward-time reachable sets, and also tools for computing robustly forward invariant sets for mixed monotone systems.

for the under-approximation of forward-time reachable sets for the initial dynamics. Finally, in Section 4.1.3, we attempt to summarise our previous results through a cohesive theory as to how reachable sets can be efficiently under and over-approximated for mixed monotone systems using a single decomposition function for the forward-time dynamics. The second part of Chapter 4, Section 4.2, studies how robustly forward invariant sets for mixed monotone system can be efficiently identified from invariant sets in the embedding space. Two main kinds of invariant sets for the embedding system are considered: (i) *equilibria* for the embedding system are studied in Section 4.2.1 and such equilibria can be used to identify hyperrectangular invariant sets for the initial system, and (ii) *closed periodic orbits* for the embedding system are studied in Section 4.2.3, and such periodic orbits can be used to identify invariant sets for the initial system with more complex geometries. An intermediary discussion is also provided in Section 4.2.2.

In Chapter 5, we further study conservatism in mixed monotone reachable set approximations and we present new tools for reducing conservatism via transformations of the initial system state space; see Figure 1.4. Given a tight decomposition function for some system, there will not exist another decomposition function for the same system that provides tighter reachable set approximations when used directly with the tools of Chapter 4; however, it is true that a tight decomposition function may be only provide conservative reachable set approximations. To that end, in Chap-

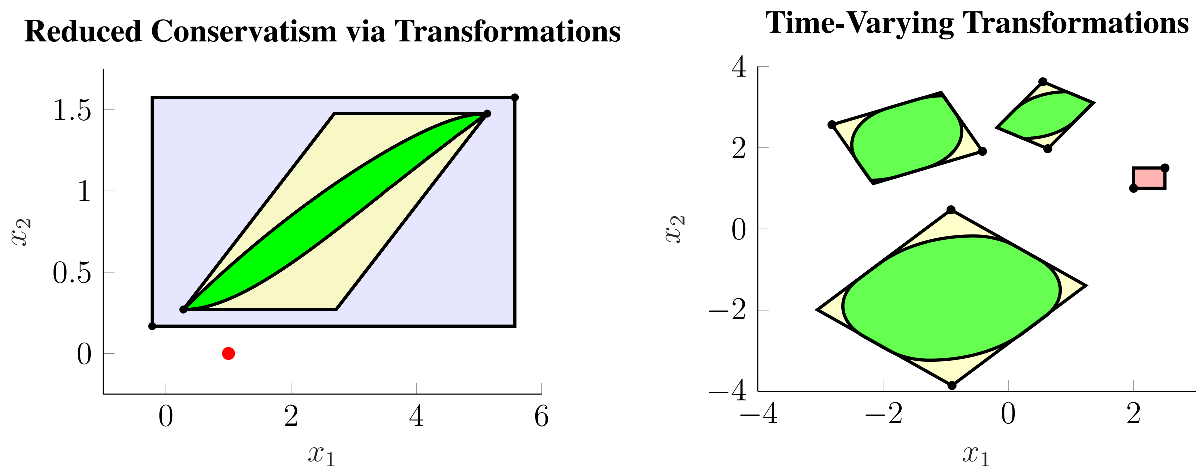
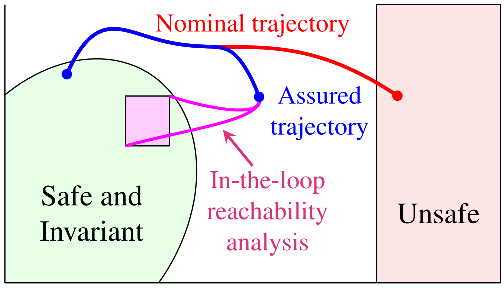


Figure 1.4: In Chapter 5, we further study conservatism in mixed monotone reachable set approximations and we present new tools for reducing conservatism via transformations of the initial system state space. Linear transformations, nonlinear transformations, time-varying transformations and state-augmentations are all considered.

ter 5, we study *how* conservatism enters the reachability analysis procedure, and we present several general methods for reducing conservatism in reachable set approximations. We begin with a discussion on conservatism in mixed monotone reachable set approximations in Section 5.1. Our discussion is presented through a series of examples, and we revisit these examples later in the chapter where we show how sometimes conservatism can be reduced by considering an *alternative tight decomposition function* corresponding to a state-transformation of the initial system dynamics. Linear, nonlinear, and time-varying transformations are studied in Sections 5.2, 5.4 and 5.5, respectively. Furthermore, we present an extended example in Section 5.3, where we consider a 7-dimensional nonlinear spacecraft system and where we demonstrate how a linear transformation of the dynamics allows for tighter reachable set approximations via mixed monotonicity. As a final approach, we show in Section 5.6 how it is sometimes possible to augment the state vector of a nonlinear system, with redundant state variables, in order to further reduce conservatism in the approximation of reachable sets.

We provide also, at the end of this thesis, two concluding case studies in Chapter 6, where we apply mixed monotone systems theory in order to verify and enforce safety properties on complex dynamical systems; see Figure 1.5. In Section 6.1, we use mixed monotonicity based reachability



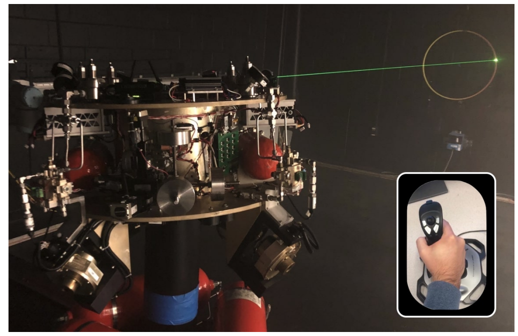


Figure 1.5: In Chapter 6, we apply mixed monotone systems theory, in order to verify and enforce safety and robustness properties on complex systems. As a particular application, we present two run time assurance architectures, that act as safe controllers, and which enforce system safety online via mixed monotone reachability analysis within the control-loop.

methods, together with control barrier functions, in order to design a run time assurance architecture for controlled dynamical systems with disturbances. The results and tools generated in this study are demonstrated though an example in Section 6.1.3 where we synthesize a safe controller for a vehicle platoon model using this approach. Next, in Section 6.2, we present the development and testing of a run time assurance mechanism for a torque-controlled spacecraft in free rotational motion. The practicality of the approach is demonstrated in with an application on a hardware testbed: the Autonomous Spacecraft Testing of Robotic Operations in Space (ASTROS) platform, at the Georgia Institute of Technology.

The code that accompanies this dissertation and generates the figures is publicly available through GitHub: `https://github.com/gtfactslab/Abate_Thesis`.

1.3 Mathematical Notation and Conventions

We denote the set of real numbers by $\mathbb{R}$ and the extended real numbers by $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$. We denote by $\mathbb{R}_{>0}$, $\mathbb{R}_{<0}$, $\mathbb{R}_{\geq 0}$ and $\mathbb{R}_{\leq 0}$ the sets of positive, negative, non-negative, and non-positive reals, respectively, and we extend this notation to $\overline{\mathbb{R}}$ as well, so that, *e.g.*, $\overline{\mathbb{R}}_{\geq 0} := \mathbb{R}_{\geq 0} \cup \{\infty\}$.

We denote by $I_n \in \mathbb{R}^{n\times n}$ the $n \times n$ identify matrix, and by $0_{n\times m} \in \mathbb{R}^{n\times m}$ an $n \times m$ matrix fully populated with 0's. When the dimensionality of a matrix is clear from context, we sometimes drop the subscript notation and use, *e.g.*, I to denote the $n \times n$ identify matrix.

Given vectors $x^1 \in \mathbb{R}^{n_1}$, $x^2 \in \mathbb{R}^{n_2}$, $\cdots$, $x^m \in \mathbb{R}^{n_m}$, we denote by

$$(x^1, x^2, \cdots, x^m) := \begin{bmatrix} x^1 \\ x^2 \\ \vdots \\ x^m \end{bmatrix} \in \mathbb{R}^{n_1+n_2+\cdots+n_m} \tag{1.1}$$

their vector concatenation. Vector and matrix entries are given via subscript, *i.e.*, x_i denotes the i^{th} entry of $x \in \mathbb{R}^n$ and $A_{i,j}$ denotes the i, j^{th} entry of $A \in \mathbb{R}^{n \times m}$. To denote collections of elements within a vector or matrix, we use $x_{i:j} \in \mathbb{R}^{j-i+1}$ to denote the i-through-j^{th} elements of $x \in \mathbb{R}^n$ and $A_{i,:} \in \mathbb{R}^{1 \times m}$ to denote the i^{th} row of $A \in \mathbb{R}^{n \times m}$:

$$\begin{aligned} x_{i:j} &:= (x_i, x_{i+1}, \cdots, x_{j-1}, x_j) \\ A_{i,:} &:= [A_{i,1}\,,\ A_{i,2}\,, \cdots,\ A_{i,m-1}\,,\ A_{i,m}]. \end{aligned} \tag{1.2}$$

Given $x \in \mathbb{R}^n$, we denote by $x_{-i} \in \mathbb{R}^{n-1}$ the vector x but where the i^{th} entry has been removed,

$$x_{-i} := (x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n) \tag{1.3}$$

and, given also $y \in \mathbb{R}^n$, we denote by $x_{[i:y]} \in \mathbb{R}^n$ the vector x but where the i^{th} entry has been replaced by the i^{th} entry of y,

$$x_{[i:y]} := (x_1, \cdots, x_{i-1}, y_i, x_{i+1}, \cdots, x_n). \tag{1.4}$$

The componentwise vector order is denoted $\preceq$, so that given $x, y \in \mathbb{R}^n$ we say $x \preceq y$ if and only if $x_i \leq y_i$ for all i. In the special instance where $x \preceq y$, we let

$$[x, y] := \{z \in \mathbb{R}^n \mid x \preceq z \text{ and } z \preceq y\} \tag{1.5}$$

denote the hyperrectangle defined by the endpoints x and y and we let

$$\langle x, y\rangle := \{z \in \mathbb{R}^n \mid z_i \in \{x_i, y_i\}\} \tag{1.6}$$

denote there finite set of 2^n corners of $[x,y]$. Given $a = (x,y) \in \mathbb{R}^{2n}$ with $x \preceq y$, we denote by $[\![a]\!] := [x,y]$ the hyperrectangle formed by the first n and last n components of a and, likewise, $\langle\!\langle a \rangle\!\rangle := \langle x,y \rangle$. Given an interval $[x,y] \subset \mathbb{R}^n$, we denote by

$$\begin{aligned} [x,y]^2 &:= [x,y] \times [x,y] \\ &:= \left\{ (z^1, z^2) \in \mathbb{R}^n \times \mathbb{R}^n \,\middle|\, z^1 \in [x,y] \text{ and } z^2 \in [x,y] \right\}, \end{aligned} \tag{1.7}$$

and, by analogy, $[x,y]^3 := [x,y] \times [x,y] \times [x,y]$.

Given $A \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{n \times m}$ we denote by $A^{\mathrm{M}+}, A^{\mathrm{M}-} \in \mathbb{R}^{n \times n}$ the *Metzler* and *non-Metzler* parts of A, respectively, and by $B^+, B^- \in \mathbb{R}^{n \times m}$ the non-negative and non-positive parts of B:

$$\begin{aligned} A^{\mathrm{M}+}_{i,j} &:= \begin{cases} A_{i,j} & \text{if } A_{i,j} \geq 0 \text{ or } i = j \\ 0 & \text{if } A_{i,j} \leq 0 \text{ and } i \neq j, \end{cases} & A^{\mathrm{M}-}_{i,j} &:= \begin{cases} A_{i,j} & \text{if } A_{i,j} \leq 0 \text{ and } i \neq j \\ 0 & \text{if } A_{i,j} \geq 0 \text{ or } i \neq j, \end{cases} \\ B^{+}_{i,j} &:= \begin{cases} B_{i,j} & \text{if } B_{i,j} \geq 0 \\ 0 & \text{if } B_{i,j} \leq 0, \end{cases} & B^{-}_{i,j} &:= \begin{cases} B_{i,j} & \text{if } B_{i,j} \leq 0 \\ 0 & \text{if } B_{i,j} \geq 0. \end{cases} \end{aligned} \tag{1.8}$$

Observe that $A = A^{\mathrm{M}+} + A^{\mathrm{M}-}$ and $B = B^+ + B^-$. We sometimes abuse notation here, and refer to B^+, B^- simply as the positive and negative parts of B, respectively. A matrix B is said to be a *positive matrix* when $B = B^+$, and a *negative matrix* when $B = B^-$.

CHAPTER 2

PRELIMINARIES ON MIXED MONOTONE SYSTEMS THEORY

This chapter presents the mixed monotonicity property of dynamical systems, which provides many useful tools for systems' analysis as described below:

We concern ourselves mainly with continuous-time dynamical systems subject to disturbance inputs. While individual solutions to such systems are computable using simulation of the dynamics, the addition of the disturbance generally prevents robust time-domain analysis using simulation alone. One particular problem of interest involves computing a system's reachable set, which is the set of possible final states of the system, given some set of inital conditions and certain metrics on the class of disturbances under consideration. Generally speaking, it is difficult to compute reachable set exactly, even in low state dimensions, since they often exhibit complex and nonstandard geometries that are not always easily discernible from the system's vector field [13].

Instead, many efficient algorithms exist for computing *over-approximations* of reachable sets. Such over-approximations have principal use cases in system verification [15, 16] and safety [8, 17], since they can be used to reason about, *i.e.*, whether system trajectories will *always* remain in a safe region of the state space or *eventually* reach an unsafe region. Moreover, over-approximations of reachable sets are generally constructed mathematically to exhibit some special geometry or property as to make them easy to compute and reason about; see, for example, [18], which deals with elliptical reachable set over-approximations. In this thesis, we mainly study the problem of computing a *hyperrectangular* over-approximation of a system's reachable set from an initial set of states that is also a hyperrectangle; indeed, numerous efficient techniques exist for over-approximating reachable sets using hyperrectangles, many of which scale nicely with the dimensionality of the system [19, 20].

One foundational theory in this area is that of *monotone* dynamical systems. State trajectories of a monotone system exhibit an ordering property [21, 22, 59], and this ordering creates a useful procedure for over-approximating reachable sets. In the special instance that a system is monotone, the tightest hyperrectangle containing a reachable set can be computed simply using two simulations of the initial system dynamics. Computing small numbers of system simulations in this way is generally a computationally unintensive task, and the main benefit of employing the monotonicity property for, *e.g.*, reachability analysis, lies in this efficiency. Despite these advantages, it should be noted that monotonicity poses a fairly restrictive assumption on the system's vector field, and more general techniques are needed to solve the reachability analysis problem in the general setting of continuous-time nondeterministic systems.

A related approach, that applies more generally, involves attempting to embed the initial system dynamics in a higher-dimensional *embedding system* with monotone dynamics. Indeed, this is an old idea—especially in the discrete-time setting, where convergent iteration algorithms were developed as early as 1959 using a similar monotone embedding [23]. Nonetheless, the power of this theory becomes most revealing when placed in the context of monotone dynamical systems, as advanced more recently in [24–28]. The primary focus of these works is in studying the stability of equilibria for systems without disturbances; indeed, a well-explored application of the monotonicity property is in studying equilibria and their stability properties, with applications in traffic theory [32] and biological systems [60]. This thesis takes a different approach and studies how such a monotone embedding can facilitate efficient reachability analysis for systems with disturbances, as emphasized and advanced more recently in [29]. Moreover, the idea of embedding a dynamical system's vector field a higher dimensional monotone system is the main idea behind the *mixed monotonicity* property of dynamical systems [30].

A dynamical system is mixed monotone if there exists a related *decomposition function* that decomposes the system's vector field into cooperative and competitive state interactions; a result that has been applied in the context of continuous-time systems [25, 27, 28, 31, 32], discrete-time systems [26, 30, 55], and systems with disturbances [29, 33, 34]. This decomposition function then facilitates embedding the initial system dynamics in a monotone embedding system as described below:

In particular, when disturbance are not present, a $2n$-dimensional symmetric embedding system can be constructed from the decomposition function of an n-dimensional mixed monotone system. This embedding system is monotone with respect to a particular southeast cone and the original dynamics are contained in an invariant n-dimensional *diagonal* subspace. Thus, tools from monotone systems theory can be applied to the embedding system to conclude properties of the original dynamics; in particular, such approaches are useful for stability analysis [37, 38], reachability analysis [26], and formal verification and synthesis [39, 40]. When disturbances are present, it is also possible to construct a symmetric monotone embedding system from the original dynamics. Here, the embedding system is nondeterministic with a $2m$-dimensional disturbance input when the original system is subject to an m-dimensional disturbance input. This result has been applied in discrete-time in [29, 34] and in continuous-time [33, 34] for the efficient over-approximation of reachable sets using hyperrectangles.

In this thesis, we take a different approach and instead study a related *deterministic* embedding system that arises from considering only the worst case disturbance inputs; an approach first studied explicitly in [35]. While this new deterministic embedding system is straightforwardly derived from the aforementioned nondeterministic formulation studied in [29], these systems exhibit different properties and should be treated differently in analysis and application. In particular, unlike the deterministic embedding system that arises in the case with no disturbance, the diagonal of this new deterministic embedding system is not forward invariant and, instead, a forward invariant *triangular* region is induced above the diagonal. Moreover, the deterministic embedding system provides several useful tools for systems' analysis that are not directly attainable from the nondeterministic formulation; for example, equilibria for the deterministic embedding system identify forward invariant sets for the original system [35, 36], an application discussed later in Chapter 4.

This chapter serves as a preliminary tutorial on the theory of mixed monotone dynamical systems and their related deterministic embedding systems described above. We begin with a discussion on the reachability analysis problem for dynamical systems in Section 2.1. Next, we present the monotonicity property of dynamical systems in Section 2.2. Monotonicity is shown to produce an efficient procedure for over-approximating reachable sets using hyperrectangles, however, the conditions on monotonicity are fairly restrictive and later, in Section 2.4, we introduce the mixed monotonicity property which applies more generally. Before this study, we present a discussion on the southeast order, in Section 2.3, which is crucial in the understanding of mixed monotonicity and mixed monotone embedding systems. Descriptions of the symmetric embedding system, the deterministic embedding system, and the reachability analysis procedure for mixed monotone systems are provided in Sections 2.4.1, 2.4.2 and 2.4.3, respectively. Numerous examples are included throughout to guide the reader in understanding mixed monotonicity and the tools on which the theory is built. In particular, a mixed monotone system will be mixed monotone with respect to a related *decomposition function* that separates the system dynamics into cooperative and competitive state interactions. While we present numerous examples and special cases for how decomposition functions are created, we hold off on presenting a formal theory for constructing decomposition functions until later in Chapter 3. Nonetheless, in Section 2.5 of this chapter, we present a brief discussion on the application of mixed monotonicity and on the construction of decomposition functions. Finally, we present a few related notions and tools, in Section 2.6, for over-approximating the reachable set of a dynamical system using hyperrectangles. These methods are then used in later sections to construct decomposition functions and reason about their related embedding systems.

2.1 Reachability Analysis For Dynamical Systems

Consider a dynamical system with disturbances

$$\dot{x} = F(x, w) \tag{2.1}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$ is the state and $w \in \mathcal{W} \subset \mathbb{R}^m$ is a bounded time-varying disturbance input. The sets $\mathcal{X} \subseteq \mathbb{R}^n$ and $\mathcal{W} \subset \mathbb{R}^m$ are the *state* and *disturbance spaces* of (2.1), respectively. We assume throughout this thesis that the vector field F is locally Lipschitz continuous in its inputs

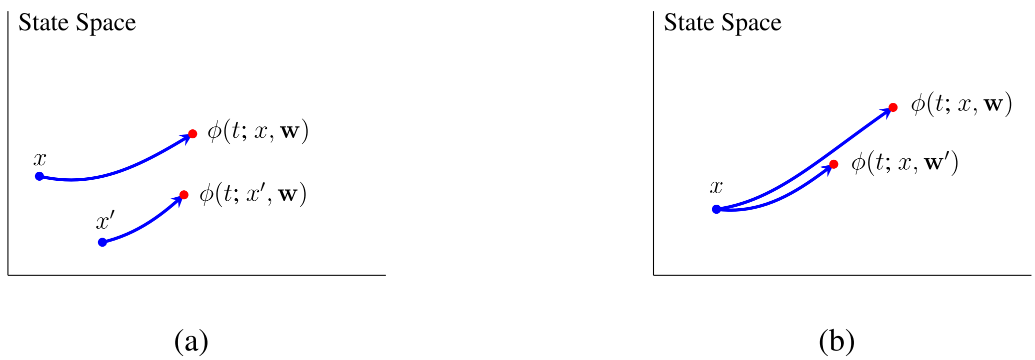


Figure 2.1: Solutions to (2.1) are dependant on the inital state and the disturbance signal, as shown by cartoon in Figures 2.1(a)-(b). Figure 2.1(a) compares the trajectories attained from different inital conditions $x, x' \in \mathbb{R}^n$ but the same disturbance signal $\mathbf{w}(t)$. Figure 2.1(b) compares the trajectories attained from the same inital condition $x \in \mathbb{R}^n$, but with different disturbance signals $\mathbf{w}(t), \mathbf{w}'(t)$.

and that disturbance signals $\mathbf{w} : [0,t] \to \mathcal{W}$ are piecewise continuous in time so that, in particular, solutions to (2.1) are unique when they exist [61]. See Figure 2.1.

We denote by $\phi(t;x,\mathbf{w}) \in \mathcal{X}$ the state of (2.1) reached at time $t \geq 0$ when beginning at state $x \in \mathcal{X}$ at time 0 and evolving subject to the disturbance signal $\mathbf{w} : [0,t] \to \mathcal{W}$. We allow for finite-time escape so that $\phi(t;x,\mathbf{w})$ need not exist for all t, however, $\phi(t;x,\mathbf{w})$ is understood to exist only when $\phi(\tau;x,\mathbf{w}) \in \mathcal{X}$ for all $\tau \in [0,t]$, and statements involving $\phi(t;x,\mathbf{w})$ are understood to apply only when $\phi(t;x,\mathbf{w})$ exists. We sometimes refer to the time-dependant signal $\phi(t;x,\mathbf{w})$ as a *trajectory* of the dynamics (2.1), and the computation of a trajectory is referred to as a *simulation*.

While individual solutions $\phi(t;x,\mathbf{w})$ to (2.1) are computable using simulation of the dynamics, the time-varying nature of the disturbance input $\mathbf{w}$ generally prevents robust time-domain analysis via simulation alone. Instead, it is useful to characterize finite-time system behavior using reachable sets.

Definition 1 (Reachable Set)**.** At time $t \geq 0$, the set of states that are reachable by (2.1) from the initial set $A \subseteq \mathcal{X}$ is given by

$$R(t;A) := \{\phi(t;x,\mathbf{w}) \in \mathcal{X} \,|\, x \in A, \text{ for some } \mathbf{w} : [0,t] \to \mathcal{W}\}. \tag{2.2}$$

(a) (b)

Figure 2.2: Reachability Analysis for Dynamical Systems: The reachable set of (2.1) is the set of states that the system is guaranteed to enter, as shown by cartoon in Figures 2.2(a)-(b). Figure 2.2(a) under-approximates $R(t; A)$ using many simulations $\phi(t; x, \mathbf{w})$, shown in green, from different initial states $x \in A$, shown in red. Computing reachable sets exactly can be computationally costly, however over-approximations of reachable sets have many useful applications when they can be computed efficiently; see Figure 2.2(b) for a depiction of an elliptical over-approximation of $R(t; A)$.

■

The set $R(t; A) \subseteq \mathcal{X}$ from (2.2) is the *time-t reachable set of* (2.1) *from* $A \subseteq \mathcal{X}$, and when A and t are clear from context, we refer to $R(t; A)$ simply as the *reachable set*. Reachable sets can be under-approximated using, *e.g.*, many system simulations $\phi(t; x, \mathbf{w})$ from different initial states $x \in A$ and with different disturbance signals $\mathbf{w}$, however this approach can be computationally intractable even when the state space dimension n is small. Instead, many efficient algorithms exist for over-approximating $R(t; A)$ using, for example, abstraction [15], energy-based techniques [62], or domain knowledge [63]. Over-approximations of reachable sets, unlike under-approximations, allow one to reason whether, *e.g.*, system trajectories will *eventually* reach a target region of the state space or *always* remain in a safe region, thus creating a necessity for over-approximations of reachable sets in system verification and safety applications [16]. See Figure 2.2.

As formalised next, the reachability analysis problem of dynamical systems involves computing an over-approximation of $R(t; A)$, given an initial set $A \subseteq \mathcal{X}$ and a time $t \geq 0$.

Problem 1 (Reachability Analysis)**.** Given a system (2.1), an initial set of states $A \subset \mathcal{X}$ and time $t \geq 0$, compute $B \subseteq \mathcal{X}$ so that $R(t; A) \subseteq B$. ■

The remainder of this chapter studies means of solving the reachability analysis problem and we explore, in particular, methods for computing *hyperrectangular* over-approximations of $R(t; A)$ from initial sets A that are also hyperrectangles. In the next section, we present one special class of systems for when hyperrectangular over-approximations of reachable sets are easily attainable; when (2.1) is a *monotone* dynamical system, the tightest hyperrectangle containing $R(t; A)$ can be computed simply using two simulations of the initial system dynamics.

Before this study, we present a related notion to reachable sets—*forward invariant sets*—that will become a main point of focus in later in Chapter 4.

Definition 2 (Robust Forward Invariance)**.** A set $A \subseteq \mathcal{X}$ is *robustly forward invariant* for (2.1) if $\phi(t; x, \mathbf{w}) \in A$ for all $x \in A$, all $t \geq 0$ and all piecewise continuous disturbance inputs $\mathbf{w} : [0, t] \to \mathcal{W}$ whenever $\phi(t; x, \mathbf{w})$ exists. When F does not depend on w we simply say A is *forward invariant*. ■

Observe that when a set A is forward invariant for (2.1), then $R(t; A) \subseteq A$ for all t, *i.e.*, the reachable set of (2.1) is contained inside A. We make use of this observation later in Chapter 4 where show how robustly forward invariant regions for (2.1) are identified using reachability analysis tools.

2.2 Monotone Systems Theory

The system (2.1) is a *monotone dynamical system* if for any pair of inital states $x, x' \in \mathcal{X}$ with $x \preceq x'$ and pair of input signals $\mathbf{w}, \mathbf{w}' : [0, \infty) \to \mathcal{W}$ with $\mathbf{w}(\tau) \preceq \mathbf{w}'(\tau)$ for all $\tau \geq 0$, it holds that

$$\phi(t; x, \mathbf{w}) \preceq \phi(t; x', \mathbf{w}') \tag{2.3}$$

for all $t \geq 0$. In other words, state trajectories of a monotone system remain *ordered* with respect to the standard order $\preceq$ for all time: a property depicted graphically in Figure 2.3. An equivalent *infinitesimal characterization* of monotonicity is provided in Definition 3 [22].

Definition 3. The system (2.1) is monotone if and only if both of the following hold:

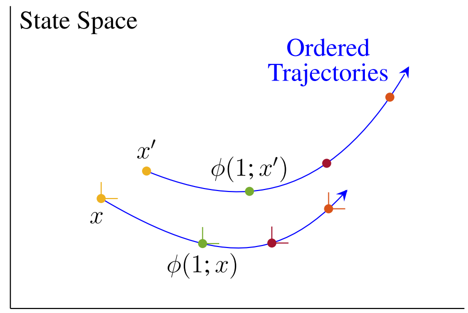


Figure 2.3: State trajectories of a monotone dynamical system remain ordered with respect to the standard order $\preceq$ for all time; that is, when $x_i \leq x_i'$ for all i, we have that $\phi_i(t; x) \leq \phi_i(t; x')$ for all i and all $t \geq 0$.

- for all $i, j \in \{1, \cdots, n\}$ with $i \neq j$,

$$\frac{\partial F_i}{\partial x_j}(x, w) \geq 0 \tag{2.4}$$

  for all $x \in \mathcal{X}$ and all $w \in \mathcal{W}$ where the derivative exists. In other words, every off-diagonal element of $\frac{\partial F}{\partial x}(x, w)$ is positive.

- for all $i \in \{1, \cdots, n\}$ and all $k \in \{1, \cdots, m\}$

$$\frac{\partial F_i}{\partial w_k}(x, w) \geq 0 \tag{2.5}$$

  for all $x \in \mathcal{X}$ and all $w \in \mathcal{W}$ where the derivative exists. In other words, $\frac{\partial F}{\partial w}(x, w)$ is a positive matrix. ■

Observe that since F is assumed to be locally Lipschitz continuous in its inputs, the derivatives in (2.4)–(2.5) exist almost everywhere.

Remark 1. A second important implication of Lipschitz continuity is that (2.1) admits unique solutions. Indeed, uniqueness of solutions is a requisite property of monotone systems. To see this, let $\phi(t; x, \mathbf{w})$ and $\phi'(t; x, \mathbf{w})$ be solutions to (2.1) for some $t \geq 0$, $x \in \mathcal{X}$, and $\mathbf{w} : [0, t] \to \mathcal{W}$.

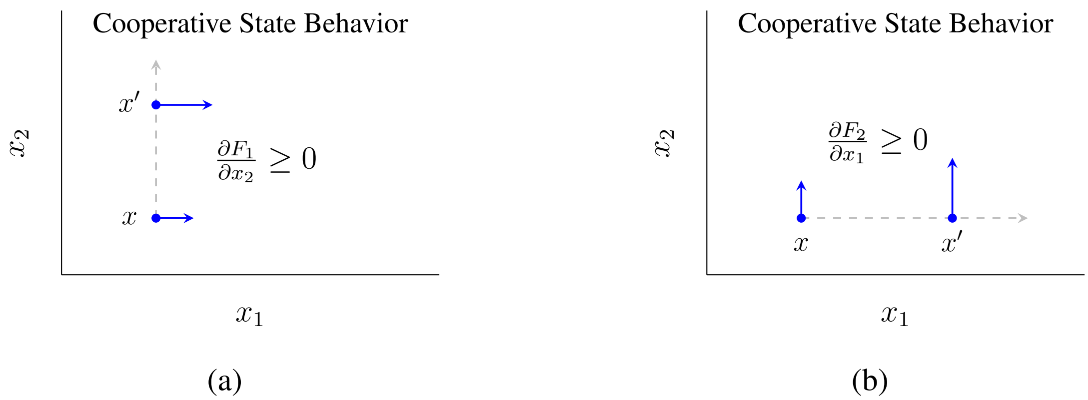


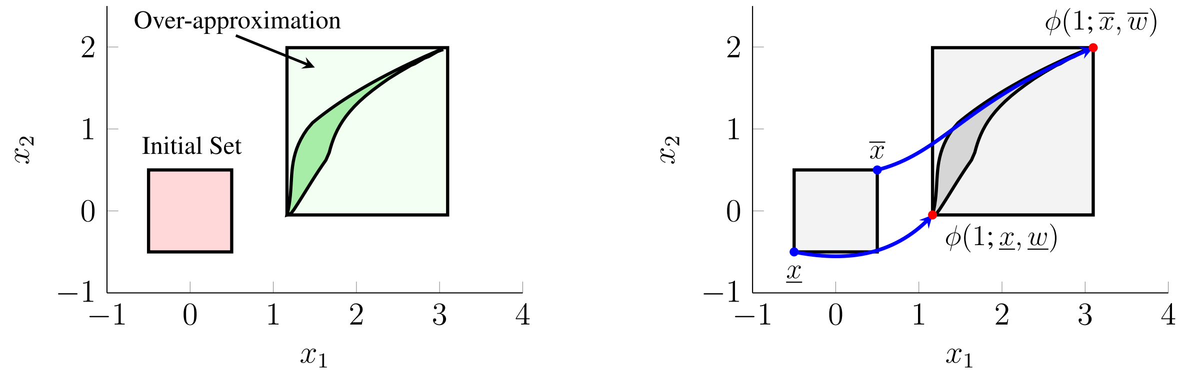
Figure 2.4: Cooperative State Behavior: When is (2.1) is a monotone system, state trajectories exhibit cooperative state interactions, as depicted graphically in Figures 2.4(a)–(b) for the case of $n = 2$ states and no disturbance input. Observe that $F_1(x) \leq F_1(x')$ for all $x, x' \in \mathcal{X}$ with $x_1 = x_1'$ and $x_2 < x_2'$. Similarly, $F_2(x) \leq F_2(x')$ for all $x, x' \in \mathcal{X}$ with $x_2 = x_2'$ and $x_1 < x_1'$.

Since, by definition, $x \preceq x$ and $\mathbf{w}(t) \preceq \mathbf{w}(t)$ for all $t \geq 0$, the condition (2.3) implies both

$$\phi(t; x, \mathbf{w}) \preceq \phi'(t; x, \mathbf{w}) \quad \text{and} \quad \phi'(t; x, \mathbf{w}) \preceq \phi(t; x, \mathbf{w}) \tag{2.6}$$

hold, which is true only when $\phi(t; x, \mathbf{w}) = \phi(t; x', \mathbf{w})$. Moreover, in our work, we impose uniqueness of solutions on (2.1) through the assumption that the vector field F is Lipschitz continuous in its inputs. See Section 2.1. ■

A fitting explanation of monotonicity is that state variables exhibit *cooperative* time-varying behavior. Informally speaking, the growth of one state entry x_i cannot hurt the growth of another x_j, as depicted by cartoon in Figure 2.4 for the case of two states and no disturbances. For this reason monotone systems, as defined in Definition 3 where the standard order $\preceq$ is used in (2.3), are sometimes referred to in literature as *cooperative systems* or also *positive systems* due to the positivity conditions presented in (2.4)–(2.5) [21, 22]. Monotonicity can be also be defined in terms of alternative (partial) orders on the system state space, allowing for more complex interpretations of system behavior [22, Cor. III.3]. Of particular interest to this work, monotonicity when defined with respect to the *southeast order* can be used to reason about, *e.g.*, set containment on a lower dimensional space, a property studied more deeply in Section 2.3. Nonetheless, the remaining



(a) (b)

Figure 2.5: Example 1: Computing reachable sets for (2.8) by applying Proposition 1. Subfigures: (a) The initial set $[\underline{x}, \overline{x}]$ is shown in pink. The time-1 reachable set $R(1; A)$ of (2.8), which was computed via exhaustive simulation, is shown in dark green. A rectangular over-approximation of $R(1; A)$ is computed using Proposition 1 and is shown in light green. (b) Applying Proposition 1, the time-t reachable set of (2.8) is over-approximated by the rectangular set $[\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})]$, and $[\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})]$ is the tightest rectangle containing $R(t; [\underline{x}, \overline{x}])$ since $\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})$ correspond to true system trajectories.

results and tools presented in this section are put in terms of the standard order $\preceq$ for ease of exposition.

An important feature of monotone dynamical systems that we exploit in this work is that tight hyperrectangular over-approximations of reachable sets can be computed simply using two simulations of the initial system dynamics in (2.1).

Proposition 1. *Let* (2.1) *be a monotone dynamical system and recall* $\mathcal{W} = [\underline{w}, \overline{w}]$. *For all* $[\underline{x}, \overline{x}] \subset \mathcal{X}$, *the hyperrectangular set of states* $[\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})] \subseteq \mathcal{X}$ *is the tightest hyperrectangle containing* $R(t; [\underline{x}, \overline{x}])$. *In other words,*

$$R(t; [\underline{x}, \overline{x}]) \subseteq [\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})] \tag{2.7}$$

and no proper hyperrectangular subset of $[\phi(t; \underline{x}, \underline{w}), \phi(t; \overline{x}, \overline{w})]$ *contains* $R(t; [\underline{x}, \overline{x}])$. ■

The proof of Proposition 1 is immediate from the definition of monotonicity presented in (2.3) and, thus, we next move to demonstrate this result through an example; see Example 1.

Example 1. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x, w) = \begin{bmatrix} x_2^3 - x_1 + w \\ x_1 \end{bmatrix} \tag{2.8}$$

with state $x \in \mathbb{R}^2$ and disturbance $w \in [\underline{w}, \overline{w}]$. The system (2.8) is a monotone system since

$$\frac{\partial F_1}{\partial x_2}(x, w) \geq 0, \quad \frac{\partial F_2}{\partial x_1}(x, w) \geq 0 \quad \text{and} \quad \frac{\partial F_1}{\partial w}(x, w) \geq 0 \tag{2.9}$$

hold always, and Proposition 1 now implies that the tightest hyperrectangle containing $R(t; [\underline{x}, \overline{x}])$ is given by $[\phi(t, \underline{x}, \underline{w}), \phi(t, \overline{x}, \overline{w})]$. An example is shown in Figure 2.5 where we take $[\underline{x}, \overline{x}] = [-\frac{1}{2}, \frac{1}{2}]^2$ and $[\underline{w}, \overline{w}] = [2.2, 2.3]$ and over-approximate $R(1; [\underline{x}, \overline{x}])$ using Proposition 1. ■

While the above example demonstrates an intriguing technique for solving the reachability analysis problem, it is important to remember that monotonicity is a structural property of the vector field F in the sense that a general system (2.1) may or may not be monotone depending on F's dependence on x and w. This structural property is captured well through the concept of Metzler matrices [64, Section 10.2].

Definition 4 (Metzler Matrix)**.** A matrix $A \in \mathbb{R}^{n \times n}$ is a Metzler matrix if for all $i \neq j$, $A_{i,j} \geq 0$, *i.e.*, all off-diagonal elements of A are positive. ■

To use the terminology introduced in Definition 4, a monotone system is one for which $\frac{\partial F}{\partial x}(x, w)$ is Metzler for all $x \in \mathcal{X}$ and all $w \in \mathcal{W}$, and likewise $\frac{\partial F}{\partial w}(x, w)$ is a positive matrix. As a trivial case of this statement, observe that any systems (2.1) with $n = 1$ state and no disturbance is a monotone dynamical system. As a second special case, we next present the monotonicity conditions for linear time-invariant systems.

Example 2. The linear time-invariant system

$$\dot{x} = Ax + Bw \tag{2.10}$$

is monotone when every off-diagonal element of $A \in \mathbb{R}^{n \times n}$ is positive and every element of $B \in \mathbb{R}^{n \times m}$ is positive, *i.e.*, A is a Metzler matrix and B is a positive matrix. ■

The reachability analysis procedure given in Proposition 1 has been successfully demonstrated in applications such as efficient finite-state abstraction [39], and monotonicity also provides tools for studying equilibria and their stability properties, with applications in traffic theory [32] and biological systems [60]. Nonetheless, monotonicity poses a fairly restrictive assumption on the vector field F, as detailed above, and more general techniques are necessary for solving the reachability analysis problem when arbitrary systems (2.1) are considered. To that end, in Section 2.4, we present the *mixed monotonicity* property of dynamical systems which provides a significant generalisation of the monotonicity property, applicable to all systems as in (2.1). As a necessary step in the development of mixed monotonicity, we present first, in Section 2.3, the definition of the *southeast order*.

2.3 The Southeast Order

In an n-dimensional state space $\mathcal{X} \subset \mathbb{R}^n$ a hyperrectangular subset $A \subseteq \mathcal{X}$ is a hyperinterval defined by two coordinates $x, y \in \mathcal{X}$ with $x \preceq y$:

$$A = [x, y] := \{z \in \mathcal{X} \mid x \preceq z \preceq y\}. \tag{2.11}$$

The southeast order is one useful tool for studying hyperrectangles and set containment.

Definition 5 (Southeast Order)**.** Let $\preceq_{\mathrm{SE}}$ denote the *southeast order* on $\mathbb{R}^{2n}$ defined by

$$\begin{bmatrix} x \\ y \end{bmatrix} \preceq_{\mathrm{SE}} \begin{bmatrix} x' \\ y' \end{bmatrix} \quad \Leftrightarrow \quad \begin{array}{c} x \preceq x' \\ y \succeq y' \end{array} \tag{2.12}$$

for $x, x', y, y' \in \mathbb{R}^n$. ■

In the remaining chapters, we mainly study hyperrectangular subsets of $\mathcal{X}$ using an equivalent

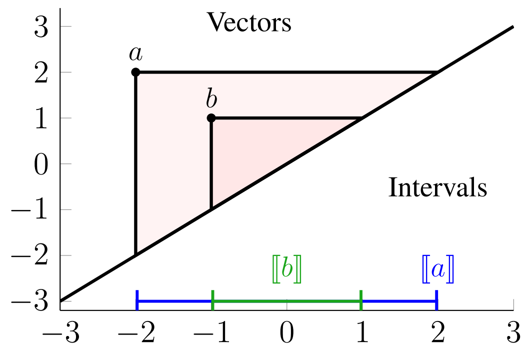


Figure 2.6: The Southeast Order: Hyperrectangular subsets of $\mathcal{X} \subseteq \mathbb{R}^n$ correspond to $2n$-dimensional vectors in $\mathcal{T}$. For example, the intervals $[\![a]\!] = [-2, 2]$ and $[\![b]\!] = [-1, 1]$ correspond to $a = (-2, 2)$ and $b = (-1, 1)$, respectively, and since $a \preceq_{\mathrm{SE}} b$ we have also $[\![b]\!] \subseteq [\![a]\!]$.

$2n$-dimensional vector representation. We denote by

$$\mathcal{T} := \{(x, y) \in \mathcal{X} \times \mathcal{X} \mid x \preceq y\} \subset \mathbb{R}^{2n} \tag{2.13}$$

the set of $2n$-dimensional vectors with corresponding hyperrectangular subsets and, for any $a = (x, y) \in \mathcal{T}$, we denote by

$$[\![a]\!] := [x, y] \subseteq \mathcal{X} \tag{2.14}$$

the hyperinterval corresponding to a. Observe that in the special instance where $a \preceq_{\mathrm{SE}} a'$ for some $a, a' \in \mathcal{T}$, we additionally have $[\![a']\!] \subseteq [\![a]\!]$, since it is true that

$$(x, y) \preceq_{\mathrm{SE}} (x', y') \quad \Leftrightarrow \quad [x', y'] \subseteq [x, y], \tag{2.15}$$

when $x \preceq y$ and $x' \preceq y'$. This connection is depicted graphically in Figure 2.6.

As a second application of the southeast order, observe that two hyperrectangles $[\underline{x}, \overline{x}]$ and $[\underline{y}, \overline{y}]$ will *intersect* one another only when

$$\begin{bmatrix} \underline{x} \\ \overline{x} \end{bmatrix} \preceq_{\mathrm{SE}} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} \underline{y} \\ \overline{y} \end{bmatrix} \tag{2.16}$$

holds, since it is true that $[\underline{x}, \overline{x}] \cap [\underline{y}, \overline{y}] \neq \varnothing$ only when $\underline{x} \preceq \overline{y}$ and $\underline{y} \preceq \overline{x}$ hold.

Just as a system may be monotone with respect to the standard order $\preceq$, see Definition 3, a system may also be monotone with respect to $\preceq_{\mathrm{SE}}$, as depicted graphically later in Figure 2.7(b). A system $\dot{a} = \varepsilon(a, b)$ with state $a \in \mathcal{X} \times \mathcal{X} \subseteq \mathbb{R}^{2n}$ and disturbance $b \in \mathcal{W} \times \mathcal{W} \subseteq \mathbb{R}^{2m}$ is said to be *monotone with respect to the southeast order* when

$$\Phi^{\varepsilon}(t; a, \mathbf{b}) \preceq_{\mathrm{SE}} \Phi^{\varepsilon}(t; a', \mathbf{b}') \tag{2.17}$$

holds for all $a, a' \in \mathcal{X} \times \mathcal{X}$ and $\mathbf{b}, \mathbf{b}' : [0, t] \to \mathcal{W} \times \mathcal{W}$ with $a \preceq_{\mathrm{SE}} a'$ and $\mathbf{b}(t) \preceq_{\mathrm{SE}} \mathbf{b}'(t)$ for all $t \geq 0$. Monotonicity with respect to the southeast order is a main focus of the next section.

2.4 Mixed Monotone Systems Theory

A dynamical system is *mixed monotone* when there exists a related *decomposition function* that decomposes the system's vector field into cooperative and competitive state interactions, a result that has been applied in the context of continuous-time systems [25, 27, 28, 31, 32], discrete-time systems [26], and systems with disturbances [29, 33, 34]. Mixed monotonicity in the context of (2.1) is defined as follows:

Definition 6 (Mixed Monotonicity [30])**.** Given a locally Lipschitz continuous function $d : \mathcal{X} \times \mathcal{W} \times \mathcal{X} \times \mathcal{W} \to \mathbb{R}^n$, the system (2.1) is *mixed monotone with respect to* d if, for all $x, \widehat{x} \in \mathcal{X}$ and all $w, \widehat{w} \in \mathcal{W}$, all of the following hold:

D1) F is embedded on the diagonal of d; that is

$$d(x, w, x, w) = F(x, w). \tag{2.18}$$

D2) For all $i, j \in \{1, \cdots, n\}$ with $i \neq j$,

$$\frac{\partial d_i}{\partial x_j}(x, w, \widehat{x}, \widehat{w}) \geq 0 \tag{2.19}$$

holds whenever the derivative exists. In other words, $\frac{\partial d}{\partial x}(x, w, \widehat{x}, \widehat{w})$ is a Metzler matrix.

D3) For all $i, j \in \{1, \cdots, n\}$,

$$\frac{\partial d_i}{\partial \widehat{x}_j}(x, w, \widehat{x}, \widehat{w}) \leq 0 \tag{2.20}$$

holds whenever the derivative exists. In other words, $\frac{\partial d}{\partial \widehat{x}}(x, w, \widehat{x}, \widehat{w})$ is a negative matrix.

D4) For all $i \in \{1, \cdots, n\}$ and all $k \in \{1, \cdots, m\}$,

$$\frac{\partial d_i}{\partial w_k}(x, w, \widehat{x}, \widehat{w}) \geq 0 \quad \text{and} \quad \frac{\partial d_i}{\partial \widehat{w}_k}(x, w, \widehat{x}, \widehat{w}) \leq 0 \tag{2.21}$$

holds whenever the derivatives exist. In other words, $\frac{\partial d}{\partial w}(x, w, \widehat{x}, \widehat{w})$ is a positive matrix and $\frac{\partial d}{\partial \widehat{w}}(x, w, \widehat{x}, \widehat{w})$ is a negative matrix. ■

If (2.1) is mixed monotone with respect to d, d is said to be a *decomposition function* for (2.1), and when d is clear from context we simply say that (2.1) is mixed monotone. Mixed monotonicity is a general property of dynamical systems and, in Chapter 3 of this work, we show that a decomposition function *always* exists for (2.1) when the vector field $F(x, w)$ is Lipshitz continuous in x and w. While we do not present a formal theory for computing decomposition functions in this chapter, we do attempt to explain the decomposition function conditions D1–D4 through example.

Remark 2. Conditions D2–D4 of Definition 6 are equivalent to the following two conditions:

K1) For all $i \in \{1, \cdots, n\}$,

$$d_i(x,\, w,\, \widehat{x},\, \widehat{w}) \leq d_i(y,\, v,\, \widehat{x},\, \widehat{w}) \tag{2.22}$$

for all $x, y, \widehat{x} \in \mathcal{X}$ such that $x \leq y$ and $x_i = y_i$, and for all $w, v, \widehat{w} \in \mathcal{W}$ such that $w \leq v$.

K2) For all $i \in \{1, \cdots, n\}$,

$$d_i(x,\, w,\, \widehat{y},\, \widehat{v}) \leq d_i(x,\, w,\, \widehat{x},\, \widehat{w}) \tag{2.23}$$

for all $x,\, \widehat{x},\, \widehat{y} \in \mathcal{X}$ such that $\widehat{x} \leq \widehat{y}$ and for all $w,\, \widehat{w},\, \widehat{v} \in \mathcal{W}$ such that $\widehat{w} \leq \widehat{v}$.

These are the so-called *Kamke* or *type-K* conditions for monotonicity, modified for the mixed monotone setting [21, Section 3]. It is sometimes more convenient to use these alternative conditions, while the infinitesimal characterization provided in Definition 6 is generally more intuitive. ■

As a special case of mixed monotonicity, observe that when (2.1) is a monotone dynamical system, as introduced previously in Definition 3, it is also true that (2.1) is mixed monotone with respect to $d(x, w, \widehat{x}, \widehat{w}) = F(x, w)$, a point discussed later in Remark 5. A common interpretation of monotonicity is requiring cooperative interaction among all state variables, and mixed monotonicity provides an extension allowing for competitive effects captured by the hatted variables. As such, an arbitrary mixed monotone system will generally be so that the decomposition function $d(x, w, \widehat{x}, \widehat{w}) \neq F(x, w)$ unless, for example, $x = \widehat{x}$ and $w = \widehat{w}$. To see this is it is instructive to revisit the case of linear time-invariant systems, as studied previously in Example 2.

Example 3. Any linear time-invariant system $\dot{x} = Ax + Bw$ is mixed monotone with respect to

$$d^{\mathrm{LTI}}(x, w, \widehat{x}, \widehat{w}) = A^{\mathrm{M}+}x + A^{\mathrm{M}-}\widehat{x} + B^{+}w + B^{-}\widehat{w} \tag{2.24}$$

where $A^{\mathrm{M}+}, A^{\mathrm{M}-} \in \mathbb{R}^{n\times n}$ in (2.24) are the Metzler and non-Metzler parts of A, respectively, and $B^{+}, B^{-} \in \mathbb{R}^{n\times m}$ are the non-negative and non-positive parts of B:

$$\begin{aligned} A^{\mathrm{M}+}_{i,j} &:= \begin{cases} A_{i,j} & \text{if } A_{i,j} \geq 0 \text{ or } i = j \\ 0 & \text{if } A_{i,j} \leq 0 \text{ and } i \neq j, \end{cases} \qquad A^{\mathrm{M}-}_{i,j} := \begin{cases} A_{i,j} & \text{if } A_{i,j} \leq 0 \text{ and } i \neq j \\ 0 & \text{if } A_{i,j} \geq 0 \text{ or } i \neq j, \end{cases} \\ B^{+}_{i,j} &:= \begin{cases} B_{i,j} & \text{if } B_{i,j} \geq 0 \\ 0 & \text{if } B_{i,j} \leq 0, \end{cases} \qquad B^{-}_{i,j} := \begin{cases} B_{i,j} & \text{if } B_{i,j} \leq 0 \\ 0 & \text{if } B_{i,j} \geq 0. \end{cases} \end{aligned} \tag{2.25}$$

Observe that since $A = A^{\mathrm{M}+} + A^{\mathrm{M}-}$ and $B = B^{+} + B^{-}$ we have that $d(x, w, x, w) = Ax + Bw$, *i.e.*, d from (2.24) satisfies the first condition in Definition 6, and is is easy to see how the remaining derivative conditions on d are also satisfied.

As a specific instance of this result, observe that the system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 1 & -2 & -3 \\ 4 & -5 & 6 \\ -7 & 8 & -9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \tag{2.26}$$

is mixed monotone with respect to

$$d^{\mathrm{LTI}}(x, \widehat{x}) = \begin{bmatrix} 1 & 0 & 0 \\ 4 & -5 & 6 \\ 0 & 8 & -9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 & -2 & -3 \\ 0 & 0 & 0 \\ -7 & 0 & 0 \end{bmatrix} \begin{bmatrix} \widehat{x}_1 \\ \widehat{x}_2 \\ \widehat{x}_3 \end{bmatrix} \tag{2.27}$$

where we use the colors blue, green, and red to emphasize how $A^{\mathrm{M}+}$ and $A^{\mathrm{M}-}$ are constructed from the diagonal entries, positive entries and non-diagonal negative entries of A, respectively. ■

We show in the next three subsections how a decomposition function for (2.1) is used to *embed* the inital system dynamics (2.1) in a related *deterministic embedding system* with monotone dynamics and how reachable sets for the initial system (2.1) are efficiently over-approximated using a single simulation of this deterministic embedding system.

We show first, in Section 2.4.1, how the decomposition function of an n-dimensional mixed monotone system with an m-dimensional disturbance is used to construct $2n$-dimensional *symmetric embedding system* with a $2m$-dimensional disturbance. This embedding system is shown to exhibit many useful properties; namely, the embedding system is monotone with respect to the southeast order—see Section 2.3—and the vector field of the embedding system is equal to that of inital system dynamics (2.1) on an invariant diagonal subspace of states. This allows for applying the rich theory of monotone dynamical systems to the embedding system and can be used to conclude many useful properties of the initial system. In particular, such approaches are useful for stability analysis [37, 38], reachability analysis [26], and formal verification and synthesis [15, 39].

Nonetheless, we study mainly in this thesis an alternative *deterministic* embedding system formulation that arises from considering only the worst case disturbance inputs. This study is the subject of Section 2.4.2. While this new deterministic embedding is straightforwardly derived from the aforementioned nondeterministic embedding system, it exhibits many key differences and enables a suite of analysis tools not previously attainable. As a particular example, we show in Section 2.4.3 how the reachable set of a system is efficiently over-approximated using a single simulation of its corresponding deterministic embedding system, and further reachability analysis tools are provided in Chapter 4.

2.4.1 The Symmetric Embedding System

Consider the nondeterministic system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = \varepsilon(x, w, \widehat{x}, \widehat{w}) := \begin{bmatrix} d(x, w, \widehat{x}, \widehat{w}) \\ d(\widehat{x}, \widehat{w}, x, w) \end{bmatrix} \tag{2.28}$$

with state $(x, \widehat{x}) \in \mathcal{X} \times \mathcal{X}$ and disturbance input $(w, \widehat{w}) \in \mathcal{W} \times \mathcal{W}$. We call (2.28) the *symmetric embedding system* relative to d, and we denote by $\Phi^{\varepsilon}(t; (\underline{x}, \overline{x}), (\mathbf{w}, \widehat{\mathbf{w}}))$ the state of (2.28) at time t when initialized at $(\underline{x}, \overline{x}) \in \mathcal{X} \times \mathcal{X}$ and when subjected to the piecewise continuous input $(\mathbf{w}, \widehat{\mathbf{w}})$.

There are two important structural features of the embedding system (2.28). First, (2.28) is a monotone control system as defined in [21] when the orders on $\mathcal{X} \times \mathcal{X}$ and $\mathcal{W} \times \mathcal{W}$ are both taken to be the southeast order; in other words, if $a, a' \in \mathcal{X} \times \mathcal{X}$ and $\mathbf{b}, \mathbf{b}' : [0, \infty) \to \mathcal{W} \times \mathcal{W}$ satisfy $a \preceq_{\mathrm{SE}} a'$ and $\mathbf{b}(t) \preceq_{\mathrm{SE}} \mathbf{b}'(t)$ for all $t \geq 0$, then

$$\Phi^{\varepsilon}(t; a, \mathbf{b}) \preceq_{\mathrm{SE}} \Phi^{\varepsilon}(t; a', \mathbf{b}') \tag{2.29}$$

holds for all $t \geq 0$, provided $\Phi^{\varepsilon}(\,\cdot\,; a, \mathbf{b})$ and $\Phi^{\varepsilon}(\,\cdot\,; a', \mathbf{b}')$ remain in $\mathcal{X} \times \mathcal{X}$ on $[0, t]$ [21]. Second, the embedding system (2.28) is *symmetric* in the sense that

$$\Phi^{\varepsilon}(t;(x,\widehat{x}),(\mathbf{w},\widehat{\mathbf{w}})) = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \Phi^{\varepsilon}(t;(\widehat{x},x),(\widehat{\mathbf{w}},\mathbf{w})) \tag{2.30}$$

holds for all $t \geq 0$, all $x \preceq \widehat{x}$, and all $\mathbf{w}, \widehat{\mathbf{w}} : [0,\infty) \to \mathcal{W}$ with $\mathbf{w}(t) \preceq \widehat{\mathbf{w}}(t)$ for all $t \in [0,\infty)$. An implication of symmetry is that the embedding system (2.28) induces an invariant diagonal space when the restriction $w = \widehat{w}$ is imposed; that is, defining

$$\Delta := \{(x,\widehat{x}) \in \mathcal{X} \times \mathcal{X} \mid x = \widehat{x}\} \tag{2.31}$$

to be the *diagonal of the embedding system*, we have that $\Phi^{\varepsilon}(t;a,(\mathbf{w},\mathbf{w})) \in \Delta$ for all $a \in \Delta$ and all $\mathbf{w} : [0,\infty) \to \mathcal{W}$. In this case, the first n and last n states in (2.28) are decoupled, and embedding system trajectories are constructed from two simulations of the initial dynamics in (2.1)

$$\Phi^{\varepsilon}(t;a,(\mathbf{w},\mathbf{w})) = \begin{bmatrix} \phi(t;x,\mathbf{w}) \\ \phi(t;x,\mathbf{w}) \end{bmatrix} \tag{2.32}$$

when $a = (x,x)$, since it is true that

$$d(x,w,x,w) = F(x,w). \tag{2.33}$$

See Equation (2.18) in Definition 6. To provide further clarity, a graphical representation of the monotonicity and symmetry properties is provided in Figure 2.7.

Since it is true that the embedding system (2.28) is monotone with respect to the southeast order, tools from monotone systems theory can be applied to the embedding system to conclude properties of the original dynamics (2.1); in particular, such approaches are useful for stability analysis [37, 38], reachability analysis [26, 33, 34], and formal verification and synthesis [39, 40]. See also [29, 34] for analogous results pertaining to discrete-time mixed monotone systems.

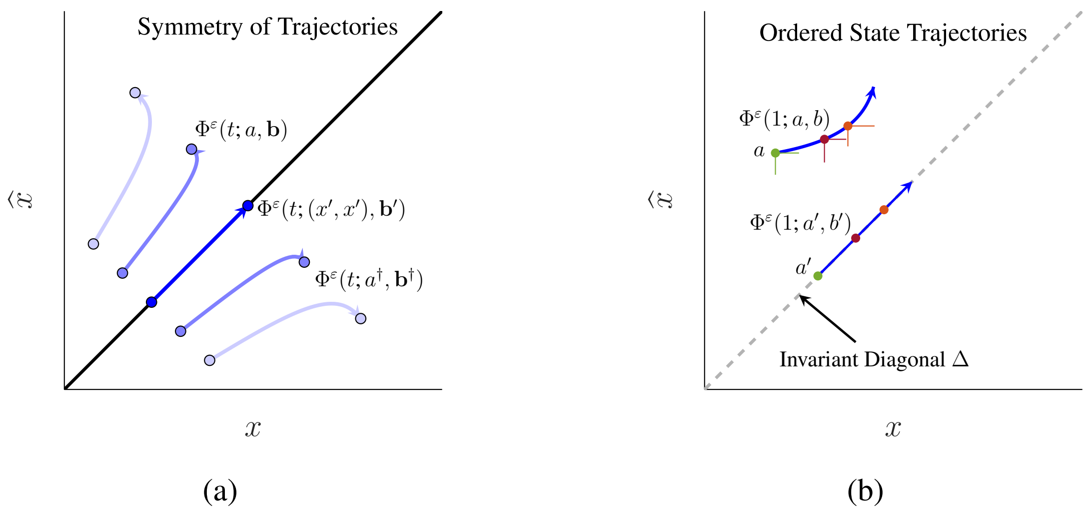


Figure 2.7: Properties of the Symmetric Embedding System (2.28). Subfigures: (a) The embedding system (2.28) exhibits a unique symmetry property, see (2.30): in the case where $a(t) = \Phi^{\varepsilon}(t; a_0, \mathbf{b})$ for some $a_0 = (x, \widehat{x})$ and some $\mathbf{b}(t) = (\mathbf{w}(t), \widehat{\mathbf{w}}(t))$, we also have $a^{\dagger}(t) = \Phi^{\varepsilon}(t; a_0^{\dagger}, \mathbf{b}^{\dagger})$ where $a_0^{\dagger} = (\widehat{x}, x)$ and $\mathbf{b}^{\dagger}(t) = (\widehat{\mathbf{w}}(t), \mathbf{w}(t))$. (b) An implication of symmetry is that the embedding system induces an invariant diagonal space Δ, given by (2.31), when the condition $\mathbf{b}' = (\mathbf{w}, \mathbf{w})$ is imposed. The embedding system (2.28) is also monotone with respect to the southeast order in the sense that $\Phi^{\varepsilon}(t; a, \mathbf{b}) \preceq_{\mathrm{SE}} \Phi^{\varepsilon}(t; a', \mathbf{b}')$ for all $a \preceq_{\mathrm{SE}} a'$ and all $\mathbf{b}, \mathbf{b}'$ with $\mathbf{b}(t) \preceq_{\mathrm{SE}} \mathbf{b}'(t)$ for all t.

In our work, we mainly rely, instead, on a $2n$-dimensional *deterministic* embedding system that arises from considering the worst case disturbance inputs, *i.e.*, we fix w and $\widehat{w}$ in (2.28) to be equal to $\underline{w}$ and $\overline{w}$, respectively. While this deterministic formulation is straightforwardly obtained from the symmetric embedding system (2.28), the deterministic embedding system exhibits fundamentally different properties and enables system analysis tools beyond those attainable from (2.28) directly. We explore this topic further in the next section.

2.4.2 The Deterministic Embedding System

Throughout most of this thesis, we instead utilize a *deterministic* embedding system formed by considering the worst case disturbance inputs:

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E(x, \widehat{x}) := \begin{bmatrix} d(x, \underline{w}, \widehat{x}, \overline{w}) \\ d(\widehat{x}, \overline{w}, x, \underline{w}) \end{bmatrix} \tag{2.34}$$

where we recall from (2.1) that the disturbance space $\mathcal{W}$ is assumed hyperrectangular with $\mathcal{W} = [\underline{w}, \overline{w}]$. We refer to E as the *embedding function relative to* d and we denote by

$$\Phi^E(t; a) := \Phi^\varepsilon(t; a, (\underline{w}, \overline{w})) \tag{2.35}$$

the state transition function of (2.34).

As was the case with (2.28), the deterministic embedding system (2.34) is monotone with respect to the southeast order, *i.e.*,

$$\Phi^E(t; a) \preceq_{\mathrm{SE}} \Phi^E(t; a') \tag{2.36}$$

for all $a, a' \in \mathcal{X} \times \mathcal{X}$ with $a \preceq_{\mathrm{SE}} a'$ and for all $t \geq 0$. However, unlike (2.28), the system (2.34) is not symmetric and Δ does not generally enjoy a forward invariance property on (2.34) unless $\underline{w} = \overline{w}$.

Nonetheless we next establish that the set of states that lie *above* the diagonal is forward invariant for the deterministic embedding system (2.34). Recall $\mathcal{T} := \{(x, y) \in \mathcal{X} \times \mathcal{X} \,|\, x \preceq y\}$ from (2.13), which is referred to hereafter as the *upper-triangle of the embedding system*.

Lemma 1. $\mathcal{T}$ is forward invariant for (2.34). ■

Proof. Choose $a = (\underline{x}, \overline{x}) \in \mathcal{T}$, then $\underline{x} \preceq \overline{x}$. Define

$$(x(t), \widehat{x}(t)) := \Phi^E(t; (\underline{x}, \overline{x})) = \Phi^\varepsilon(t; (\underline{x}, \overline{x}), (\underline{w}, \overline{w})), \tag{2.37}$$

where from (2.30) we now have

$$\begin{aligned}(x(t), \widehat{x}(t)) &= \Phi^\varepsilon(t; (\underline{x}, \overline{x}), (\underline{w}, \overline{w})),\\ (\widehat{x}(t), x(t)) &= \Phi^\varepsilon(t; (\overline{x}, \underline{x}), (\overline{w}, \underline{w})).\end{aligned}$$

Since $(\underline{x}, \overline{x}) \preceq_{\mathrm{SE}} (\overline{x}, \underline{x})$ and $(\underline{w}, \overline{w}) \preceq_{\mathrm{SE}} (\overline{w}, \underline{w})$ we have $(x(t), \widehat{x}(t)) \preceq_{\mathrm{SE}} (\widehat{x}(t), x(t))$ for all $t \geq 0$.

Equivalently, $x(t) \preceq \widehat{x}(t)$ for all $t \geq 0$, and thus $\Phi^E(t; (\underline{x}, \overline{x})) \in \mathcal{T}$. Therefore, $\mathcal{T}$ is forward invariant for (2.34). □

Since (2.34) does not exhibit the symmetry property from Section 2.4.1, observe that while the upper triangle set $\mathcal{T}$ is forward for the deterministic embedding system (2.34), the reflection $\{(x, y) \in \mathcal{X} \times \mathcal{X} \mid y \preceq x\}$ is generally not a forward invariant set, unless $\underline{w} = \overline{w}$. Nonetheless, we next establish a second forward invariant region for (2.34)—the set of points in $\mathcal{T}$ such that the embedding system's vector field points into the southeast cone,

$$\mathcal{S} := \{(x, \widehat{x}) \in \mathcal{T} \mid 0 \preceq_{\mathrm{SE}} E(x, \widehat{x})\}. \tag{2.38}$$

The following lemma is a direct result of [21, Chapter 3, Proposition 2.1].

Lemma 2. The set $\mathcal{S}$ is forward invariant for (2.34), and $\Phi^E(t_1; a) \preceq_{\mathrm{SE}} \Phi^E(t_2; a)$ for all $a \in \mathcal{S}$ and all $0 \leq t_1 \leq t_2$. ■

These results play a key role later in Chapter 4, where we specifically study how invariant regions for (2.1) are identified using invariant regions for the embedding system (2.34). Before this study, we first introduce a method for over-approximating reachable sets of mixed monotone systems in Section 2.4.3.

Remark 3. While the deterministic embedding system (2.34) is straightforwardly derived from the nondeterministic embedding system (2.28), there are important structural differences worth further discussion[1]. Indeed, we have discussed already how (2.34) does not exhibit the symmetry property (2.30) or induce an invariant diagonal space (2.31), unlike (2.28). However, the deterministic embedding system (2.34) *can* induce stable or even globally stable equilibria in its upper-triangular set $\mathcal{T}$, which is not possible in the nondeterministic setting of (2.28), and identifying these equilibria can allow one to reason about forward invariant at attractive regions for the initial system (2.1);

[1]Observe that when the inital system (2.1) contains no disturbance, so that $\dot{x} = F(x)$, the symmetric embedding system (2.28) and the deterministic embedding system (2.34) are the same, *i.e.*, $E(x, \widehat{x}) = \varepsilon(x, \widehat{x})$ always. Thus, in Remark 3, we consider mainly the nondeterministic setting of (2.1), where $\underline{w} \neq \overline{w}$.

see Chapter 4. As a final difference, observe that every symmetric embedding system (2.28) corresponds to a unique mixed monotone system (2.1), since it is true that every function $d(x, w, \widehat{x}, \widehat{w})$ that satisfies the derivative conditions D2–D4 from Definition (6) is a decomposition function for the unique system $\dot{x} = F(x, w)$ with $F(x, w) = d(x, w, x, w)$. A deterministic embedding systems as in (2.34), however, will generally not correspond to a unique inital system (2.1) in the sense that it is generally not possible to recover the inital nondeterministic dynamics (2.1) by studying only the vector field of (2.34). This is a major point of study in Chapter 5, where we show how it is sometimes possible for two different dynamical system, with *different* vector fields and decomposition functions, to admit the *same* deterministic embedding system. ■

2.4.3 Efficient Reachability Analysis for Mixed Monotone Systems

Unlike the initial system (2.1), which is nondeterministic due to the effect of the unknown input, the embedding system (2.34) contains no input and trajectories of (2.34) provide bounds on the reachable set of (2.1), as discussed next in Proposition 2.

Proposition 2 ([30], Proposition 3)**.** *Let* (2.1) *be mixed monotone with respect to* d*. Choose a hyperrectangular set of initial states* $[\![a]\!] \subseteq \mathcal{X}$*, so that* $a \in \mathcal{T} \subset \mathbb{R}^{2n}$*. If* $\Phi^E(\tau; a) \in \mathcal{T}$ *for all* $0 \leq \tau \leq t$*, then*

$$R(t; [\![a]\!]) \subseteq [\![\Phi^E(t; a)]\!]. \tag{2.39}$$

■

Proof. Let $a = (\underline{x}, \overline{x}) \in \mathcal{T}$. Choose $x \in [\![a]\!] = [\underline{x}, \overline{x}]$ and $\mathbf{w} : [0, t] \to \mathcal{W}$ for some $t \geq 0$. Then from (2.28) we have

$$(\phi(t; x, \mathbf{w}), \phi(t; x, \mathbf{w})) = \Phi^\varepsilon(t; (x, x), (\mathbf{w}, \mathbf{w})),$$

$$\Phi^E(t; (\underline{x}, \overline{x})) = \Phi^\varepsilon(t; (\underline{x}, \overline{x}), (\underline{w}, \overline{w})).$$

Since $(\underline{x}, \overline{x}) \preceq_{\mathrm{SE}} (x, x)$ and $(\underline{w}, \overline{w}) \preceq_{\mathrm{SE}} (\mathbf{w}(\tau), \mathbf{w}(\tau))$ for all $\tau \in [0, t]$, we now have

$$\Phi^E(t; (\underline{x}, \overline{x})) \preceq_{\mathrm{SE}} \begin{bmatrix} \phi(t; x, \mathbf{w}) \\ \phi(t; x, \mathbf{w}) \end{bmatrix} \tag{2.40}$$

and thus $\phi(t; x, \mathbf{w}) \in [\![\Phi^E(t; (\underline{x}, \overline{x}))]\!]$. Therefore $R(t; [\![a]\!]) \subseteq [\![\Phi^E(t; (\underline{x}, \overline{x}))]\!]$. $\square$

Proposition 2 provides an efficient procedure for solving the reachability analysis problem, Problem 1; a simulation of the deterministic embedding system for time horizon t, starting from state $(\underline{x}, \overline{x})$, identifies a hyperrectangular over-approximation of $R(t; [\underline{x}, \overline{x}])$ where the largest and smallest points in the rectangular approximation are taken to be the first n and last n coordinates of the simulation endpoint $\Phi^E(t; (\underline{x}, \overline{x}))$. Simulating a deterministic dynamical system is generally a computationally unintensive task and the main benefit of employing the mixed monotonicity property for, *e.g.*, reachability analysis, lies in this efficiency. As a final note, observe that—unlike the monotonicity property, which can be applied to compute the *tightest* hyperrectangle containing a reachable set [21]—the application of the mixed monotonicity can result in *more conservative* reachable set approximations since, in general, $\Phi^E_{1:n}(\,\cdot\,; (\underline{x}, \overline{x}))$ and $\Phi^E_{n+1:2n}(\,\cdot\,; (\underline{x}, \overline{x}))$ are not solutions to the initial system dynamics (2.1) [43]. See Remark 3.

Before moving further, we demonstrate the reachability analysis procedure from Proposition 2 through two examples.

Example 4. Recall from Example 3 that any linear time-invariant system $\dot{x} = Ax + Bw$ is mixed monotone with a decomposition function given by $d(x, w, \widehat{x}, \widehat{w}) = A^{\mathrm{M}+}x + A^{\mathrm{M}-}x + B^{+}w + B^{-}\widehat{w}$. In this case, the deterministic embedding system (2.34) that arises from d is a linear-affine system and is given by

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E(x, \widehat{x}) = \overline{A} \begin{bmatrix} x \\ \widehat{x} \end{bmatrix} + \overline{B} \begin{bmatrix} \underline{w} \\ \overline{w} \end{bmatrix} \tag{2.41}$$

where

$$\overline{A} = \begin{bmatrix} A^{\mathrm{M}+} & A^{\mathrm{M}-} \\ A^{\mathrm{M}-} & A^{\mathrm{M}+} \end{bmatrix} \quad \text{and} \quad \overline{B} = \begin{bmatrix} B^{+} & B^{-} \\ B^{-} & B^{+} \end{bmatrix} \tag{2.42}$$

and where we recall also that $\underline{w}$ and $\overline{w}$ are fixed *a priori* as parameters of the dynamics. As a specific instance of this result, observe that the system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} \begin{bmatrix} -2 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 4 \\ 0 \end{bmatrix} w \tag{2.43}$$

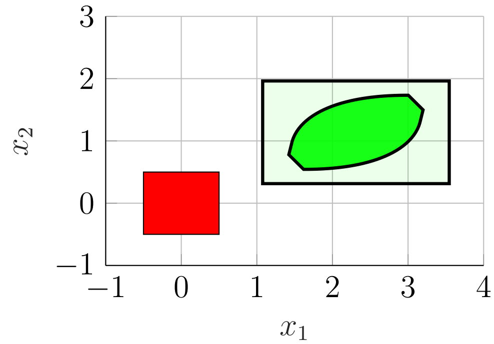
with $x \in \mathbb{R}^2$ and $w \in [1, 2]$ is mixed monotone with respect to

$$d(x, w, \widehat{x}, \widehat{w}) = \begin{bmatrix} -2 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \widehat{x}_1 \\ \widehat{x}_2 \end{bmatrix} + \begin{bmatrix} 4 \\ 0 \end{bmatrix} w \tag{2.44}$$

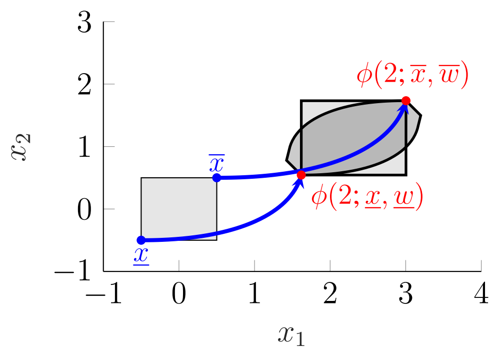
and applying (2.34) with $\underline{w} = 1$ and $\overline{w} = 2$, we attain the deterministic embedding system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{\widehat{x}}_1 \\ \dot{\widehat{x}}_2 \end{bmatrix} = E(x, \widehat{x}) = \begin{bmatrix} -2 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \widehat{x}_1 \\ \widehat{x}_2 \end{bmatrix} + \begin{bmatrix} 4 \\ 0 \\ 8 \\ 0 \end{bmatrix}. \tag{2.45}$$

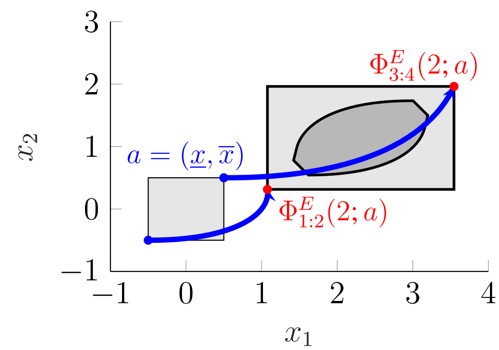
To add further clarity in (2.44) and (2.45), we keep with our color scheme from Example 3 and use the colors Blue-Green and Red to emphasize how the decomposition and embedding function of (2.43) is constructed from the Metzler, and non-Metzler parts of A, respectively. Moreover, Proposition 2 now implies that the time-t reachable set of (2.43) from the rectangular set of initial conditions $[\underline{x}, \overline{x}]$ is efficiently over-approximated using a time-t simulation of the deterministic embedding system (2.45) from initial state $(\underline{x}, \overline{x}) \in \mathcal{T}$. We demonstrate this technique in Figure 2.8 where we take an initial set $[\underline{x}, \overline{x}] = [-\frac{1}{2}, \frac{1}{2}]^2$ and compute a rectangular over-approximation of $R(2; [\underline{x}, \overline{x}])$ via a 2-time-unit simulation of (2.45) from initial state $(\underline{x}, \overline{x}) = (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. ■



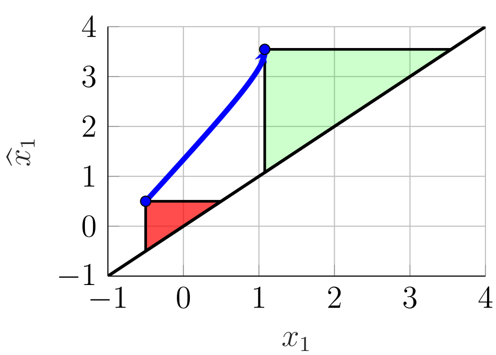
(a)



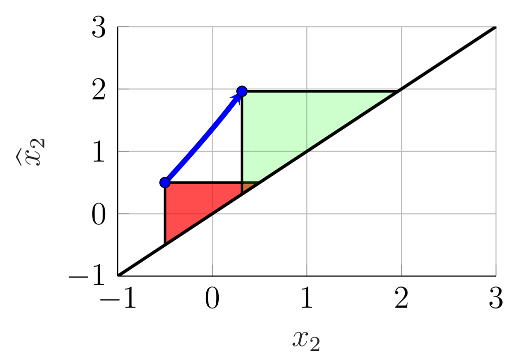
(b)



(c)



(d)



(e)

Figure 2.8: Example 4: Computing reachable sets for (2.43) by applying Proposition 2. Subfigures: (a) The initial set $[\underline{x}, \overline{x}] = [-\frac{1}{2}, \frac{1}{2}]^2$ is shown in red, the time-2 reachable set $R(2; [\underline{x}, \overline{x}])$ is shown in dark green, and the rectangular over-approximation of $R(2; [\underline{x}, \overline{x}])$ attained from the application of Proposition 2 with d from (2.44) is shown in light green. (b) Observe that (2.43) is not a monotone system since $\frac{\partial F}{\partial x} = A$ is not Metzler; therefore, $R(2; [\underline{x}, \overline{x}]) \not\subseteq [\phi(2; \underline{x}, \underline{w}), \phi(2; \overline{x}, \overline{w})]$. (c) The system (2.43) is mixed monotone and the first 2 and last 2 coordinates of $\Phi^E(2; (\underline{x}, \overline{x}))$ form a rectangle containing $R(2; [\underline{x}, \overline{x}])$. To add further clarity, we depict the embedding system trajectory $\Phi^E(\,\cdot\,; (\underline{x}, \overline{x}))$ graphically in (d) and (e), through its projections onto the x_1–$\widehat{x}_1$ and x_2–$\widehat{x}_2$ planes, respectively.

Example 5. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_2^2 + 2 \\ x_1 \end{bmatrix} \tag{2.46}$$

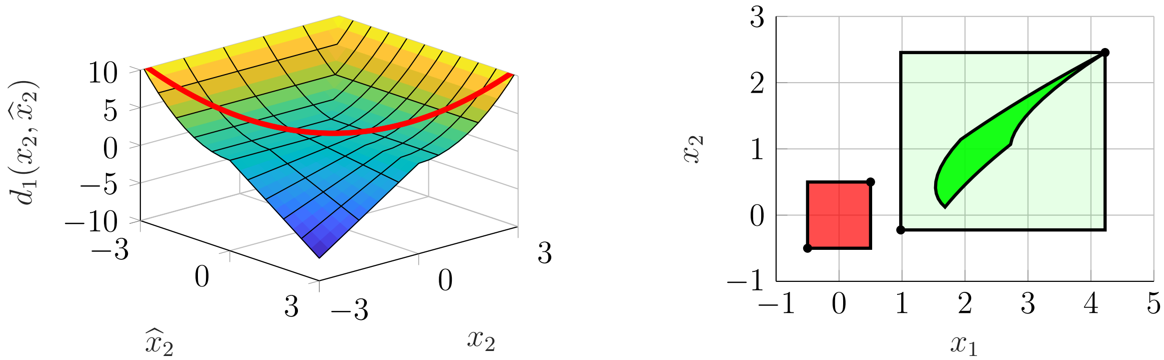
with state $x \in \mathbb{R}^2$ and no disturbance input. Consider also d given elementwise by

$$\begin{aligned} d_1(x, \widehat{x}) &= \begin{cases} x_2^2 + 2 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2 \\ \widehat{x}_2^2 + 2 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 \leq -\widehat{x}_2 \\ x_2\widehat{x}_2 + 2 & \text{if } x_2 \leq 0 \text{ and } \widehat{x}_2 \geq 0 \end{cases} \\ d_2(x, \widehat{x}) &= x_1. \end{aligned} \tag{2.47}$$

While d from (2.47) is given as a piecewise function of x and $\widehat{x}$, and is perhaps more difficult to visualize than, *e.g.*, the decomposition function construction for linear time-invariant systems (2.24), d from (2.47) is indeed a decomposition function for (2.46). To see this, observe that $d(x, x) = F(x)$ always, and the partial derivatives

$$\begin{aligned} \frac{\partial d_1}{\partial x_2}(x, \widehat{x}) &= \begin{cases} 2x_2 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2 \\ 0 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 \leq -\widehat{x}_2 \\ \widehat{x}_2 & \text{if } x_2 \leq 0 \text{ and } \widehat{x}_2 \geq 0, \end{cases} & \frac{\partial d_1}{\partial \widehat{x}_2}(x, \widehat{x}) &= \begin{cases} 0 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2 \\ 2\widehat{x}_2 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 \leq -\widehat{x}_2 \\ x_2 & \text{if } x_2 \leq 0 \text{ and } \widehat{x}_2 \geq 0 \end{cases} \\ \frac{\partial d_2}{\partial x_1}(x, \widehat{x}) &= 1 & \frac{\partial d_2}{\partial \widehat{x}_1}(x, \widehat{x}) &= 0 \end{aligned} \tag{2.48}$$

satisfy the mixed monotonicity conditions D2–D4. We show later in Chapter 3 that when constructing decomposition functions it is common to arrive at such a piecewise structure. To add further clarity, we plot $d_1(x, \widehat{x})$ in Figure 2.9(a) above the x_2–$\widehat{x}_2$, as to shine light on derivative conditions in Definition 6. Secondly, we apply Proposition 2 using d from (2.47) in order to compute a hyperrectangular over-approximation of $R(2; [\underline{x}, \overline{x}])$ from set of inital conditions $[\underline{x}, \overline{x}] = [-\frac{1}{2}, \frac{1}{2}]^2$.



(a) (b)

Figure 2.9: Example 5: Decomposition function and reachable set over-approximations for (2.46). Subfigures: (a) the first entry of the decomposition function $d_1(x, \widehat{x})$ from (2.47) is plotted above the x_2–$\widehat{x}_2$ plane, where we label the z-axis $d_1(x_2, \widehat{x}_2)$ to emphasize the fact that d_1 is dependant only on the second coordinates of x and $\widehat{x}$. Observe that $d_1(x, \widehat{x})$ evaluates to $F_1(x)$ when $x = \widehat{x}$, *i.e.*, d_1 satisfies the first condition in Definition 6 since F is embedded on the diagonal of d. Similarly, $d_1(x_2, \widehat{x}_2)$ is increasing in x_2 and decreasing $\widehat{x}_2$, *i.e.*, d_1 satisfies the remaining derivative conditions in Definition 6. (b) The initial set $[\underline{x}, \overline{x}] = [-\frac{1}{2}, \frac{1}{2}]^2$ is shown in red, the time-1 reachable set $R(1;\, [\underline{x}, \overline{x}])$ is shown in dark green, and the hyperrectangular over-approximation of $R(1;\, [\underline{x}, \overline{x}])$ attained from the application of Proposition 2 with d from (2.47) is shown in light green. The vectors $\underline{x}, \overline{x}, \Phi^E_{1:2}(1;\, (\underline{x}, \overline{x}))$ and $\Phi^E_{3:4}(1;\, (\underline{x}, \overline{x}))$ are also shown as black dots.

Simulation results are provided in Figure 2.9(b).

■

Remark 4. Note that in the application of Proposition 2, a decomposition function $d(x, w, \widehat{x}, \widehat{w})$ will only ever be evaluated when either $(x, w) \preceq (\widehat{x}, \widehat{w})$ or when $(\widehat{x}, \widehat{w}) \preceq (x, w)$. This is a result of Lemma 1 and the fact that the initial state $a \in \mathcal{T}$. For this reason, it is generally possible to relax the conditions of Definition 6 so that a decomposition function is valid when conditions D2–D4 are satisfied only on $\{(x, w, \widehat{x}, \widehat{w}) \in \mathcal{X} \times \mathcal{W} \times \mathcal{X} \times \mathcal{W} \mid (x, w) \preceq (\widehat{x}, \widehat{w}) \text{ or } (\widehat{x}, \widehat{w}) \preceq (x, w)\}$. Further discussion on this point is provided in Chapter 3 where we present an algorithm for constructing decomposition functions on this domain. ■

As a final point, observe that mixed monotone reachability methods exhibit a useful *nesting* so that when $A = [\underline{x}, \overline{x}]$ and $B = [\underline{y}, \overline{y}]$ are hyperrectangles with $A \subseteq B$, it holds also that

$$[\![\Phi^E(t; (\underline{x}, \overline{x}))]\!] \subseteq [\![\Phi^E(t; (\underline{y}, \overline{y}))]\!], \tag{2.49}$$

for all $t \geq 0$. Equivalently, when $A \subseteq B$, the hyperrectangular approximation containing $R(t; A)$ will contain that of $R(t; B)$ for all $t \geq 0$. We apply this observation later in Chapter 3 in order to reason about the *tightness* of decomposition functions and mixed monotone reachable set over-approximations.

2.5 Discussion on Mixed Monotonicity

Mixed monotonicity and the results of Proposition 2 provide a powerful technique for solving the reachability analysis problem, Problem 1. This technique has three main steps:

(i) Construct a decomposition function d for (2.1). In general, such decomposition functions are constructed without explicit knowledge of $\underline{w}, \overline{w}$.

(ii) Construct the embedding function E from (2.34) using the decomposition function d and the disturbance bounds $\underline{w}, \overline{w}$.

(iii) Conduct a t-time-unit simulation of the embedding system (2.34) from inital state $a \in \mathcal{T}$ in order to attain a hyperrectangular over-approximation of $R(t; [\![a]\!])$. See Proposition 2.

In particular, once step (i) above is solved, and a decomposition function is obtained for (2.1), generally speaking, steps (ii) and (iii) are straightforward to complete, since it is true that conducting a simulation of a deterministic system is not computationally or conceptually challenging. As such, the main challenge in employing the mixed monotonicity property in applications is in constructing a decomposition function for one's system, *i.e.*, completing step (i) above.

The general theory of how decomposition functions are formed is the subject of the next chapter, where our main result is to show that all dynamical systems bearing a locally Lipschitz continuous vector field are mixed monotone. We observe, in particular, that an arbitrary system as in (2.1) will generally be mixed monotone with respect to multiple different decomposition functions; however certain decomposition functions may provided more conservative estimates of reachable sets than others when used with Proposition 2. Nonetheless, computing a suitable decomposition function in one's setting can be a challenging problem, or not possible, and there do not exist universal algorithms for doing so. As a rule of thumb, useful decomposition functions should be such that $d(x, w, \widehat{x}, \widehat{w})$ is close to $F(x, w)$ when x is close to $\widehat{x}$ and w is close to $\widehat{w}$, but we do not provide a formal notion of closeness and observe that decomposition function construction usually leverages structural properties of F or domain knowledge of the underlying physical system; see [53] for representative examples.

2.6 Related Notions

While mixed monotonicity itself provides an efficient means of solving the reachability analysis problem, there are, indeed, other related techniques in literature for computing hyperrectangular over-approximations reachable sets. This section serves to highlight several of these approaches.

We begin, in Section 2.6.1, with a discussion on mixed monotonicity in the context of *discrete-time* systems with disturbances. Just as in the continuous-time setting, mixed monotone discrete-time systems are defined in reference to a related decomposition function that separates the system's update-map into cooperative and competitive state interactions. Such a decomposition function then enables efficient reachability analysis for the inital discrete-time system using a similar approach to that of the continuous-time setting. In the context of discrete-time mixed monotonicity, however, we take a different formal definition for decomposition functions from that presented in Section 2.4. An important observation made in this section is that decomposition functions for continuous-time mixed monotone systems can be computed using the tools of discrete-time mixed monotonicity; however, applying this techniques generally results in decomposition functions that provide overly-conservative reachable set approximations. Nonetheless, computing decomposition functions for continuous-time systems using discrete-time mixed monotonicity becomes most reveling when studied through the tools of *interval reachability analysis*.

It is particularly interesting to observe the connection between discrete-time mixed monotonicity and *interval reachability analysis* [65–67], as discussed more thoroughly in Section 2.6.2. The fundamental tool of interval reachability analysis is the *inclusion function*, which is used to over-approximate the image of a vector-valued function using a hyperrectangle. In the context of dynamical systems, such an inclusion function can then be used to over-approximate a system's reachable set in either continuous-time or discrete-time [65, 68]. In Section 2.6.2, we show an equivalence between the discrete-time mixed monotonicity and interval reachability analysis in the sense that an inclusion function for the update-map of a discrete-time system will induce a corresponding decomposition function for the same system that is capable of producing the same reachable set approximation when used with the tools of discrete-time mixed monotonicity. Several works exploit this connection to generate decomposition functions for *continuous-time* systems using an inclusion function for the system's vector field [42, 54].

As a final related tool, we also provide a brief discussion on *contractive* dynamical systems in Section 2.6.3 [64, 69]. See also [45, 46] which use contraction theory, together with mixed monotonicity, in order to verify safety properties for neural networks.

2.6.1 Mixed Monotonicity for Discrete-Time Dynamical Systems

We have already discussed, in Section 2.4, mixed monotonicity in the context of continuous-time dynamical systems. In this section, we study the related notion of mixed monotonicity in the context of discrete-time dynamical systems.

We consider a nondeterministic discrete-time system

$$x^+ = F(x, w) \tag{2.50}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$ is the state and $w \in \mathcal{W} \subseteq \mathbb{R}^m$ is the disturbance, and where x^+ denotes the state of (2.50) at the next time step. As before, we assume that $\mathcal{X}$ is an extended hyperrectangle and that $\mathcal{W} := [\underline{w}, \overline{w}]$ is a hyperrectangle for some $\underline{w}, \overline{w} \in \mathbb{R}^m$ with $\underline{w} \preceq \overline{w}$. Last, we assume that the update map $F : \mathcal{X} \times \mathcal{W} \to \mathbb{R}^n$ is continuous in its inputs. Note that F is not required to map only to $\mathcal{X}$, however, the results below hold as long as the state trajectory remains in $\mathcal{X}$ for all time. Mixed monotonicity in the context of (2.50) is defined as follows.

Definition 7 (Mixed Monotonicity for Discrete-Time Systems [55])**.** Given a continuous function

$d : \mathcal{X} \times \mathcal{W} \times \mathcal{X} \times \mathcal{W} \to \mathbb{R}^n$, the system (2.50) is mixed monotone with respect to d if for all $x, \widehat{x} \in \mathcal{X}$ and all $w, \widehat{w} \in \mathcal{W}$ all of the following hold:

- F is embedded on the diagonal of d; that is

$$d(x, w, x, w) = F(x, w). \tag{2.51}$$

- $\frac{\partial d}{\partial x}(x, w, \widehat{x}, \widehat{w})$ is a positive matrix and $\frac{\partial d}{\partial \widehat{x}}(x, w, \widehat{x}, \widehat{w})$ is a negative matrix.
- $\frac{\partial d}{\partial w}(x, w, \widehat{x}, \widehat{w})$ is a positive matrix and $\frac{\partial d}{\partial \widehat{w}}(x, w, \widehat{x}, \widehat{w})$ is a negative matrix. ■

As in the continuous-time case, when (2.50) is mixed monotone with respect to d, a deterministic monotone embedding systems can be constructed from the decomposition function

$$\begin{bmatrix} x^+ \\ \widehat{x}^+ \end{bmatrix} = E(x, \widehat{x}) = \begin{bmatrix} d(x, \underline{w}, \widehat{x}, \overline{w}) \\ d(\widehat{x}, \overline{w}, x, \underline{w}) \end{bmatrix} \tag{2.52}$$

with state $(x, \widehat{x}) \in \mathcal{X} \times \mathcal{X}$. Furthermore, the deterministic embedding system (2.52) retains the monotonicity property of its continuous-time counterpart (2.34):

$$E(x, \widehat{x}) \preceq_{\mathrm{SE}} E(x', \widehat{x}') \tag{2.53}$$

hold for all $(x, \widehat{x}) \preceq_{\mathrm{SE}} (x', \widehat{x}')$. This fact allows for employing the embedding system (2.52) for finite-time reachability analysis in a manner similar to that in the continuous time case. In particular,

$$x(k+1) = F(x(k), w(k)) \in [\![E(\underline{x}, \overline{x})]\!] \tag{2.54}$$

for all $x(k) \in [\underline{x}, \overline{x}] \subset \mathcal{X}$, all $w(k) \in \mathcal{W}$, and all k.

Observe that the first and second derivative conditions in Definition 7 are the same in the sense that a decomposition function d must be monotonically non-decreasing in its first two arguments monotonically non-increasing in its second two arguments, where now, unlike the continuous-time setting, d_i's dependence on x_i is important. In this way, when $x^+ = F(x, w)$ is mixed monotone with respect to $d(x, w, \widehat{x}, \widehat{w})$ we also have that

$$x^+ = f(v) = F(x, w) \tag{2.55}$$

is mixed monotone with respect to

$$d^f(v, \widehat{v}) := d(x, w, \widehat{x}, \widehat{w}) \tag{2.56}$$

where $v := (x, w) \in \mathcal{X} \times \mathcal{W}$ in (2.55) is viewed as a disturbance. Furthermore, we observe that when the discrete-time system $x^+ = F(x, w)$ is mixed monotone with respect to $d(x, w, \widehat{x}, \widehat{w})$, the continuous-time system $\dot{x} = F(x, w)$ is mixed monotone with respect to $d(x, w, \widehat{x}, \widehat{w})$ as well, where now the update map F is considered as a vector-field; in this instance, we also have d', defined element-wise by

$$d'_i(x, w, \widehat{x}, \widehat{w}) = d_i(x, w, \widehat{x}_{[i:x]}\widehat{w}), \tag{2.57}$$

is a decomposition function for $\dot{x} = F(x, w)$ and where we recall $\widehat{x}_{[i:x]} \in \mathcal{X}$ denotes the vector $\widehat{x}$ but where the i^{th} entry has been replaced by the i^{th} entry of $x \in \mathcal{X}$. A demonstration of this fact is provided next in Example 6.

Example 6. Consider the discrete-time system

$$\begin{bmatrix} x_1^+ \\ x_2^+ \end{bmatrix} = F(x) = \begin{bmatrix} |x_1 - x_2| \\ -x_1 \end{bmatrix} \tag{2.58}$$

with $\mathcal{X} = \mathbb{R}^2$, which is mixed monotone with respect to d given by

$$d_1(x,\,\widehat{x}) = \begin{cases} 0 & \text{if } \max\{\underline{x}_1, \underline{x}_2\} \leq \min\{\overline{x}_1, \overline{x}_2\}, \\ \min\langle x, \widehat{x}\rangle & \text{if } x_1 \leq \widehat{x}_1 \leq x_2 \leq \widehat{x}_2 \text{ or } x_2 \leq \widehat{x}_2 \leq x_1 \leq \widehat{x}_1, \\ \max\langle \widehat{x}, x\rangle & \text{if } \widehat{x} \preceq x, \end{cases} \tag{2.59}$$

$$d_2(x,\,\widehat{x}) = -\widehat{x}_1.$$

Consider also the continuous-time system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x) = \begin{bmatrix} |x_1 - x_2| \\ -x_1 \end{bmatrix} \tag{2.60}$$

with $\mathcal{X} = \mathbb{R}^2$, which is mixed monotone with respect to d' given by

$$d_1'(x,\,\widehat{x}) = \begin{cases} 0 & \text{if } x_2 \leq x_1 \leq \widehat{x}_2, \\ x_2 - x_1 & \text{if } 2x_1 \leq \min\{2x_2,\, x_2 + \widehat{x}_2\}\ , \\ x_1 - \widehat{x}_2 & \text{if } 2x_1 \geq \min\{2\widehat{x}_2,\, x_2 + \widehat{x}_2\}, \end{cases} \tag{2.61}$$

$$d_2(x,\,\widehat{x}) = -\widehat{x}_1.$$

Observe that $d'(x, w, \widehat{x}, \widehat{w}) = d(x, w, \widehat{x}_{[i:x]}, \widehat{w})$. ■

2.6.2 Interval Reachability Analysis

A second reachability analysis tool, that applies mainly in the discrete-time setting of (2.50), is in *interval reachability analysis* [20, 66].

Interval reachability analysis studies the problem of over-approximating the image of a function, over a hyperrectangular domain of inputs. In other words, given a vector-valued function

$F : \mathbb{R}^n \to \mathbb{R}^m$, the goal is to construct a set-valued map $\mathbf{F} : \mathbb{IR}^n \to \mathbb{IR}^m$ so that

$$F(x) \in \mathbf{F}(A) \quad \text{when} \quad x \in A \tag{2.62}$$

for all rectangles $A \in \mathbb{IR}^n$, and where $\mathbb{IR}^n$ and $\mathbb{IR}^m$ denote the sets of interval subsets of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively, and are given by

$$\begin{aligned}\mathbb{IR}^n &:= \{[\underline{x}, \overline{x}] \subseteq \mathbb{R}^n \mid \underline{x}, \overline{x} \in \mathbb{R}^n, \underline{x} \preceq \overline{x}\} \subset 2^{\mathbb{R}^n},\\ \mathbb{IR}^m &:= \{[\underline{y}, \overline{y}] \subseteq \mathbb{R}^m \mid \underline{y}, \overline{y} \in \mathbb{R}^m, \underline{y} \preceq \overline{y}\} \subset 2^{\mathbb{R}^m}.\end{aligned} \tag{2.63}$$

In this case, we refer to the set-valued map $\mathbf{F}$ as an *inclusion function* for F [66, Sec. 2.4.1]. Furthermore, we generally impose a few basic assumptions on inclusion functions so that, ***e.g.***, we assume always $\mathbf{F}(x) = F(x)$ for all $x \in \mathbb{R}^n$ and $\mathbf{F}(A) \subseteq \mathbf{F}(B)$ when $A \subseteq B$.

There are known similarities between mixed monotone systems theory and interval reachability analysis, as highlighted recently in [42, 54]. Both theories provide efficient techniques for over-approximating reachable sets using hyperrectangles and, of particular importance, inclusion functions can be generated from decomposition functions. That is, given a discrete-time dynamical system

$$x^+ = F(x), \tag{2.64}$$

where $x \in \mathcal{X}$ is the state, the interval function

$$\mathbf{F}([\underline{x}, \overline{x}]) := [d(\underline{x}, \overline{x}), d(\overline{x}, \underline{x})] \tag{2.65}$$

is an inclusion function for F when $d(x, \widehat{x})$ is a decomposition function for (2.64). Moving in the reverse direction, it is also generally possible to construct decomposition functions for mixed monotone systems using an inclusion function for the system's update map or vector field, and we explore this connection further in the next chapter.

Indeed, in the next chapter, we present a more formal study on how decomposition functions are constructed for mixed monotone systems and one may wonder whether preexisting results in the area of interval reachability analysis can leveraged for these purposes. There are, for example, existing toolboxes for generating inclusion functions and conducting interval reachability analysis, such as the COntinuous Reachability Analyzer (CORA) toolbox [70–72]. We generally observe that while tools such as CORA can be leveraged to compute reachable set over-approximations using hyperrectangles, it can often be difficult to back out closed-form representations for inclusion functions using these tools and, in our work, we are most interested in these closed-form representations. This is due to the fact that closed-form representations for decomposition functions are requisite when conducting stability analysis for the embedding system (2.34), an application discussed more thoroughly in Chapter 4.

2.6.3 ℓ_∞ Contractive Systems

Another efficient procedure for over-approximating reachable sets using hyperrectangles comes from the theory of *contractive dynamical systems* [73]. A continuous-time dynamical system, without a disturbance input, is said to be contracting when an appropriate *matrix measure* of the system's Jacobian matrices is uniformly negative for all states in the system state space. Such a matrix measure is defined with respect to a vector norm, and in specific instance where the ℓ_∞-norm is used, contraction can be used to reason about, *e.g.*, the growth of reachable sets from initial sets that are hyperrectangular [74, Section 2.5], since it is true the sublevel-sets of ℓ_∞ norm equate to hyperrectangular regions of the system state space. While there are, indeed, certain similarities and connections between contraction and mixed monotonicity, we do not provide a formal definition or thorough discussion on contraction here. As a particular connection, however, we recall that computing a matrix measure, when taken with respect to either the ℓ_1 norm or the ℓ_∞, will involve computing a Metzler-matrix representation of the system's Jacobian matrix [75]. Further results on the contraction property and its applications in efficient reachability analysis are collected in [19, 76], and see also [45, 64].

2.7 Conclusion

We have presented, in this chapter, the mixed monotonicity property of dynamical systems, which is shown to provide a powerful approach for solving the reachability analysis problem using hyperrectangles. A fundamental tool in the application of mixed monotonicity is the decomposition function, which separates the system dynamics into cooperative and competitive state interactions and which facilitates efficient reachability analysis through the simulation of a related deterministic embedding system. While we have demonstrated this result thoroughly, we have not yet provided a formal theory as to *when* a system is mixed monotone, *i.e.*, when a decomposition function exists and *how* to compute it. Answering these the fundamental questions is subject of the next chapter, where we present several tools for computing decomposition functions for mixed monotone systems. In particular, our main result in Chapter 3 is to show that all continuous-time systems are mixed monotone with respect to a unique *tight decomposition function*, applicable to any system. Further tools for reachability analysis using mixed monotone systems theory are provided in Chapter 4.

2.8 Exercises

Problem 2.1: Consider the 1-dimensional linear time-invariant system

$$\dot{x} = -x \tag{2.66}$$

with state $x \in \mathbb{R}$ and no disturbance. Indeed, (2.66) is a monotone dynamical system, since (2.66) contains $n = 1$ state and no disturbance input; see Section 2.2. Using Proposition 1, compute an interval over-approximation of $R(1, A)$ where the initial set is taken to be $A = [10, 15]$. Can the reachable set $R(1, A)$ be computed *exactly* using this approach? If so, why?

Even though (2.66) is a monotone system, and reachable sets can be computed exactly via the application of Proposition 1, the system (2.66) is also mixed monotone. Consider the following three functions

1. $d^1(x, \widehat{x}) = -x$

2. $d^2(x, \widehat{x}) = -\widehat{x}$

3. $d^3(x, \widehat{x}) = -\frac{1}{2}x - \frac{1}{2}\widehat{x}$

with scalar inputs $x, \widehat{x} \in \mathbb{R}$. Show that (2.66) is mixed monotone with respect to each of the functions $d^1(x, \widehat{x})$, $d^2(x, \widehat{x})$ and $d^3(x, \widehat{x})$.

Using each of these decomposition functions, apply the reachability analysis procedure given in Proposition 2 to compute an interval over-approximation of $R(1, [10, 15])$. How do these approximations differ from those attained using Proposition 1? What may be the reason for this discrepancy? Hint: What are the stability properties of the embedding systems in these three cases?

Problem 2.2: Let $x, \widehat{x} \in \mathbb{R}^2$ and $w, \widehat{w} \in \mathbb{R}$, and consider the function

$$d(x, w, \widehat{x}, \widehat{w}) = \begin{bmatrix} -7/4 & 0 \\ 5/4 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} -1/4 & -1 \\ -1/4 & 0 \end{bmatrix} \begin{bmatrix} \widehat{x}_1 \\ \widehat{x}_2 \end{bmatrix} + \begin{bmatrix} 4 \\ 1/2 \end{bmatrix} w + \begin{bmatrix} 0 \\ -1/2 \end{bmatrix} \widehat{w} \tag{2.67}$$

Is d from (2.67) a decomposition function for *some* system? If so, which system? Hint: See Remark 3.

Practice computing reachable set over-approximations with Proposition 2 and the decomposition function d from (2.67), if applicable. How do the reachable sets approximations derived from d compare to the reachable sets derived approximations in Example 4? What might be the reason for any discrepancy? Hint: See Problem 2.1.

Problem 2.3: How might you go about deriving a decomposition function for the 2-dimensional deterministic system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_1^3 + x_2 \\ -x_1^2 \end{bmatrix} \tag{2.68}$$

with state $x \in \mathbb{R}^2$? Hint: See Example 5. Does there exists a subset of the state space $\mathcal{X} \subseteq \mathbb{R}^2$

so that (2.68) is a monotone system on $\mathcal{X}$? Use this observation to justify why, in Example 5, the rectangular over-approximation of $R(1;\,[\underline{x},\overline{x}])$ contains $\Phi^E_{1:2}(1;\,[\underline{x},\overline{x}])$, *i.e.*, the reachable set over-approximation touches the true reachable set.

CHAPTER 3

DECOMPOSITION FUNCTIONS FOR MIXED MONOTONE SYSTEMS

Just as a Lyapunov function provides means for studying the stability properties of a nonlinear system, a decomposition function provides means for studying reachability and invariance, through the mixed monotonicity property and the deterministic embedding system of Section 2.4.2. Indeed, we have shown already in Chapter 2 how a decomposition function enables the efficient over-approximation of reachable sets for nonlinear systems and we extend these results in Chapter 4 where we show how this same decomposition function can be used for, for example, computing backward-time reachable sets and forward invariant sets. To that end, in this chapter, we attempt to establish a foundational theory as to *how* decomposition functions are constructed for mixed monotone systems. In doing so, we reveal the generality of the mixed monotonicity property and we demonstrate the unique benefit of employing mixed monotonicity in applications.

A main result in this chapter is to show that all continuous-time systems bearing a locally Lipschitz continuous vector field are mixed monotone and we observe, in particular, that an arbitrary dynamical system will usually be mixed monotone with respect to many *different* decomposition functions. It may further be the case that certain decomposition functions for a system provide less-conservative reachable set approximations than others when used with the tools provided in Chapter 2, and these observations motivate the need for new methods of obtaining decomposition functions and reasoning about their *tightness*. Nonetheless, analogous to searching for Lyapunov functions, constructing closed-form decomposition functions for complex systems can be difficult, and there do not exist universal techniques for doing so.

One classical approach for constructing decomposition functions—that is known to be broadly applicable [31]—involves using single-sided bounds on a system's Jacobian matrices [29, 34, 35]. Such decomposition functions can generally be obtained and evaluated simply, thus aiding in applications where, *e.g.*, decomposition functions need be constructed on-the-fly for high-dimensional nonlinear systems; see [52] for an application of this kind in machine learning. Despite these advantages, this approach is generally understood to produce overly-conservative decomposition functions, except in a few, albeit important, special cases, such as when the inital system is linear time-invariant or admits sign-stable Jacobian matrices [53]. See also [54].

Conservatism in mixed monotone reachable set approximations was first studied in [55], in a discrete-time setting, where it was shown that all discrete-time systems are mixed monotone with respect to a unique *tight decomposition function* that can be applied to compute the tightest hyperrectangle containing a system's 1-step reachable set. This tight decomposition function is defined as an optimization problem and evaluating the decomposition function at any point in the embedding space requires explicitly computing or reasoning about the reachable set itself. For this reason, tight decomposition functions in discrete-time do not provide many practical benefits in solving the reachability analysis problem; nonetheless, knowing that a decomposition function does exist means that a search directed by, *e.g.*, domain expertise, is not generally unreasonable.

In this chapter, we mainly concern ourselves with continuous-time systems and we present a basic theory of *how* conservatism enters the reachability analysis procedure. Unlike in the discrete-time setting, continuous-time mixed monotonicity cannot generally be applied to compute the tightest hyperrectangle containing a reachable set, except in certain special cases such as when a system is monotone. Nonetheless, we prove an analogous result by providing a construction for a similar *tight decomposition function* that provides the tightest approximations of reachable sets attainable when used with the continuous-time tools. Our construction is similarly defined as an optimization problem, however, unlike in the discrete-time setting, computing a tight decomposition function for a continuous-time system does not require computing or reasoning about the system's reachable set explicitly. This distinction makes it so that tight decomposition functions are significantly easier to evaluate in the continuous-time setting and we show through a series of examples how, in certain instances, a tight decomposition function may be attained in closed-form.

Even when a tight decomposition function is available in closed-form, however, we observe that it is often defined as a piece-wise expression, and the number of pieces can scale exponentially with the dimension of the state and input spaces. This observation appears to contradict the purported benefit of employing mixed monotonicity in applications: a main benefit, as discussed earlier in Chapter 2, is that reachable sets for an n-dimensional mixed monotone system with disturbances can efficiently over-approximated via a single simulation of a related $2n$-dimensional embedding system constructed from the decomposition function. However, in instances where evaluating the tight decomposition function requires a large number of function evaluations, the tractability of the approach diminishes, and one cannot expect computations to scale linearly in the state dimension. Furthermore, the complexity of our construction is representative of a larger trade-off in mixed monotone systems theory: generally, decomposition functions that provide *tighter* approximations of reachable sets are also more difficult to evaluate algorithmically.

Regardless, in our experience, it is most beneficial to attempt to generate a tight decomposition function for one's system from the onset of analysis; rather than attempt to generate a more-conservative decomposition function, first. We observe, in particular, that often-times a more-conservative decomposition function will in fact require more function evaluations than a tight decomposition function for the same system. Furthermore, once a tight decomposition function is attained in closed-form, it is sometimes possible to remove pieces and reduce function evaluations, in order to arrive at a more-conservative decomposition function, that is less-complex to evaluate algorithmically. In this chapter, we make heavy use of these insights to apply mixed monotonicity to practically meaningful systems where naive Jacobian-bounds provide woefully conservative reachable set approximations.

We begin, in Section 3.1 by introducing the *kinematic unicycle model* dynamics which will become a primary case study in this chapter; throughout, we present several different methods for decomposing the unicycle dynamics, and we compare each of the decomposition functions obtained in terms of their conservatism and and their computational complexity. As a first technique, we show in Section 3.2 how decomposition functions can sometimes be constructed from single-sided bounds on the system Jacobian matrices. An important observation made in this section is that, generally speaking, many different decomposition functions for the same system can be produced using Jacobian-bounds, and this observation motivates the need for new techniques of obtaining and reasoning about decomposition functions. To address this point, we provide, in Section 3.3, a basic theory of how conservatism enters the reachability analysis procedure and this theory is presented alongside a set of technical lemmas. Then, following this theory, we show in Section 3.4 that all continuous-time dynamical system, possibly subject to a disturbance input, are mixed monotone and we provide an explicit construction for the unique tight decomposition function that provides the tightest attainable approximations of reachable sets. Our construction is presented, initially, as a nonconvex optimization problem evaluated over a hyperrectangular set of states. However, we show through example how a tight decomposition function can sometimes be computed in closed-form and, in Section 3.5 of this work, we present a basic method for obtaining closed-form representations. A concluding case study is presented in Section 3.6 where we compute a tight decomposition function for a 4-dimensional nonlinear bicycle model in closed-form using this approach.

3.1 Example and Opening Remarks

There are many different results, methods and nuances that must be understood in the study of how decomposition functions are formed for general nonlinear systems. As these nuances present themselves throughout this chapter, we attempt, when possible, to demonstrate each through an illustrative example. A particular system of interest in this chapter, which will become a recurring example in the later sections, is the *kinematic unicycle model*.

Definition 8. The main application example in this section is the *kinematic unicycle model*,

$$\begin{aligned} \dot{p}_x &= v\cos(\theta) \\ \dot{p}_x &= v\sin(\theta) \\ \dot{\theta} &= \omega \end{aligned} \tag{3.1}$$

where $(p_x, p_y) \in \mathbb{R}^2$ and $\theta \in \mathbb{R}$ denote the position and rotation of the unicycle and $v \in \mathbb{R}$ and

$\omega \in \mathbb{R}$ are the linear and angular velocities, respectively. We allow for a multiple cover of the rotation space in the sense that we allow $\theta(t) \in \mathbb{R}$ instead of, *e.g.*, only $[0, 2\pi)$, for example. Moreover, for purposes of clarity, we generally represent the dynamics (3.1) as

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = F^{\text{uni}}(x, w) = \begin{bmatrix} w_1 \cos(x_3) \\ w_1 \sin(x_3) \\ w_2 \end{bmatrix} \tag{3.2}$$

where $x = (p_x, p_y, \theta) \in \mathbb{R}^3$ is now the state vector and $w = (v, \omega) \in \mathbb{R}^2$ is taken to be a disturbance input in the sense of (2.1). ■

In the following sections, we present several different methods for decomposing the unicycle dynamics (3.2), and we compare each of the decomposition functions obtained in terms of their conservatism and and their computational complexity. Furthermore, in certain early demonstrations where we believe it is preferable, we consider in place of (3.2) a reduced 1-dimensional model,

$$\dot{x} = F^{\cos}(w) = \cos(w) \tag{3.3}$$

with state $x \in \mathbb{R}$ and disturbance $w \in \mathbb{R}$. While it is true that (3.3) presents a significant simplification of (3.2) that contains only one state and one disturbance, there are important reasons for studying, first, the simplified model (3.3) and we attempt to highlight these reasons later through discussion in Section 3.3.

3.2 The Jacobian-Bound Construction

We have already provided, in the last chapter, several preliminary examples and special cases for how and when decomposition functions can be constructed, *e.g.*, in the cases where (2.1) is monotone (Definition 3) or linear time-invariant (Example 3). In this section, we both unify and generalize these special cases through a framework for computing decomposition functions for systems whose state and disturbance Jacobian matrices are uniformly bounded on one side [29].

An important observation made in this section is that, generally speaking, many *different* decomposition functions for the same system can be produced using Jacobian-bounds, and certain of these decomposition functions may provide more or less conservative reachable set approximations than others when used with Proposition 2. Moreover, this observation motivates the need for new techniques of obtaining and reasoning about decomposition functions, which will become a main focus of the later sections of this chapter.

We consider, first, the problem of rewriting a system's vector field as the *sum* of two functions: one that is monotonically non-decreasing in its inputs and one that is monotonically non-increasing. In other words, given $F(x, w)$ the goal is to construct two functions $f : \mathcal{X} \times \mathcal{W} \to \mathbb{R}^n$ and $g : \mathcal{X} \times \mathcal{W} \to \mathbb{R}^n$ so that

- $F(x, w) = f(x, w) + g(x, w)$,
- $\frac{\partial f}{\partial x}(x, w)$ is a Metzler matrix and $\frac{\partial f}{\partial w}(x, w)$ is a positive matrix, and
- $\frac{\partial g}{\partial x}(x, w)$ is a negative matrix and $\frac{\partial g}{\partial w}(x, w)$ is a negative matrix.

When such a *decomposition* can be achieved, observe that the system $\dot{x} = F(x, w)$ is mixed monotone, and a decomposition function for this system is given by

$$d(x, w, \widehat{x}, \widehat{w}) = f(x, w) + g(\widehat{x}, \widehat{w}). \tag{3.4}$$

Many relevant pieces of literature exploit this observation to compute decomposition functions for (2.1), in cases where, *e.g.*, given F, there are natural choices for f and g [32]. A particular classical technique for constructing decomposition functions in this manner involves forming f and g from bounds on the system's Jacobian matrices; see Proposition 3.

Proposition 3 ([35], Special Case 1)**.** *Consider the system* (2.1)*. If there exists* $\underline{J}_x \in \overline{\mathbb{R}}^{n\times n}_{\leq 0}$, $\overline{J}_x \in \overline{\mathbb{R}}^{n\times n}_{\geq 0}$, $\underline{J}_w \in \overline{\mathbb{R}}^{n\times m}_{\leq 0}$*, and* $\overline{J}_w \in \overline{\mathbb{R}}^{n\times m}_{\geq 0}$ *so that*

- *for all* $x \in \mathcal{X}$ *and all* $w \in \mathcal{W}$*, both* $\frac{\partial F}{\partial x}(x, w) \in [\underline{J}_x, \overline{J}_x]$ *and* $\frac{\partial F}{\partial w}(x, w) \in [\underline{J}_w, \overline{J}_w]$ *hold,*

- *for all $i \neq j$, either $(\underline{J}_x)_{i,j} > -\infty$ or $(\overline{J}_x)_{i,j} < \infty$ holds, and*

- *for all i, k, either $(\underline{J}_w)_{i,k} > -\infty$ or $(\overline{J}_w)_{i,k} < \infty$ holds,*

then (2.1) *is mixed monotone and a decomposition function is constructed in the following way:*

1. *For all $i, j \in \{1, \cdots, n\}$ with $i \neq j$ and all $k \in \{1, \cdots, m\}$, choose $\delta_{i,j},\ \epsilon_{i,k} \in \{0, 1\}$ so that*

$$\begin{aligned} \delta_{i,j} = 0 \Rightarrow (\underline{J}_x)_{i,j} \neq -\infty, \quad & \delta_{i,j} = 1 \Rightarrow (\overline{J}_x)_{i,j} \neq \infty, \\ \epsilon_{i,k} = 0 \Rightarrow (\underline{J}_w)_{i,k} \neq -\infty, \quad & \epsilon_{i,k} = 1 \Rightarrow (\overline{J}_w)_{i,k} \neq \infty. \end{aligned} \tag{3.5}$$

   Note that such a choice exists by hypothesis.

2. *For all $i \in \{1, \cdots, n\}$, define $\xi^i, \alpha^i \in \mathbb{R}^n$ and $\pi^i, \beta^i \in \mathbb{R}^m$ element-wise according to*

$$(\xi^i_j, \alpha^i_j) = \begin{cases} (x_i, 0) & \text{if } i = j, \\ (x_j, -(\underline{J}_x)_{i,j}) & \text{if } i \neq j \text{ and } \delta_{i,j} = 0, \\ (\widehat{x}_j, (\overline{J}_x)_{i,j}) & \text{if } i \neq j \text{ and } \delta_{i,j} = 1, \end{cases} \qquad (\pi^i_k, \beta^i_k) = \begin{cases} (w_k, -(\underline{J}_w)_{i,k}) & \text{if } \epsilon_{i,k} = 0, \\ (\widehat{w}_k, (\overline{J}_w)_{i,k}) & \text{if } \epsilon_{i,k} = 1. \end{cases} \tag{3.6}$$

3. *Lastly, define the i^{th} element of the decomposition function d according to*

$$d_i(x, w, \widehat{x}, \widehat{w}) = F_i(\xi^i, \pi^i) + (\alpha^i)^\mathsf{T}(x - \widehat{x}) + (\beta^i)^\mathsf{T}(w - \widehat{w}), \tag{3.7}$$

   which is always well-defined on $\mathcal{X} \times \mathcal{W} \times \mathcal{X} \times \mathcal{W}$ since $\mathcal{X}$ and $\mathcal{W}$ are assumed to be hyperrectangles. ■

The connection between the decomposition function (3.7) and the functions f and g from (3.4) is made more explicit later in Example 7.

Remark 5. All *monotone* dynamical systems satisfy the hypothesis of Proposition 3, and thus mixed monotonicity generalizes the classical notion of monotonicity. In particular, if (2.1) is monotone, *i.e.*, $\frac{\partial F}{\partial x}(x, w)$ is a Metzler matrix and $\frac{\partial F}{\partial w}(x, w)$ is a positive matrix, then (2.1) is mixed monotone with decomposition function $d(x, w, \widehat{x}, \widehat{w}) = F(x, w)$. One can also show that, when considering linear time-invariant systems as discussed previously in Example 3, it is possible to apply the approach from Proposition 3 in order to arrive at the decomposition function constructed in (2.24). ■

A restrictive version of Proposition 3 requiring sign-stability of the Jacobian matrices is first introduced in [53], and the essential observation that this extends to the case when the entries of the Jacobian are bounded is made in [31] and is also in [33, 34]. However, [31, 33] require the diagonal entries of $\frac{\partial F}{\partial x}(x, w)$ to be also bounded, and [33, 34] do not allow the other entries to be unbounded in one direction. In our characterization, we observe that is possible to take the corresponding δ or ϵ variable as 0 or 1 when an entry of the Jacobian is both upper and lower bounded. An implication of this generalization is that Proposition 3 can be used to generate multiple different decomposition functions from the same vector field F, in the specific instance where either $\frac{\partial F}{\partial x}(x, w)$ or $\frac{\partial F}{\partial w}(x, w)$ is uniformly bounded from above and from below in some entries. To demonstrate this observation, we show in Example 7 how two different decomposition functions for the simplified unicycle model (3.3) can be attained by applying Proposition 3 with two choices of ϵ.

Example 7. Consider the dynamical system

$$\dot{x} = F^{\cos}(w) = \cos(w) \tag{3.8}$$

as previously introduced in (3.3), where $x \in \mathbb{R}$ is the state and $w \in \mathbb{R}$ is a disturbance input. Observe that the system is mixed monotone with respect to the decomposition function

$$d^1(w, \widehat{w}) = \cos(w) + w - \widehat{w} \tag{3.9}$$

since it is true that

- $d^1(w, w) = F^{\cos}(w)$ for all $w \in \mathbb{R}$,
- $\frac{\partial d^1}{\partial w}(w, \widehat{w}) \geq 0$ for all $w, \widehat{w} \in \mathbb{R}$ since $f(w) = \cos(w) + w$ is monotonically non-decreasing

in w, and

- $\frac{\partial d^1}{\partial \widehat{w}}(w, \widehat{w}) \geq 0$ for all $w, \widehat{w} \in \mathbb{R}$ since $g(\widehat{w}) = -\widehat{w}$ is monotonically non-increasing in $\widehat{w}$.

A rudimentary explanation of the theory behind this construction is that the decomposition function (3.9) is computed from a lower-bound on the Jacobian of the vector field; that is, since

$$\frac{\partial F^{\cos}}{\partial w}(w) = -\sin(w) \geq \underline{J} = -1 \tag{3.10}$$

holds for all $w \in \mathbb{R}$,

$$d^1(w, \widehat{w}) = F^{\cos}(w) - \underline{J}(w - \widehat{w}) \tag{3.11}$$

satisfies the conditions of Definition 6 and is a decomposition function for $\dot{x} = F^{\cos}(w)$. Using this same approach, it can also be shown that (3.8) is mixed monotone with respect to

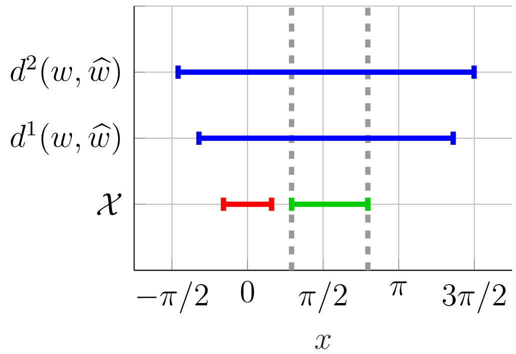
$$d^2(w, \widehat{w}) = \cos(\widehat{w}) - \widehat{w} + w \tag{3.12}$$

where we employ a slight modification of the construction (3.11) that exploits the fact that the Jacobian $\frac{\partial F^{\cos}}{\partial w}(w) \leq \overline{J} = 1$ is similarly bounded from above:

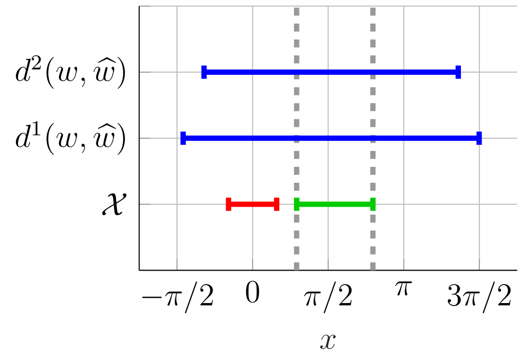
$$d^2(w, \widehat{w}) = F^{\cos}(\widehat{w}) + \overline{J}(w - \widehat{w}). \tag{3.13}$$

Moreover, observe that the decomposition function (3.9) is constructed by applying Proposition 3 to (3.8) with $\epsilon_{1,1} = 0$, whereas (3.12) is constructed by applying the same result with $\epsilon_{1,1} = 1$, and both decomposition functions are possible since $\frac{\partial F^{\cos}}{\partial w}(w) = -\sin(w) \in [-1, 1]$ is both bounded from above and below.

We demonstrate in Figure 3.1 how d^1 and d^2 are used to compute interval over-approximations of reachable sets for (3.8). While these decomposition functions were attained using similar procedures, we observe that they provide different reachable set approximations when used with Proposition 2, and these reachable set approximations can vary in conservatism depending on the choice



(a)



(b)

Figure 3.1: Example 7: Computing reachable sets for (3.8) using d^1 from (3.9) and d^2 from (3.12). In both subfigures, the inital set $A = [-\frac{1}{2}, \frac{1}{2}]$ is shown as a red interval and the time-1 reachable set $R(1; A)$ is shown as a green interval. The interval-approximations of $R(1; A)$ attained from using Proposition 2 with d^1 and d^2 are both shown in blue. In (a) the disturbance space is $\mathcal{W} = [-\frac{\pi}{8}, \frac{\pi}{4}]$ and d^1 provides a less conservative approximation of $R(1; A)$ than d^2. In (b) the disturbance space is $\mathcal{W} = [-\frac{\pi}{4}, \frac{\pi}{8}]$ and d^2 provides a less conservative approximation of $R(1; A)$ than d^1.

$\mathcal{W} = [\underline{w}, \overline{w}]$. Indeed, the decomposition functions d^1 and d^2 exhibit fundamentally different properties in the context of mixed monotonicity, since it is true that

- $d^1(w, \widehat{w})$ from (3.9) is a nonlinear function of w and a linear function of $\widehat{w}$, whereas
- $d^2(w, \widehat{w})$ from (3.12) is a linear function of w and a nonlinear function of $\widehat{w}$. ■

The hypothesis of Proposition 3 is known to apply quite generally [31], and is even taken to be the definition of mixed monotonicity in [33, 34]. Thus, given the generality of this approach, two natural questions arise: First, are there systems that do not satisfy the hypothesis of Proposition 3 but are nonetheless mixed monotone with respect to some decomposition function other than (3.7)? Second, for systems that do satisfy the hypothesis of Proposition 3, do there exist other, perhaps more useful, decomposition functions than (3.7)? In the following example, we answer both questions affirmatively, where we reconsider the 2-dimensional polynomial system (2.46) as previously studied in Example 5.

Example 8. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x) = \begin{bmatrix} x_2^2 + 2 \\ x_1 \end{bmatrix} \tag{3.14}$$

with $\mathcal{X} = \mathbb{R}^2$, as previously studied in Example 5. Note that $\frac{\partial F_1}{\partial x_2}(x) = 2x_2$ is neither lower or upper bounded on $\mathcal{X}$ and thus the system does not satisfy the hypothesis of Proposition 3. Nonetheless, (3.14) is mixed monotone on $\mathcal{X}$ with decomposition function

$$\begin{aligned} d_1(x, \widehat{x}) &= \begin{cases} x_2^2 + 2 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2, \\ \widehat{x}_2^2 + 2 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 < -\widehat{x}_2, \\ x_2\widehat{x}_2 + 2 & \text{if } x_2 < 0 \text{ and } \widehat{x}_2 > 0, \end{cases} \\ d_2(x, \widehat{x}) &= x_1, \end{aligned} \tag{3.15}$$

as introduced previously in (2.46).

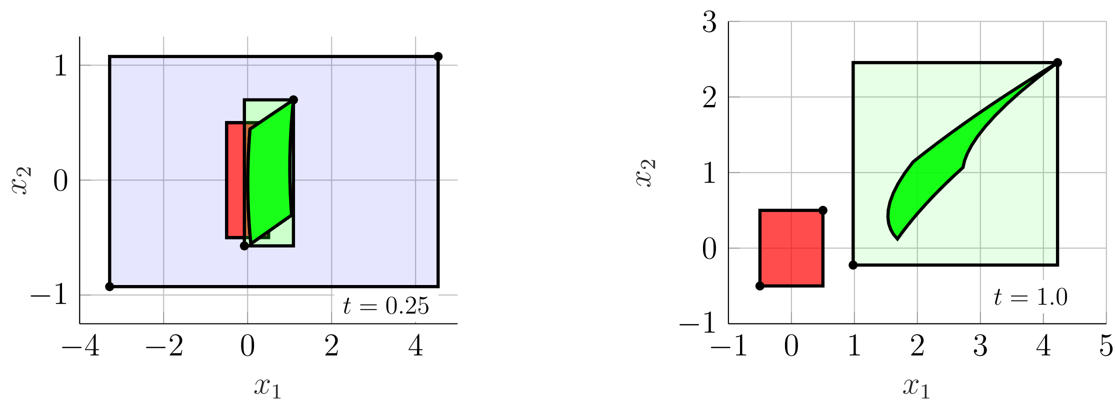
Even though $\frac{\partial F}{\partial x}(x)$ is not uniformly bounded on $\mathcal{X} = \mathbb{R}^2$, we can restrict our analysis to a compact subset $\mathcal{X}' \subset \mathcal{X}$ so that the decomposition function construction defined in Proposition 3 is applicable. For instance, on the subset $\mathcal{X}' = [-5, 5]^2$ we have $\frac{\partial F}{\partial x}(x) \in [\underline{J}_x, \overline{J}_x]$ for

$$\frac{\partial F}{\partial x}(x) = \begin{bmatrix} 0 & 2x_2 \\ 1 & 0 \end{bmatrix} \quad \text{and } \underline{J}_x = \begin{bmatrix} 0 & -10 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \overline{J}_x = \begin{bmatrix} 0 & 10 \\ 1 & 0 \end{bmatrix}. \tag{3.16}$$

Now, applying Proposition 3, with $\delta_{1,2} = \delta_{2,1} = 1$, we have that

$$d'(x, \widehat{x}) = \begin{bmatrix} \widehat{x}_2^2 + 2 + 10(x_2 - \widehat{x}_2) \\ x_1 \end{bmatrix} \tag{3.17}$$

is a decomposition function for (3.14) on $\mathcal{X}'$, and Proposition 2 then allows for computing reach-



(a)

(b)

Figure 3.2: Example 8: Comparing the decomposition functions d from (3.15) and d' from the Jacobian-bound construction in (3.17). Subfigures: (a) The initial set is $[\![a]\!] = [-\frac{1}{2}, \frac{1}{2}]^2$ is shown in red and the time-$\frac{1}{4}$ reachable set $R(\frac{1}{4}; [\![a]\!])$ is shown in dark green. The rectangular reachable-set over-approximations derived from d and d' shown in green and blue, respectively. Observe that $\Phi^{E'}(t; a)$ leaves $\mathcal{X}' \times \mathcal{X}' = [-5, 5]^4$ at time $t = 0.27$ and therefore cannot be used to approximate reachable sets on longer time horizons. Moreover, the decomposition function d leads to significantly tighter reachable set approximations when used with Proposition 2, and can be used to compute reachable sets on longer time-horizons. An example is shown in (b), previously Figure 2.9(b), where we compute a rectangular over-approximation of $R(1; [\![a]\!])$ using d.

able sets for (3.14) using d' so long as the trajectories of the resulting embedding system remain within $\mathcal{X}' \times \mathcal{X}'$. An example is shown in Figure 3.2 where we compare two reachable set over-approximations derived from the decomposition functions d' and d, respectively. Note that, even though Proposition 3 is made applicable by restricting the domain, the decomposition function given by (3.15) allows for a significantly tighter approximation of $R(t; A)$ and is applicable on arbitrarily long time-horizons. ∎

The above examples and discussion motivate the need for new techniques of obtaining and reasoning about decomposition functions. While we have shown that, *e.g.*, an arbitrary system as in (2.1) will generally be mixed monotone with respect to many decomposition that vary in conservatism, we have not yet provided a formal theory as to *when* an arbitrary system (2.1) is mixed monotone, nor have we outlined a theory of *how* conservatism enters the reachability procedure, Proposition 2. The remainder of this chapter deals with answering these fundamental questions.

3.3 Technical Lemmas and Discussion

We have shown already how a mixed monotone system will generally be mixed monotone with respect to many decomposition functions and how certain decomposition functions may provide more or less conservative reachable set approximations than others when used with Proposition 2.

In order to move further in the understanding of how decomposition functions are formed, it is beneficial to internalize certain technical lemmas relating to how one or more *known* decomposition functions for (2.1) can be modified or combined to form a *new* decomposition function for (2.1) that provides a tighter approximation of reachable sets than any of the decomposition functions from which it is constructed. As such, the purpose of this section is to highlight certain relevant results in this area and, in doing so, we lay a preliminary theory of how conservatism enters the reachability procedure, Proposition 2. Conservatism in the approximation of reachable sets is also a main focus of Section 3.4 and Chapter 5 in this work.

We begin with a discussion on how decomposition functions are created in the more general setting, where, *e.g.*, the hypothesis of Proposition 3 may not apply. We observe, in particular, that the conditions on a decomposition function in Definition 6 apply element-wise in the sense that the conditions on the i^{th} element of the decomposition function are dependant only on the i^{th} entry of the vector field F from (2.1). In this way, constructing a decomposition function for an n-dimensional system generally involves constructing individual decomposition functions for n separate 1-dimensional systems; see, *e.g.*, Example 5 where d_1 and d_2 are computed and reasoned about separately. See also Lemma 3, which is generalized and proved later in Section 3.5.

Lemma 3. Consider a dynamical system

$$\dot{x} = F(x, w) \tag{3.18}$$

with state $x \in \mathcal{X} := \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \subseteq \mathbb{R}^n$ and disturbance $w \in \mathcal{W} \subseteq \mathbb{R}^m$. For all $i \in \{1, \cdots, n\}$, consider also a 1-dimensional system

$$\dot{x}_i = f^i(x_i, v) := F_i(x, w) \tag{3.19}$$

where now $x_i \in \mathcal{X}_i \subseteq \mathbb{R}$ is the state, and $v := (x_{-i}, w) \in \mathcal{X}_{-i} \times \mathcal{W} \subset \mathbb{R}^{n-1} \times \mathbb{R}^m$ is viewed as a disturbance. In the instance where (3.19) is mixed monotone with respect to $d^i(x_i, v, \widehat{x}_i, \widehat{v})$ for all i, we have also that (3.18) is mixed monotone with respect to

$$d(x, w, \widehat{x}, \widehat{w}) := \begin{bmatrix} d^1(x_1, (x_{-1}, w), \widehat{x}_i, (\widehat{x}_{-1}, \widehat{w})) \\ \vdots \\ d^n(x_n, (x_{-n}, w), \widehat{x}_i, (\widehat{x}_{-n}, \widehat{w})) \end{bmatrix}. \tag{3.20}$$

■

In the context of this chapter, and its examples, the results of Lemma 3 provide some justification for studying the simplified unicycle model (3.3) rather than the full system (3.2). Observe that the simplified system (3.3) comes from studying (3.19) with $f^1(v) = F_1^{\text{uni}}(x, w)$ and where we fix $w_1 = 1$ for ease of exposition. Moreover, we show in the following example how a decomposition function for the 3-dimensional unicycle system (3.2) is formed using Lemma 3 with decomposition functions for the individual entries of the vector field of (3.2).

Example 9. Consider the kinematic unicycle model

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} \cos(x_3) \\ \sin(x_3) \\ w_2 \end{bmatrix} \tag{3.21}$$

as previously introduced in (3.2), but where we fix $w_1 = 1$ and $w_2 \in \mathcal{W}_2 = [-0.1, 0.1]$. Also consider the following three 1-dimensional systems

$$\text{(i)}\ \dot{x}_1 = \cos(v), \qquad \text{(ii)}\ \dot{x}_2 = \sin(v), \qquad \text{and} \qquad \text{(iii)}\ \dot{x}_3 = v, \tag{3.22}$$

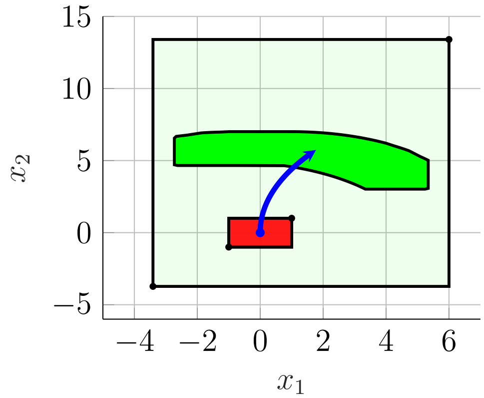


Figure 3.3: Example 9: Approximating reachable sets for the kinematic unicycle model (3.21) using d from (3.24). The initial set $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$ is shown in red, the time-6 reachable set $R(6; A)$ is shown in dark green, and the rectangular over-approximation of $R(6; A)$ attained by applying Proposition 2 with d from (3.24) is shown in light green; all projected onto the position-space, *i.e.*, the x_1–x_2 plane. A sample system trajectory $\phi(1; (0, 0, \frac{\pi}{2}), -0.1)$ beginning from A is also shown in blue.

all with state space $\mathbb{R}$ and disturbance space $\mathbb{R}$. Decomposition functions for each of the three 1-dimensional systems are computed using Proposition 3 and are given by

$$\text{(i) } d^1(v, \widehat{v}) = \cos(v) + v - \widehat{v}, \quad \text{(ii) } d^2(v, \widehat{v}) = \sin(v) + v - \widehat{v}, \quad \text{and} \quad \text{(iii) } d^3(v, \widehat{v}) = v, \tag{3.23}$$

respectively. Now applying Lemma 3, we have that the 3-dimensional unicycle model (3.21) is mixed monotone with respect to

$$d(x, w, \widehat{x}, \widehat{w}) = \begin{bmatrix} d^1(x_3, \widehat{x}_3) \\ d^2(x_3, \widehat{x}_3) \\ d^3(w_2, \widehat{w}_2) \end{bmatrix} = \begin{bmatrix} \cos(x_3) + x_3 - \widehat{x}_3 \\ \sin(x_3) + x_3 - \widehat{x}_3 \\ w_2 \end{bmatrix}. \tag{3.24}$$

An example is provided in Figure 3.3 where we over-approximate $R(6; A)$ for (3.21) using Proposition 2 with d from (3.24), and where the initial set is taken to be $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$. ■

We next move to study conservatism in the reachable set approximations derived from the application Proposition 2. Our first result is to show how knowledge of two decomposition functions for a system allows for constructing a new *composite* decomposition function for the same system that provides a tighter approximation of reachable sets when used with Proposition 2 than is attainable by, *e.g.*, applying Proposition 2 with each of the initial decomposition functions individually and then taking the intersection of their respective reachable set over-approximations.

Lemma 4. Let (2.1) be mixed monotone with respect to both d^1 and d^2. Then (2.1) is mixed monotone with respect to d defined element-wise by

$$d_i(x, w, \widehat{x}, \widehat{w}) = \begin{cases} \max\{d_i^1(x, w, \widehat{x}, \widehat{w}), d_i^2(x, w, \widehat{x}, \widehat{w})\} & \text{if } x \preceq \widehat{x} \text{ and } w \preceq \widehat{w}, \\ \min\{d_i^1(x, w, \widehat{x}, \widehat{w}), d_i^2(x, w, \widehat{x}, \widehat{w})\} & \text{if } \widehat{x} \preceq x \text{ and } \widehat{w} \preceq w. \end{cases} \tag{3.25}$$

Moreover, the decomposition function d will provide a tighter approximations of reachable sets when used with Proposition 2, than is attainable from either d^1, d^2: denoting by E, E^1, E^2 the embedding functions relative to d, d^1, d^2, respectively, we have that

$$[\![\Phi^E(t; a)]\!] \subseteq [\![\Phi^{E^1}(t; a)]\!] \cap [\![\Phi^{E^2}(t; a)]\!] \tag{3.26}$$

for all $t \geq 0$ and all $a \in \mathcal{T}$. ■

Remark 6. Observe the following: Proposition 2 over-approximates $R(t; [\![a]\!])$ using a t-time-unit simulation of the embedding system $\Phi^E(t; a)$. Since $\mathcal{T}$ is forward invariant for (2.34)—See Lemma 1—and since $a \in \mathcal{T}$ when $[\![a]\!]$ is a hyperrectangle, we also have $\Phi^E(t; a) \in \mathcal{T}$ for $t \geq 0$. Therefore, in the application of Proposition 2, the embedding function $E(x, \widehat{x})$ will only ever be evaluated when $x \preceq \widehat{x}$, and the decomposition function $d(x, w, \widehat{x}, \widehat{w})$ will only ever be evaluated when either $(x, w) \preceq (\widehat{x}, \widehat{w})$ or $(\widehat{x}, \widehat{w}) \preceq (x, w)$. For this reason, it is generally possible to relax the conditions of Definition 6 so that D1–D4 apply only when $(x, w) \preceq (\widehat{x}, \widehat{w})$ or $(\widehat{x}, \widehat{w}) \preceq (x, w)$ and we observe, in particular, that the composite decomposition function (3.25) is evaluable only on this domain. See also Remark 4. ■

The composite decomposition function d from (3.25) is guaranteed to provide a tighter approximation of reachable sets than either of its two subcomponents d^1 and d^2. However, this reduction in conservatism brings with it added computational complexity. Indeed, evaluating $d(x, w, \widehat{x}, \widehat{w})$ from (3.25) at some point in the embedding space will be at least as computationally complex as evaluating both $d^1(x, w, \widehat{x}, \widehat{w})$ and $d^2(x, w, \widehat{x}, \widehat{w})$ individually. This result is representative of a larger trade-off in mixed monotonicity and the application of decomposition functions: generally decomposition functions that provide *tighter* approximations of reachable sets are also more difficult to evaluate algorithmically. Nonetheless, composite decomposition functions are almost always preferable in application when one's computational resources allow for their use, and we observe, in particular, that Lemma 4 is well suited for use with Proposition 3 since, generally speaking, many different more-conservative decomposition functions can be constructed via Jacobian-bounds.

Before demonstrating Lemma 4 through example, we first present a related result showing how uniform bounds on the system's vector field can be incorporated in the procedure to attain less-conservative decomposition functions in a similar way.

Lemma 5. Let (2.1) be mixed monotone with respect to d'. If for some i and some $\underline{F} \in \mathbb{R}$

$$F_i(x, w) \geq \underline{F} \tag{3.27}$$

holds for all $x \in \mathcal{X}$ and all $w \in \mathcal{W}$, then (2.1) is mixed monotone with respect to d defined element-wise by

$$d_j(x, w, \widehat{x}, \widehat{w}) = \begin{cases} d'_j(x, w, \widehat{x}, \widehat{w}) & \text{if } j \neq i, \\ \max\{d'_j(x, w, \widehat{x}, \widehat{w}), \underline{F}\} & \text{if } i = j. \end{cases} \tag{3.28}$$

Similarly, if for some i and some $\overline{F} \in \mathbb{R}$

$$F_i(x, w) \leq \overline{F} \tag{3.29}$$

holds for all $x \in \mathcal{X}$ and all $w \in \mathcal{W}$, then (2.1) is mixed monotone with respect to d defined element-wise by

$$d_j(x, w, \widehat{x}, \widehat{w}) = \begin{cases} d'_j(x, w, \widehat{x}, \widehat{w}) & \text{if } j \neq i, \\ \min\{d'_j(x, w, \widehat{x}, \widehat{w}), \overline{F}\} & \text{if } i = j. \end{cases} \tag{3.30}$$

In both cases, d is will provide a tighter approximation of reachable sets than d', when used with Proposition 2, in the sense that

$$[\![\Phi^E(t; a)]\!] \subseteq [\![\Phi^{E'}(t; a)]\!] \tag{3.31}$$

holds for all $t \geq 0$ and all $a \in \mathcal{T}$, where E and E' are the embedding functions relative to d and d', respectively. ■

We demonstrate the application of Lemmas 4 and 5 in the following example where we reconsider the 3-dimensional unicycle model (3.2).

Example 10. Consider first the simplified unicycle model,

$$\dot{x} = F^{\cos}(w) = \cos(w) \tag{3.32}$$

as studied previously in Example 7 and recall that (3.32) is mixed monotone with respect to both d^1 from (3.9) and d^2 from (3.12). Now applying Lemma 4 with d^1 and d^2 we have also that (3.32) is mixed monotone with respect to d^3 given by

$$d^3(w, \widehat{w}) = \begin{cases} \max\{\cos(w) + w - \widehat{w},\, \cos(\widehat{w}) + w - \widehat{w}\} & \text{if } w \leq \widehat{w}, \\ \min\{\cos(w) + w - \widehat{w},\, \cos(\widehat{w}) + w - \widehat{w}\} & \text{if } \widehat{w} \leq w. \end{cases} \tag{3.33}$$

Furthermore, the vector field $F^{\cos}(w) \in [-1, 1]$ is uniformly bounded both from above and below and, applying Lemma 5, we find that (3.32) is also mixed monotone with respect to d^4 given by

$$d^4(w, \widehat{w}) = \begin{cases} -1 & \text{if } d^3(w, \widehat{w}) \leq -1, \\ d^3(w, \widehat{w}) & \text{if } -1 \leq d^3(w, \widehat{w}) \leq 1, \\ 1 & \text{if } d^3(w, \widehat{w}) \geq 1. \end{cases} \tag{3.34}$$

Lemmas 4 and 5 now imply that the decomposition functions d^3 and d^4 will provide tighter approximations of reachable sets for (3.32) than either d^1 or d^2 when used with Proposition 2. An example is shown in Figure 3.4(a) where we over-approximate $R(1; [-\frac{1}{2}, \frac{1}{2}])$ using d^3 and d^4, and where the disturbance space is taken to be $\mathcal{W} = [-\frac{\pi}{8}, \frac{\pi}{4}]$.

Building off this approach, we next apply Lemmas 4 and 5 to compute a composite decomposition functions for the 3-dimensional unicycle model (3.2). We show in Figure 3.4(b) how this composite decomposition functions allows for tighter reachable set approximations than are attainable from, *e.g.*, the decomposition function (3.24) from Example 9. ■

Hereafter in this section, we say that a decomposition function d is *tighter* than a decomposition function d' when

(i) $d'(x, w, \widehat{x}, \widehat{w}) \preceq d(x, w, \widehat{x}, \widehat{w})$ holds when $x \preceq \widehat{x}$ and $w \preceq \widehat{w}$, and

(ii) $d(x, w, \widehat{x}, \widehat{w})) \preceq d'(x, w, \widehat{x}, \widehat{w})$ holds when $\widehat{x} \preceq x$ and $\widehat{w} \preceq w$,

since in this case d will always produce tighter approximations of reachable sets than d' when used with Proposition 2; see Lemma 4. To visualise the conditions (i) and (ii) above, it is beneficial to reconsider the deterministic embedding system (2.34) and it's role in reachable set over-approximations, as discussed previously in Remark 6. Recall that the deterministic embedding system, taken with respect to a decomposition function d, is given by

$$\begin{bmatrix} \dot{\underline{x}} \\ \dot{\overline{x}} \end{bmatrix} = E(\underline{x}, \overline{x}) = \begin{bmatrix} d(\underline{x}, \underline{w}, \overline{x}, \overline{w}) \\ d(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \end{bmatrix} \tag{3.35}$$

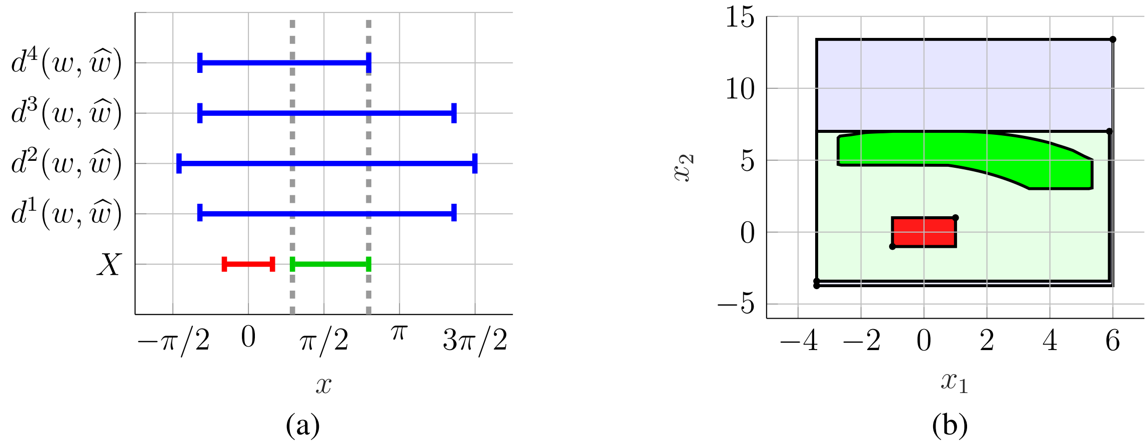


Figure 3.4: Example 10: Applying Lemmas 4 and 5 to achieve tighter approximations of reachable sets for the kinematic unicycle model. Figure 3.4(a) compares the reachable sets attained from applying Proposition 2 with the decomposition functions d^1, d^2, d^3 and d^4. The initial set $A = [-\frac{1}{2}, \frac{1}{2}]$ is shown in red and $R(1; A)$ is shown in green, where $\mathcal{W} = [-\frac{\pi}{8}, \frac{\pi}{4}]$. The interval-approximations of $R(1; A)$ attained from using Proposition 2 with d^1, d^2, d^3 and d^4 are all shown in blue. Figure 3.4(b) compares the decomposition function d from (3.24) with a another decomposition function for the 3-dimensional unicycle model (3.32) that was derived by applying Lemmas 4 and 5 and with d and a second decomposition function computed from Proposition 3. The reachable set over-approximations derived from these decomposition functions are shown in blue and light green, respectively. In both figures, observe that the decomposition functions attained from the application of Lemmas 4 and 5 provide tighter approximations of reachable sets than the decomposition functions from which they are formed.

where we replace the state variables $x(t)$ and $\widehat{x}(t)$ in (2.34) with the variables $\underline{x}(t)$ and $\overline{x}(t)$ for ease of exposition. Given a hyperrectangular set of initial conditions $[\underline{x}_0, \overline{x}_0]$, Proposition 2 then allows for over-approximating the time-t reachable set $R(t; [\underline{x}_0, \overline{x}_0])$ via a simulation of the embedding system, where initial condition of the simulation is $(\underline{x}(0), \overline{x}(0)) = (\underline{x}_0, \overline{x}_0)$ and the over-approximation of $R(t; [\underline{x}_0, \overline{x}_0])$ is given by $[\underline{x}(t), \overline{x}(t)] = [\![\Phi^E(t; (\underline{x}_0, \overline{x}_0))]\!]$. In this way, the role of the decomposition function changes when considering the first n and last n coordinates of the embedding system (3.35):

- the first n coordinates of (3.35) describe the dynamics of the lower-bound $\underline{x}(t)$ and, in these coordinates, $d(x, w, \widehat{x}, \widehat{w})$ is evaluated only when $(x, w) \preceq (\widehat{x}, \widehat{w})$, whereas
- the last n coordinates of (3.35) describe the dynamics of the upper-bound $\overline{x}(t)$ and, in these coordinates, $d(x, w, \widehat{x}, \widehat{w})$ is evaluated only when $(\widehat{x}, \widehat{w}) \preceq (x, w)$.

For this reason, when attempting to construct *less-conservative* decomposition functions for a system, it is generally preferable to ensure that the evaluation of $d(x, w, \widehat{x}, \widehat{w})$ is *as large as possible* when $(x, w) \preceq (\widehat{x}, \widehat{w})$ and *as small as possible* when $(\widehat{x}, \widehat{w}) \preceq (x, w)$, as to achieve tight lower and upper bounds on the system's reachable set. Note that the techniques posited in Lemmas 4 and 5 implicitly attempt to maximize or minimize the valuation of a decomposition function in this way, in order to achieve less-conservative decomposition functions. See also, *e.g.*, [54] which studies mixed monotone systems through separate *upper* and *lower-decomposition functions*, defined on these two domains.

To add further clarity, we next present a second example where we reconsider the 2-dimensional polynomial system (2.46).

Example 11. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x) = \begin{bmatrix} x_2^2 + 2 \\ x_1 \end{bmatrix}, \tag{3.36}$$

as previously studied in Examples 5 and 8. Recall that the system (3.36) is mixed monotone on $\mathcal{X} = \mathbb{R}^2$ with decomposition function

$$\begin{aligned} d_1^1(x, \widehat{x}) &= \begin{cases} x_2^2 + 2 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2, \\ \widehat{x}_2^2 + 2 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 < -\widehat{x}_2, \\ x_2 \widehat{x}_2 + 2 & \text{if } x_2 < 0 \text{ and } \widehat{x}_2 > 0, \end{cases} \\ d_2^2(x, \widehat{x}) &= x_1, \end{aligned} \tag{3.37}$$

and mixed monotone on $\mathcal{X}' = [-5, 5]$ with decomposition function

$$d^2(x, \widehat{x}) = \begin{bmatrix} \widehat{x}_2^2 + 2 + 10(x_2 - \widehat{x}_2) \\ x_1 \end{bmatrix}. \tag{3.38}$$

We observe that $d^1(x, \widehat{x})$ always provides tighter reachable set approximations than $d^2(x, \widehat{x})$ when used with Proposition 2 since it is true that $d^2(x, \widehat{x}) \preceq d^1(x, \widehat{x})$ holds for all $x, \widehat{x} \in \mathcal{X}'$ with $x \preceq \widehat{x}$, and $d^1(x, \widehat{x}) \preceq d^2(x, \widehat{x})$ holds when $\widehat{x} \preceq x$. Nonetheless, the entries of vector field $F(x)$ are bounded on $\mathcal{X}$ and Lemma 5 can be employed with d^1 to compute an even tighter decomposition function for the same system. We observe in particular that the first entry of the vector field $F_1(x)$ is uniformly bounded from below on $\mathcal{X} = \mathbb{R}^2$

$$F_1(x) = x_2^2 + 2 \geq 2 \tag{3.39}$$

and Lemma 5 now implies that

$$\begin{aligned} d_1^3(x, \widehat{x}) &= \max\{2, d_1^1(x, \widehat{w})\} \\ &= \begin{cases} x_2^2 + 2 & \text{if } x_2 \geq 0 \text{ and } x_2 \geq -\widehat{x}_2, \\ \\ \widehat{x}_2^2 + 2 & \text{if } \widehat{x}_2 \leq 0 \text{ and } x_2 < -\widehat{x}_2, \\ \\ 2 & \text{if } x_2 < 0 \text{ and } \widehat{x}_2 > 0, \end{cases} \\ d_2^3(x, \widehat{x}) &= x_1, \end{aligned} \tag{3.40}$$

is a decomposition function for (3.36). We show in Figure 3.5 how the decomposition function (3.40) can be employed to reduce conservatism in the approximation of reachable sets for (3.36), where we recompute $R(1; A)$ for $A = [-\frac{1}{2}, \frac{1}{2}]^2$. ■

Remark 7. Example 11 demonstrates a second important reason for beginning one's study of

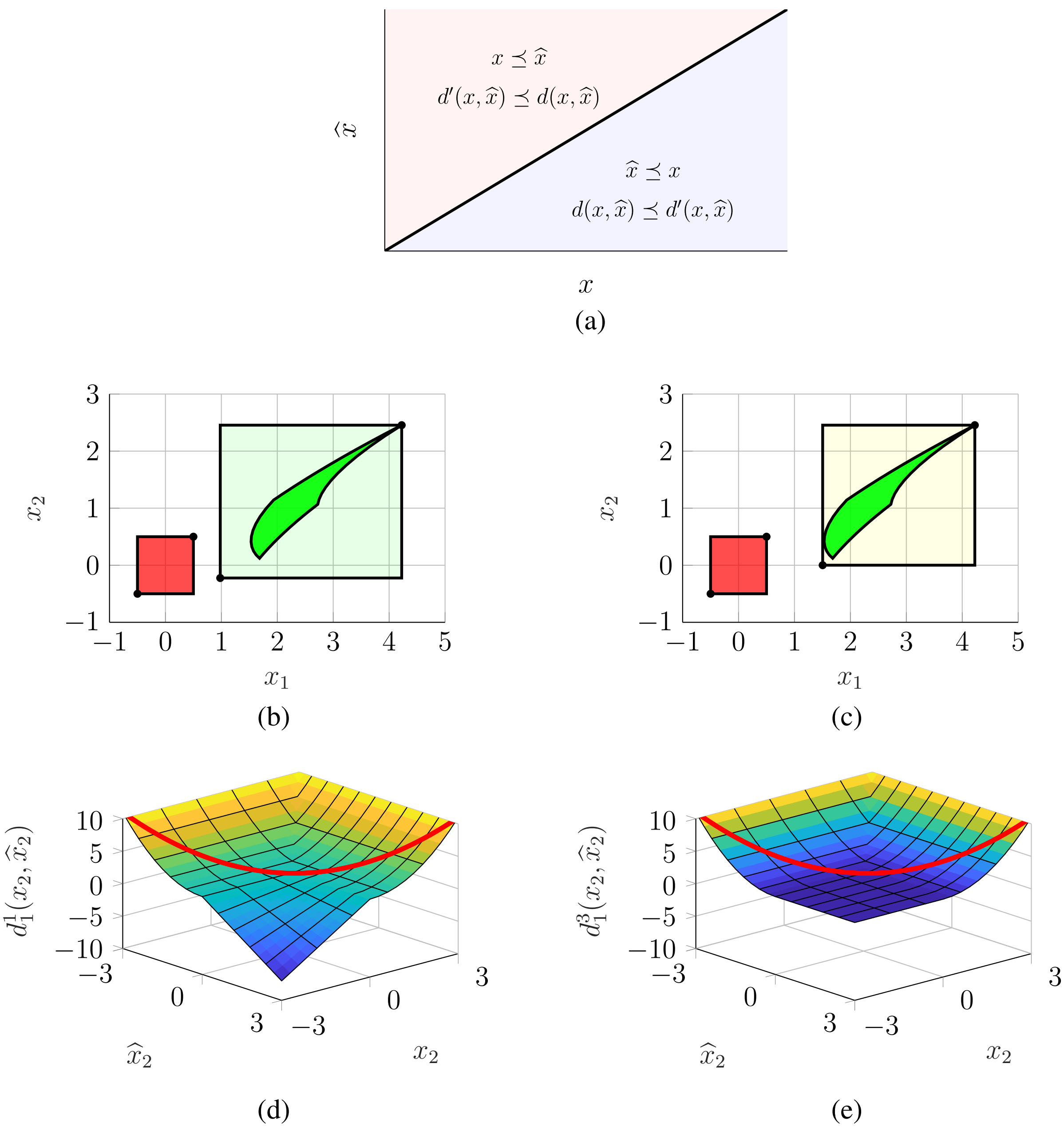


Figure 3.5: Example 11: Applying Lemma 5 to achieve tighter decomposition functions for (3.36). Subfigures: (a) Given two decomposition functions, d and d' for the same system, Proposition 2 will provide a tighter approximation of reachable sets when used with d, rather than d', in the instance where $d'(x,\widehat{x}) \preceq d(x,\widehat{x})$ holds when $x \preceq \widehat{x}$ and $d(x,\widehat{x}) \preceq d'(x,\widehat{x})$ holds when $\widehat{x} \preceq x$. (b) and (c) show approximations of $R(1;A)$ attained by applying d^1 from (3.37) and d^3 from (3.40), respectively. Observe that d^3 is a tighter decomposition function than d^1, and computes reachable sets with less conservatism. (d) and (e) plot the decomposition functions d^1 and d^3 above the x_2–$\widehat{x}_2$ plane, respectively. Observe that $d^1(x,\widehat{x}) \preceq d^3(x,\widehat{x})$ holds when $x \preceq \widehat{x}$ and $d^3(x,\widehat{x}) \preceq d^1(x,\widehat{x})$ holds when $\widehat{x} \preceq x$. Therefore d^3 is a tighter decomposition function for (3.36) than d^1. In both subfigures, $F_1(x) = d_1(x,x) = x_2^2 + 2$ is plotted above the diagonal Δ in red.

decomposition functions with 1-dimensional systems. In particular, the ability to visualize one's decomposition function through a plot allows for ease in (i) ensuring the validity of a decomposition function by checking that the conditions in Definition 6 hold, see Figure 2.9(a), and (ii) reasoning about the tightness of decomposition functions, see Figures 3.5(d)–(e). Such visualizations can generally only be created in cases where some entry of the vector field F_i is dependant on only one state or input variable, excluding x_i. ■

In summary, the main observations of this section are as follows:

1. Decomposition functions are generally computed element-wise since the conditions on the i^{th} element of a decomposition function, in Definition 6, are dependant only on the i^{th} element of the vector field F. For this reason constructing a decomposition function for an n-dimensional system generally involves computing individual decomposition functions for n separate 1-dimensional systems. See Lemma 3.

2. In the application of Proposition 2, a decomposition function $d(x, w, \widehat{x}, \widehat{w})$ will only ever be evaluated when either $(x, w) \preceq (\widehat{x}, \widehat{w})$ or $(\widehat{x}, \widehat{w}) \preceq (x, w)$. For this reason, the conditions in Definition 6 can generally be relaxed so that a decomposition function need only be defined on this domain. See Remark 4.

3. Given two decomposition functions, d and d' for the same system, Proposition 2 will provide a tighter approximation of reachable sets with used with d, rather than d', in the instance where $d'(x, w, \widehat{x}, \widehat{w}) \preceq d(x, w, \widehat{x}, \widehat{w})$ holds when $(x, w) \preceq (\widehat{x}, \widehat{w})$ and $d(\widehat{x}, \widehat{w}, x, w) \preceq d'(x, w, \widehat{x}, \widehat{w})$ holds when $(\widehat{x}, \widehat{w}) \preceq (x, w)$. In this way, when constructing decomposition functions it is generally preferable to ensure that the evaluation of $d(x, w, \widehat{x}, \widehat{w})$ is *as large as possible* when $(x, w) \preceq (\widehat{x}, \widehat{w})$ and *as small as possible* when $(\widehat{x}, \widehat{w}) \preceq (x, w)$. Note that the techniques posited in Lemmas 4 and 5 implicitly attempt to maximize or minimize the valuation of a decomposition function in this way, in order to achieve less-conservative decomposition functions.

These observations play a key role in the results of the next section, where we show that (i) every continuous-time nondeterministic system as in (2.1) is mixed monotone and that (ii) there exists a unique *tight decomposition function* for each system that provides the least conservative reachable set approximations of any decomposition function for the same system when used with Proposition 2.

3.4 The Tight Decomposition Function

We next move to study the generality of the mixed monotonicity property and we provide an explicit answer to the question *When is a system mixed monotone with respect to some decomposition function?* Indeed, the main result of this section is to show that all continuous-time dynamical systems as in (2.1) are mixed monotone and, going further, we apply the theory developed in the previous section to provide an explicit construction for the decomposition function that provides the tightest attainable reachable set approximations when used with Proposition 2.

While the main results and theory provided in this work deal with continuous-time dynamical systems, we begin in Section 3.4.1 with a discussion on mixed monotonicity in the discrete-time setting of (2.50). In discrete-time, existence of decomposition functions was recently studied in [55] where it was shown that all discrete-time systems are mixed monotone with respect to a unique *tight decomposition function* that provides tighter approximations of reachable sets than any other decomposition function for the same system when used with the procedure described in (2.54). This tight decomposition function is defined as a, generally nonconvex, optimization problem which is evaluated over the system's update map and, in this way, evaluating a tight decomposition function at any point in the embedding space generally requires explicitly computing or reasoning about the system's reachable set itself. For this reason, tight decomposition functions for discrete-time systems cannot generally be used for efficient reachability analysis, unless the system's update map exhibits some special structure as to make it so that the tight decomposition function can be represented by a closed-form expression.

Following this discussion, we next move to the continuous-time setting in Section 3.4.2, and we prove an analogous result showing that all continuous-time system's as in (2.1) are mixed monotone. In the setting of continuous-time systems, it is generally not possible to compute the tightest hyperrectangle containing a reachable set exactly when using the theory of mixed monotone systems, except in a few, albeit, important special cases such as when (2.1) is monotone. Nonetheless, we provide a similar tight decomposition function construction which is applicable to all system as in (2.1), and which provides the tightest reachable sets attainable using Proposition 2. While our construction is similarly represented as an optimization problem, we observe that, in continuous-time, computing a tight decomposition function generally does *not* require computing or reasoning about the reachable set of (2.1), explicitly. This nuance can reduce the complexity of computing tight decomposition functions in closed-form, and we demonstrate though several examples how these closed-form representations then enable efficient reachability analysis for (2.1) using Proposition 2. Despite these advantages, even when a solution is available in closed-form, it is often defined piece-wise, and the number of pieces can scale exponentially with the dimension of the state and disturbance space. To address this point, we provide further discussion on the computational complexity of evaluating tight decomposition functions in Section 3.4.3.

3.4.1 Tight Decomposition Functions for Discrete-Time Mixed Monotone Systems

Consider the discrete-time system

$$x^+ = F(x, w) \tag{3.41}$$

as previously introduced in (2.50), where $x \in \mathcal{X}$ is the state and $w \in \mathcal{W}$ is the disturbance input. We are interested in applying the theory of mixed monotone systems to compute a hyperrectangular over-approximation of the system's 1-step reachable set

$$R(A) := \{F(x, w) \in \mathbb{R} \,|\, x \in A, w \in \mathcal{W}\}. \tag{3.42}$$

We recall from (2.54) that when $d(x, w, \widehat{x}, \widehat{w})$ is a decomposition function for (3.41), as defined in Definition 7, the reachable set of (3.41) can be efficiently over-approximated using two evaluations of the decomposition function:

$$R([\underline{x},\overline{x}]) \subseteq [\![E(\underline{x},\overline{x})]\!] := [d(\underline{x},\underline{w},\overline{x},\overline{w}), d(\overline{x},\overline{w},\underline{x},\underline{w})]. \tag{3.43}$$

As such, we are interested to know when there exists such a decomposition function for (3.41), *i.e.*, *When is the discrete-time system* (3.41) *mixed monotone?*

Existence of decomposition functions is a main point of study in [55], where the authors show how a decomposition function can always be attained via inspection of the set-containment relation (3.43). We recall this result below:

Proposition 4 ([55], Theorem 1)**.** *Any system of the form* (3.41) *is mixed monotone with respect to* d *constructed element-wise according to*

$$d_i(x,w,\widehat{x},\widehat{w}) = \begin{cases} \min\limits_{\substack{y\in[x,\widehat{x}]\\ z\in[w,\widehat{w}]}} F_i(y,z) & \textit{if } x \preceq \widehat{x} \textit{ and } w \preceq \widehat{w}, \\ \\ \max\limits_{\substack{y\in[\widehat{x},x]\\ z\in[\widehat{w},w]}} F_i(y,z) & \textit{if } \widehat{x} \preceq x \textit{ and } \widehat{w} \preceq w. \end{cases} \tag{3.44}$$

■

Observe that d from (3.44) satisfies the decomposition function conditions given in Definition 7 since it is true that, *e.g.*, d is monotonically non-decreasing in its first two inputs and monotonically non-increasing in its second two inputs, and that $d(x,w,x,w) = F(x,w)$. Furthermore, we derive d in (3.44), directly from the set containment condition in (3.43).

We refer to the unique decomposition function constructed in (3.44) as the *tight decomposition function* for the discrete-time system (3.41). When used with (3.43), a tight decomposition function will always provide the tightest hyperrectangle containing $R(\underline{x},\overline{x})$ in the sense that $R([\underline{x},\overline{x}]) \subseteq [\![E(\underline{x},\overline{x})]\!]$ and no proper hyperrectangular subset of $[\![E(\underline{x},\overline{x})]\!]$ contains $R([\underline{x},\overline{x}])$, since it is true that $d_i(x,w,\widehat{x},\widehat{w})$ is defined to be the minimum or maximum element of the update map $F(x,w)$ in the i^{th} coordinate. In contrast, iterating the embedding dynamics beyond one time-step generally results in hyperrectangular reachable set approximations that are no longer tight.

Despite the advantages of employing a tight decomposition function for reduced conservatism, computing the valuation of $d(x, w, \widehat{x}, \widehat{w})$ from (3.44) at any point in the embedding space generally requires computing the reachable set $R([\underline{x}, \overline{x}])$ of (2.50) in itself. For this reason, (3.44) cannot generally be employed to efficiently solve the reachability analysis problem unless, *e.g.*, a closed-form representation of d can be derived from the optimization problem structure in (3.44). On the other hand, knowing that such a decomposition function does exists means that a search directed by, for example, domain knowledge, is generally not unreasonable.

In the following section, we present an analogous definition for tight decomposition functions in the context of continuous-time mixed monotone systems. Importantly, evaluating a tight decomposition function in the continuous-time setting generally does not require explicitly computing or reasoning about a system's reachable set; although, our construction is similarly defined as an optimization problem. Nonetheless, we present numerous examples demonstrating how, in certain instances, a closed-form solution for a tight decomposition function can be attained by exploiting the structure of its construction as an optimazation problem.

3.4.2 Tight Decomposition Functions for Continuous-Time Mixed Monotone Systems

We now return to the continuous-time setting of (2.1). Our main result is to show that all continuous-time dynamical as in (2.1) are mixed monotone, and we provide an explicit construction for the decomposition function that provides the tightest reachable set approximations via Proposition 2.

In the setting of continuous-time systems, it is generally not possible to compute the tightest hyperrectangle containing a reachable set exactly when using the theory of mixed monotone systems, except in a few, albeit, important special cases such as when (2.1) is monotone. Nonetheless, we next move to define the notion of tight decomposition functions in the context of continuous-time systems, which differs from its discrete-time counterpart (3.44).

Definition 9 (Tight Decomposition Function)**.** A decomposition function d for (2.1) is *tight* if for any other decomposition function d' for (2.1), the follow hold for all $(x, w, \widehat{x}, \widehat{w})$ in the domain of

d

T1) $d'(x, w, \widehat{x}, \widehat{w}) \preceq d(x, w, \widehat{x}, \widehat{w})$ when $(x, w) \preceq (\widehat{x}, \widehat{w})$,

T2) $d(x, w, \widehat{x}, \widehat{w}) \preceq d'(x, w, \widehat{x}, \widehat{w})$ when $(\widehat{x}, \widehat{w}) \preceq (x, w)$. ■

Equivalently, $E'(x, \widehat{x}) \preceq_{\mathrm{SE}} E(x, \widehat{x})$ holds for all $x \preceq \widehat{x}$, where E and E' denote the corresponding embedding functions of d and d', respectively.

Observe that Definition 9 follows naturally from the theory laid out in Section 3.3, where we show how, *e.g.*, attempting to minimize or maximize the elements of $d(x, w, \widehat{x}, \widehat{w})$ can be used to arrive at tighter decomposition functions for (2.1). Furthermore, we next present an explicit construction for the tight decomposition function of an arbitrary continuous-time system as in (2.1).

Theorem 1. *Any system of the form* (2.1) *is mixed monotone with respect to* d *constructed element-wise according to*

$$d_i(x, w, \widehat{x}, \widehat{w}) = \begin{cases} \min\limits_{\substack{y \in [x, \widehat{x}] \\ y_i = x_i \\ z \in [w, \widehat{w}]}} F_i(y,\, z) & \text{if } x \preceq \widehat{x} \text{ and } w \preceq \widehat{w}, \\ \\ \max\limits_{\substack{y \in [\widehat{x}, x] \\ y_i = x_i \\ z \in [\widehat{w}, w]}} F_i(y,\, z) & \text{if } \widehat{x} \preceq x \text{ and } \widehat{w} \preceq w. \end{cases} \tag{3.45}$$

Moreover, d *is a tight decomposition function for* (2.1). ■

Proof. We begin by establishing that d from (3.45) is Lipschitz continuous; this is done by showing that d_i is Lipschitz in x, and Lipschitz continuity holds with respect to other arguments by analogous reasoning. Let $x^1, x^2, \widehat{x} \in \mathcal{X}$ and $w, \widehat{w} \in \mathcal{W}$, where we assume without loss of generality that $x^1 \preceq \widehat{x}$, $x^2 \preceq \widehat{x}$, and $w \preceq \widehat{w}$. Observe that for any $y^1 \in [x^1, \widehat{x}]$ with $y^1_i = x^1_i$, there exists $y^2 \in [x^2, \widehat{x}]$ with $y^2_i = x^2_i$ such that $\|y^1 - y^2\|_1 \leq \|x^1 - x^2\|_1$, and vice-versa, where $\|\cdot\|_1$ denotes the usual one-norm on $\mathbb{R}^n$. In particular, for any minimizer (y^1, z) that achieves the value of $d_i(x^1, w, \widehat{x}, \widehat{w})$ in the definition (3.45), there exists a point y^2 so that $F_i(y^2, z)$ upper bounds $d_i(x^2, w, \widehat{x}, \widehat{w})$ with $\|y^1 - y^2\|_1 \leq \|x^1 - x^2\|_1$, and vice-versa. It follows then that $\|d_i(x^1, w, \widehat{x}, \widehat{w}) - d_i(x^2, w, \widehat{x}, \widehat{w})\|_1 \leq L\|x^1 - x^2\|_1$ where L is a Lipschitz constant for F applicable on a neighborhood of $[x^1, \widehat{x}] \cup [x^2, \widehat{x}]$. Thus d_i is Lipschitz in x, and moreover d is Lipschitz in $x, \widehat{x}, w, \widehat{w}$.

We next show that d is a decomposition function for (2.1). Trivially, $d_i(x, w, x, w) = F_i(x, w)$ for all i and all $x \in \mathcal{X}$, $w \in \mathcal{W}$. We show that d satisfies Conditions D2–D4 from Definition 6 by showing that d_i satisfies the Kamke conditions K1 and K2 in Remark 2. Choose $x, y, \widehat{x} \in \mathcal{X}$ and $w, v, \widehat{w} \in \mathcal{W}$ as to satisfy the hypothesis of K1. Then $d_i(x, w, \widehat{x}, \widehat{w}) \leq d_i(y, v, \widehat{x}, \widehat{w})$ follows from the min/max construction of (3.45). This proves K1, and K2 is proven analogously. Thus, (2.1) is mixed monotone with respect to d.

Lastly, we show that d is a tight decomposition function for (2.1). Let d' be another decomposition function for (2.1) and choose $\underline{x}, \overline{x}, \underline{w}, \overline{w}$ so that $\underline{x} \preceq \overline{x}$ and $\underline{w} \preceq \overline{w}$. Additionally, choose $x \in [\underline{x}, \overline{x}]$ and $w \in [\underline{w}, \overline{w}]$. Then $(\underline{x}, \overline{x}) \preceq_{\mathrm{SE}} (x, x)$ and $(\underline{w}, \overline{w}) \preceq_{\mathrm{SE}} (w, w)$, and therefore

$$\begin{bmatrix} d'(\underline{x}, \underline{w}, \overline{x}, \overline{w}) \\ d'(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \end{bmatrix} \preceq_{\mathrm{SE}} \begin{bmatrix} d'(x, w, x, w) \\ d'(x, w, x, w) \end{bmatrix} = \begin{bmatrix} F(x, w) \\ F(x, w) \end{bmatrix}. \tag{3.46}$$

Since (3.46) holds for all $x \in [\underline{x}, \overline{x}]$ and all $w \in [\underline{w}, \overline{w}]$ we now have

$$\begin{bmatrix} d'(\underline{x}, \underline{w}, \overline{x}, \overline{w}) \\ d'(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \end{bmatrix} \preceq_{\mathrm{SE}} \begin{bmatrix} \min\limits_{y \in [\underline{x}, \overline{x}], y_i = \underline{x}_i, z \in [\underline{w}, \overline{w}]} F(y, z) \\ \max\limits_{y \in [\underline{x}, \overline{x}], y_i = \underline{x}_i, z \in [\underline{w}, \overline{w}]} F(y, z) \end{bmatrix},$$

and thus

$$\begin{bmatrix} d'(\underline{x}, \underline{w}, \overline{x}, \overline{w}) \\ d'(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \end{bmatrix} \preceq_{\mathrm{SE}} \begin{bmatrix} d(\underline{x}, \underline{w}, \overline{x}, \overline{w}) \\ d(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \end{bmatrix}.$$

Therefore d is a tight decomposition function for (2.1) as $\underline{x} \preceq \overline{x}$ and $\underline{w} \preceq \overline{w}$ were selected arbitrarily. This completes the proof. $\square$

The results of Theorem 1 are important in that they emphasize the generality of the mixed monotonicity property. Indeed, a key result of Theorem 1 is to show that all continuous-time dynamical systems as in (2.1) are mixed monotone, and a decomposition function can always be attained from the optimization problem (3.45). Note that, unlike its discrete-time counter part in (3.44), solving the optimization problem in (3.45) does not necessarily require explicit knowledge of the reachable set or its geometry. Moreover, while computing a tight decomposition function generally requires solving a nonconvex optimisation problem for each quadruple $(x, w, \widehat{x}, \widehat{w})$, we demonstrate later through many examples how the structure of the optimization problem in (3.45) can sometimes be exploited to compute tight decomposition functions in closed-form, as to allow for efficient reachability analysis using Proposition 2. Before this study, we next establish that a tight decomposition function, when used with Proposition 2, will provide tighter approximations of reachable sets than of any other decomposition function for the same system.

Proposition 5. *If d' is a decomposition function for* (2.1) *and d is a tight decomposition function for* (2.1)*, then for all $t \geq 0$*

$$[\![\Phi^E(t;\, a)]\!] \subseteq [\![\Phi^{E'}(t;\, a)]\!] \tag{3.47}$$

for all $a \in \mathcal{T}$ where Φ^E and $\Phi^{E'}$ denote the state transition functions of the embedding system (2.34) *constructed from d and d', respectively. Equivalently, d provides the tightest reachable set approximations, of any decomposition function for* (2.1)*, when used with Proposition 2.* ■

Proof. Let d and d' be such that T1 and T2 in Definition 9 hold. Let E and E' denote the embedding functions relative to d and d', respectively, and let Φ^E and $\Phi^{E'}$ denote the state transition functions of their respective embedding systems. Choose $a \in \mathcal{T}$, and define

$$\varphi^{E'}(t) = \Phi^{E'}(t;\, a), \text{ and } \varphi^{E}(t) = \Phi^{E}(t;\, a), \tag{3.48}$$

where we write $\varphi^{E'} =: (\underline{\varphi}^{E'}, \overline{\varphi}^{E'})$ and $\varphi^{E} =: (\underline{\varphi}^{E}, \overline{\varphi}^{E})$. Then

$$\dot{\varphi}^{E'} = E'(\underline{\varphi}^{E'}, \overline{\varphi}^{E'}), \text{ and } \dot{\varphi}^{E} = E(\underline{\varphi}^{E}, \overline{\varphi}^{E}). \tag{3.49}$$

We now show that $\varphi^{E'}(0) \preceq_{\mathrm{SE}} \varphi^{E}(0)$ implies $\varphi^{E'}(t) \preceq_{\mathrm{SE}} \varphi^{E}(t)$ for all $t \geq 0$. Assume there exists a time $T \geq 0$ such that

$$\varphi_i^{E'}(T) = \varphi_i^{E}(T) \text{ and } \varphi^{E'}(T) \preceq_{\mathrm{SE}} \varphi^{E}(T) \tag{3.50}$$

for some $i \in \{1, \cdots, 2n\}$. Consider first the case that $i \in \{1, \cdots, n\}$. Then

$$\begin{aligned} d_i'(\underline{\varphi}^{E'}(T), \underline{w}, \overline{\varphi}^{E'}(T), \overline{w}) &\leq d_i(\underline{\varphi}^{E'}(T), \underline{w}, \overline{\varphi}^{E'}(T), \overline{w}), \\ &\leq d_i(\underline{\varphi}^{E}(T), \underline{w}, \overline{\varphi}^{E}(T), \overline{w}), \end{aligned} \tag{3.51}$$

where the first inequality comes from the fact that d is a tight decomposition function for (2.1), and where the second inequality comes from Conditions K1 and K2 in Remark 2. Thus we now have $\dot{\varphi}_i^{E'}(T) \leq \dot{\varphi}_i^{E}(T)$. If instead (3.50) holds for some $i \in \{n+1, \cdots, 2n\}$, by a symmetric argument, $\dot{\varphi}_i^{E'}(T) \geq \dot{\varphi}_i^{E}(T)$. Therefore, always $\varphi^{E'}(t) \preceq_{\mathrm{SE}} \varphi^{E}(t)$, which is equivalently to (3.47) by (2.12). This completes the proof. □

Before proceeding further, we next move to demonstrate applicability of Theorem 1 through two examples where we show how, in certain instances, a tight decomposition function can be attained in closed-form.

Example 12. Consider the 1-dimensional quadratic polynomial system

$$\dot{x} = F^{\mathrm{Quad}}(w) = aw^2 + bw + c \tag{3.52}$$

where $x \in \mathbb{R}$ is the state, $w \in \mathbb{R}$ is the input and $a, b, c \in \mathbb{R}$ are fixed parameters of the vector field. We compute a tight decomposition function for (3.52) by exploiting the structure of the optimization problem (3.45) in order to arrive at a closed-form solution. We observe, in particular, that the minimum, or maximum, of a scalar-valued function, as in F^{Quad}, will either occur on the boundary of the function's domain or at a critical point in the interior of the domain. Furthermore, we observe that for all choices of a, b, c the function $F^{\mathrm{Quad}}(w)$ has only 1-critical point: $\frac{\partial F^{\mathrm{Quad}}}{\partial w}(w) = 0$

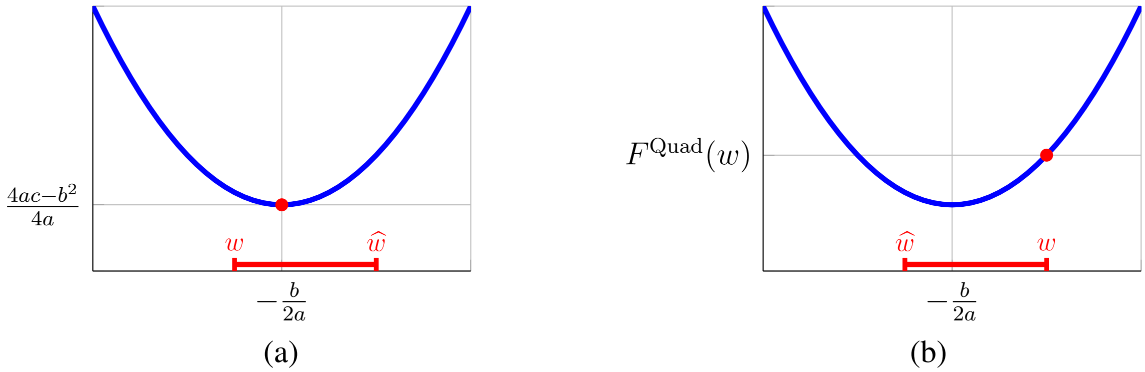


Figure 3.6: Example 12: Computing the tight decomposition function for the quadratic polynomial system (3.52). We show by cartoon how the decomposition function in (3.53) is formed. Subfigures: (a) When $w \leq \widehat{w}$, the tight decomposition function $d(w, \widehat{w})$ evaluates to the minimum of F^{Quad} over $[w, \widehat{w}]$, so that, *e.g.*, when $w \leq \frac{b}{2a} \leq \widehat{w}$ the evaluation is is $d(w, \widehat{w}) = \frac{4ac-b^2}{4a}$. (a) When $\widehat{w} \leq w$, the tight decomposition function $d(w, \widehat{w})$ evaluates to the minimum of F^{Quad} over $[\widehat{w}, w]$, so that, *e.g.*, when $|\widehat{w} + \frac{b}{2a}| \leq |w + \frac{b}{2a}|$ the evaluation is $d(w, \widehat{w}) = F^{\text{Quad}}(w)$.

only when $w = -\frac{b}{2a}$. This observation allows for attaining a closed-form solution to (3.45) in the context of (3.52) using the reasoning presented graphically in Figure 3.6. Moreover, we find that the system (3.52) is mixed monotone with a tight decomposition function given in closed-form by

$$\begin{aligned} d^{\text{Quad}}(w, \widehat{w}) &= \begin{cases} \min\limits_{z \in [w, \widehat{w}]} \; az^2 + bz + c & \text{if } w \leq \widehat{w}, \\ \\ \max\limits_{z \in [\widehat{w}, w]} \; az^2 + bz + c & \text{if } \widehat{w} \leq w \end{cases} \\ &= \begin{cases} \frac{-b^2+4ac}{4a} & \text{if } \frac{-b}{2} \in [aw, a\widehat{w}], \\ F^{\text{Quad}}(w) & \text{if } \frac{-b}{2} \notin [aw, a\widehat{w}] \text{ and } 0 \leq aw + a\widehat{w} + b, \\ F^{\text{Quad}}(\widehat{w}) & \text{if } \frac{-b}{2} \notin [aw, a\widehat{w}] \text{ and } 0 \geq aw + a\widehat{w} + b, \end{cases} \end{aligned} \tag{3.53}$$

an this construction is applicable across all choices of a, b, c.

As a specific instance of this result, consider the case where $a = 1$, $b = 0$ and $c = 2$ so that the quadratic dynamics in (3.52) become

$$\dot{x} = w^2 + 2 \tag{3.54}$$

and (3.54) is mixed monotone with respect to the tight decomposition function

$$d^{\mathrm{Quad}}(w, \widehat{w}) = \begin{cases} w^2 + 2 & \text{if } w \geq 0 \text{ and } w \geq -\widehat{w}, \\ \\ \widehat{w}_2^2 + 2 & \text{if } \widehat{w} \leq 0 \text{ and } w < -\widehat{w}, \\ \\ 2 \end{cases} \tag{3.55}$$

as prescribed in (3.53). Next, reconsider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x) = \begin{bmatrix} x_2^2 + 2 \\ x_1 \end{bmatrix}, \tag{3.56}$$

as previously studied in Examples 5, 8 and 11. We observe that the first entry of the dynamics

$$F_1(x) = F^{\mathrm{Quad}}(x_2) \tag{3.57}$$

where F^{Quad} in (3.57) refers to the case where $a = 1$, $b = 0$ and $c = 2$, and Lemma 3 now implies that a decomposition function for (3.56) is given by

$$d(x, \widehat{x}) = \begin{bmatrix} d^{\mathrm{Quad}}(x_2, \widehat{x}_2) \\ x_1 \end{bmatrix} \tag{3.58}$$

where, again, d^{Quad} in (3.58) refers to the setting in (3.55) where $a = 1$, $b = 0$ and $c = 2$. Indeed, (3.58) is a tight decomposition function for the 2-dimensional system (3.56), since it is true that d from (3.58) solves the optimization problem (3.45) in each entry, when taken with respect to the vector field F from (3.56). Furthermore, we observe that the tight decomposition function (3.58) is the *same* decomposition function for (3.56) as computed previously in (3.40) from Example 11; that is, (3.40) from Example 11 is a tight decomposition function for (3.56), and no other decomposition function for the same system will produce a tighter approximation of reachable sets when used with Proposition 2. We refer the reader back to Example 11 for a demonstration of how conservatism in the approximation of reachable sets is reduced using (3.58). ■

Example 13. Reconsider the simplified unicycle model

$$\dot{x} = F^{\cos}(w) = \cos(w) \tag{3.59}$$

as studied previously in Examples 7 and 10. Unlike in the setting of Example 12, where the vector field has at most one critical point within the domain of the optimization problem, the vector field $F^{\cos}$ has infinitely many critical points, and the general non-convexity of the dynamics reduces intuition as to how (3.45) may be solved. Nonetheless, we observe that a tight decomposition function for (3.59) can be attained in closed-form and is given by

$$d^{\cos}(w, \widehat{w}) := \begin{cases} \cos(w) & \text{if } (\sin(w),\, \sin(\widehat{w})) \preceq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \cos(\widehat{w}) & \text{if } (\sin(w),\, \sin(\widehat{w})) \succeq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \mathrm{sign}(w - \widehat{w}) & \text{if } |w - \widehat{w}| \geq 2\pi, \\ \mathrm{sign}(w - \widehat{w}) & \text{if } \sin(w) \geq 0 \geq \sin(\widehat{w}) \text{ and } |w - \widehat{w}| \leq 2\pi, \\ \mathrm{sign}(w - \widehat{w}) & \text{if } \sin(w)\sin(\widehat{w}) \geq 0 \text{ and } \pi \leq |w - \widehat{w}| \leq 2\pi, \\ \min\{\cos(w), \cos(\widehat{w})\} & \text{if } w \leq \widehat{w} \text{ and } \sin(w) \leq 0 \leq \sin(\widehat{w}) \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi, \\ \max\{\cos(w), \cos(\widehat{w})\} & \text{if } w \geq \widehat{w} \text{ and } \sin(w) \leq 0 \leq \sin(\widehat{w}) \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi. \end{cases} \tag{3.60}$$

To add further intuition, we plot the tight decomposition function $d^{\cos}(w, \widehat{w})$ in Figure 3.7(a) above the w–$\widehat{w}$ plane. Finally, we apply Proposition 2 with the tight decomposition function $d^{\cos}$ in order to attain a hyperrectangular over-approximation of $R(1; A)$ for $A = [-\frac{1}{2}, \frac{1}{2}]$ and $\mathcal{W} = [-\frac{\pi}{8}, \frac{\pi}{4}]$. We provide, in Figure 3.7(b), a comparison between the reachable sets attained from the tight

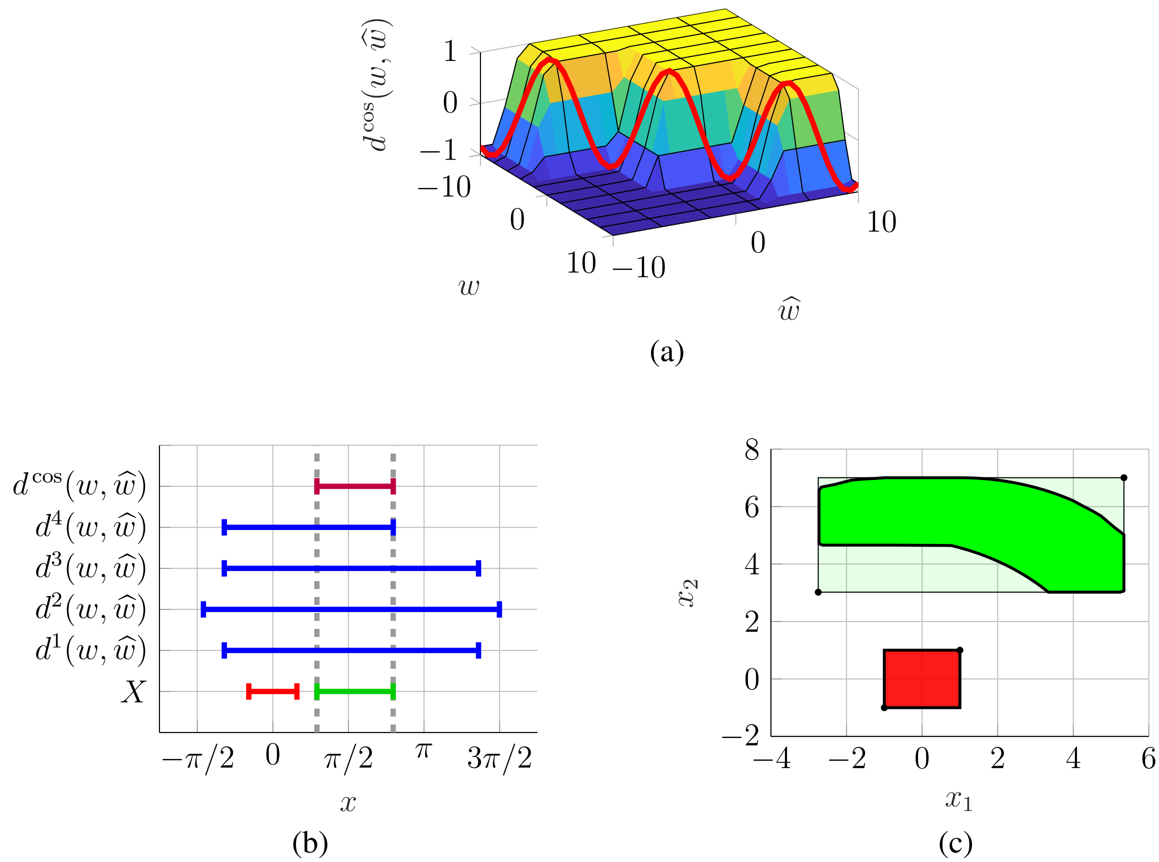


Figure 3.7: Example 13: Computing reachable sets for the kinematic unicycle model using a tight decomposition function. Subfigures: (a) The tight decomposition function for the simplified unicycle model (3.59) is plotted above the w–$\widehat{w}$ plane. Observe that $d^{\cos}(w, w) = \cos(w)$ and that $d^{\cos}(w, \widehat{w})$ is monotonically non-decreasing in w and monotonically non-increasing in $\widehat{w}$. (b) We compare the reachable sets attained from the tight decomposition function $d^{\cos}$ to those attained from the other, nontight, decomposition functions d^1, d^2, d^3 and d^4 for (3.61), as computed in Examples 7 and 10. The inital set $A = [-\frac{1}{2}, \frac{1}{2}]$ is shown as a red interval, the time-1 reachable set $R(1; A)$ is shown in green and the interval approximation of $R(1; A)$ attained from he application of Proposition 2 with $d^{\cos}$ is shown in purple. (c) We apply Proposition 2 with the tight decomposition (3.62) in order to over-approximate reachable sets for the 3-dimensional unicycle model (3.61). The inital set $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$ is shown in red, the time-6 reachable set $R(6; A)$ is shown in dark green and the rectangular reachable set approximation derived from the application of Proposition 2 is shown in light green.

decomposition function $d^{\cos}$, and those attained from the other, nontight, decomposition functions d^1, d^2, d^3 and d^4 for (3.61), as computed in Examples 7 and 10.

Furthermore, we next return to the setting of the 3-dimensional unicycle model

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = F^{\mathrm{Uni}}(x, w) = \begin{bmatrix} \cos(x_3) \\ \sin(x_3) \\ w_2 \end{bmatrix} \tag{3.61}$$

as previously studied in Examples 9 and 10, and where we recall $w_2 \in \mathcal{W}_2 = [-0.1, 0.1]$. A tight decomposition for the 3-dimensional system (3.61) is constructed via the application of Lemma 3 with individual tight decomposition functions for the three entries of the vector field F^{Uni}. This tight decomposition function is given by

$$d(x, w, \widehat{x}, \widehat{w}) = \begin{bmatrix} d^{\cos}(x_3, \widehat{x}_3) \\ d^{\sin}(x_3, \widehat{x}_3) \\ w_2 \end{bmatrix} \tag{3.62}$$

where $d^{\cos}$ denotes the tight decomposition function for (3.59), and is given by (3.60), and where $d^{\sin}$ denotes the tight decomposition function of the scalar system $\dot{x} = \sin(w)$ and is given by

$$d^{\sin}(w, \widehat{w}) := d^{\cos}\left(w - \frac{\pi}{2}, \widehat{w} - \frac{\pi}{2}\right). \tag{3.63}$$

The derivation of this result is provided in Section 3.5 of this work, and we refer the reader also to Appendix A which tabulates many other trigonometric systems and their associated tight decomposition functions. Moreover, we next apply the tight decomposition function (3.62) with Proposition 2, in order to over-approximate the reachable set $R(6; A)$ of (3.62) from the set of initial conditions $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$. Simulation results are provided in Figure 3.7(c). ■

The tight decomposition function constructed in (3.45) is given as a generally nonconvex optimization problem; however, the above examples do demonstrate how, in certain instances, it may be possible to attain a tight decomposition function in closed-form. In the following sections and examples, we demonstrate this point further, and provide methods and theory as to how tight decomposition functions can be constructed for more-complex and more-highly-nonlinear systems. Before this study, we first provide a more formal discussion on the computational complexity of obtaining and implementing tight decomposition functions.

3.4.3 Discussion

The main result of this section is to show that every continuous-time dynamical system as in (2.1) is mixed monotone, and we provide an explicit construction for the unique tight decomposition function that provides the tightest attainable reachable set approximations when used with Proposition 2. While computing a tight decomposing function at any point in the embedding space generally requires solving a nonconvex optimization problem, we show through example how, in certain instances, a tight decomposition function can be attained in closed-form, as to allow for, *e.g.*, efficient reachability analysis via Proposition 2.

In particular, we observe that, unlike the discrete-time setting of (3.44), computing the optimization problem in (3.45) does not require computing or reasoning about the system's reachable set explicitly. Instead, evaluating $d_i(x, w, \widehat{x}, \widehat{w})$ from (3.45) at some point in the embedding space requires computing the minimum or maximum of a system's vector-field over one face of an n-dimensional hyperrectangle. This distinction makes tight decomposition functions significantly easier to evaluate in the continuous-time setting, rather than in the discrete-time case; especially, in the instance where the state dimension n and the disturbance dimension m are small. Indeed, in this section, we have only demonstrated cases where, *e.g.*, tight decomposition functions can be attained for systems whose vector field's depend on at most one state or disturbance variable in each coordinate. In Section 3.5 of this work, we move significantly past the case of single-variable systems and vector fields, and study cases where closed-form representations of tight decomposition functions can be computed for more-complex higher-dimensional systems. Our approach is to represent each entry of the vector field in (2.1) as a composition of two functions, and we show how analysis of these functions can sometimes be used to compute a tight decomposition function for the initial dynamics in (2.1). See also the case study of Section 5.3 where we compute a decomposition function for a 7-dimensional nonlinear spacecraft system with disturbances using this approach.

Nonetheless, even when a solution is available in closed-form, it is often defined piece-wise, and the number of pieces can scale exponentially with the dimension of the state and disturbance space. This observation appears to contradict the purported benefit of employing mixed monotonicity in applications: a main benefit, as discussed earlier in Chapter 2, is that reachable sets for an n-dimensional mixed monotone system with disturbances can be *efficiently* over-approximated via a single simulation of a related $2n$-dimensional embedding system constructed from the decomposition function. However, in the instance where evaluating the tight decomposition function at a particular state in the embedding space may require a large number of function evaluations, the tractability of the approach diminishes, and one cannot expect computations to scale linearly in state dimension.

Regardless, in our experience, it is most beneficial to attempt to generate a tight decomposition function for one's system from the onset of analysis; rather than attempt to generate a more-conservative decomposition function, first. We observe, in particular, that often times a more-conservative decomposition function will in fact require more function evaluations than a tight decomposition function for the same system:

- this is the case in Example 11, for instance, where the tight decomposed function (3.40) requires the same number of function evaluations as the more-conservative decomposition function (3.37), and
- this is the case in Examples 10 and 13 where the tight decomposition function (3.60) requires less function evaluations than the more-conservative decomposition function (3.34), which is derived via the application of Lemmas 4 and 5.

Furthermore, once a tight decomposition function is attained in closed-form, it is sometimes possible to remove pieces and reduce function evaluations, in order to arrive at a more-conservative decomposition function, that is less-complex to evaluate algorithmically. In the next section, we present one such methodology for computing tight decomposition functions in closed form.

3.5 Compound Approaches for Computing Decomposition Functions

We show in this section how a tight decomposition function can sometimes be attained in closed-form, when the inital system's vector field F can be rewritten as the composition of two functions.

For ease of exposition in this section, we consider dynamical systems with one state but, perhaps, a high-dimensional disturbance input:

$$\dot{x} = F(x, w) \tag{3.64}$$

where $x \in \mathcal{X} \subset \mathbb{R}$ and $w \in \mathcal{W} \subset \mathbb{R}^m$. Recall from Section 3.3 that computing a decomposition function for an n-dimensional system generally requires computing individual decomposition functions for n different 1-dimensional system as in (3.64) and, moreover, the results of this section can generally be applied to systems of any state-dimension via the application of Lemma 3.

In particular, we consider a representation of the vector field of (3.64) as the composition of two functions

$$\dot{x} = f(x, g(w)) := F(x, w) \tag{3.65}$$

where $f : \mathcal{X} \times \mathbb{R}^p \to \mathbb{R}$ and $g : \mathcal{W} \to \mathbb{R}^p$ are chosen by hypothesis. Our main result is as follows:

Proposition 6. *Consider* (3.64) *and choose* $f : \mathcal{X} \times \mathbb{R}^p \to \mathbb{R}$ *and* $g : \mathcal{W} \to \mathbb{R}^p$ *so that* $f(x, g(w)) = F(x, w)$ *holds. If*

- *the system*

$$\dot{x} = f(x, v) \tag{3.66}$$

  with state $x \in \mathcal{X}_i$ *and disturbance input* $v \in \mathbb{R}^p$ *is mixed monotone with respect to a decomposition function* $d^f(x, v, \widehat{x}, \widehat{v})$*, and*

- $d^g(w, \widehat{w})$ *is an inclusion function for* g *as defined in Section 2.6.2, i.e., the discrete-time* *system*

$$v^+ = g(w) \tag{3.67}$$

with state $v \in \mathbb{R}^p$ *and disturbance input* $w \in \mathbb{R}^m$ *is mixed monotone with respect to* $d^g(w, \widehat{w})$*,*

then the system (3.64) *is mixed monotone with respect to* d *given by*

$$d(x, w, \widehat{x}, \widehat{w}) = d^f\left(x, d^g\left(w, \widehat{w}\right), \widehat{x}, d^g\left(\widehat{w}, w\right)\right). \tag{3.68}$$

■

Proof. We show that d is a decomposition function for (3.64) by showing that d satisfies the four conditions in Definition 6. Since d^f is a decomposition function for (3.66), and since $d^g(w, w) = w$, it holds that $d(x, w, x, w) = F(x, w)$ for all $x \in \mathcal{X}$ and $w \in \mathcal{W}$. To show that d from (3.68) satisfies conditions (D2)–(D4) of Definition 6, it is enough to show that, *e.g.*, $d^g(w, \widehat{w})$ is increasing in its first argument and decreasing in its second argument, so that, *e.g.*, $\frac{\partial d}{\partial w}(x, w, \widehat{x}, \widehat{w}) \geq 0$ and the remaining derivative conditions are satisfied similarly. □

We next show in Theorem 2 how, in some cases, Proposition 6 can be used for constructing a tight decomposition function for the system (3.64).

Theorem 2. *Consider* (3.64) *and choose* $f : \mathcal{X} \times \mathbb{R}^p \to \mathbb{R}$ *and* $g : \mathcal{W} \to \mathbb{R}^p$ *so that* $f(x, g(w)) = F(x, w)$ *holds. If*

- *no entry of* $w \in \mathcal{W} \subseteq \mathbb{R}^m$ *appears in more than one entry of* $g(w)$*,*
- $d^f(x, v, \widehat{x}, \widehat{v})$ *is the tight decomposition function for* (3.66)*, and*
- $d^g(w, \widehat{w})$ *is the tight decomposition function* (3.67)*,*

then the system (3.64) *is mixed monotone and the decomposition function* d *from* (3.68) *is a tight decomposition function for* (2.1). ■

The proof of Theorem 2 involves showing

$$d(x, w, \widehat{x}, \widehat{w}) = \begin{cases} \min\limits_{y \in [d^g(w,\widehat{w}), d^g(\widehat{w},x)]} f(x, y) & \text{if } (x, w) \preceq (\widehat{x}, \widehat{w}), \\ \max\limits_{y \in [d^g(\widehat{w},w), d^g(w,\widehat{w})]} f(x, y) & \text{if } (\widehat{x}, \widehat{w}) \preceq (x, w). \end{cases} \tag{3.69}$$

See also [42] for further generalizations of this result.

In practice, in our experience, Proposition 6 and Theorem 2 provide the dominant and most tractable methods for obtaining decomposition functions for nonlinear systems with more than a few state dimensions. As a demonstration, we next consider the 3-dimensional unicycle model in the more general setting of (3.2) and show how a tight decomposition function for this system can be computed by applying Theorem 2.

Example 14. Reconsider the 3-dimensional unicycle model

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = F^{\text{uni}}(x, w) = \begin{bmatrix} w_1 \cos(x_3) \\ w_1 \sin(x_3) \\ w_2 \end{bmatrix} \tag{3.70}$$

as studied previously in Examples 9, 10 and 13, but where we now consider a 2-dimensional disturbance $w \in \mathcal{W} \subset \mathbb{R}^2$. In the following, we show how a tight decomposition function for (3.70) is constructed using Theorem 2.

We begin by computing a tight decomposing function of the first entry of (3.70)

$$\dot{x}_1 = F(w) = w_1 \cos(x_3) \tag{3.71}$$

where now $x_1 \in \mathbb{R}$ is the state and $(w_1, x_3) \in \mathbb{R}^2$ is viewed as a disturbance, as prescribed in, *e.g.*, Lemma 3. Define

$$\begin{aligned} g(w_1, x_3) &= \begin{bmatrix} w_1 \\ \cos(x_3) \end{bmatrix} \\ F^{\text{Mult}}(v) &= v_1 v_2 \end{aligned} \tag{3.72}$$

where we observe that

$$F^{\text{Mult}}(g(w_1, x_3)) = w_1 \cos(x_3) = F_1^{\text{uni}}(x, w). \tag{3.73}$$

Furthermore, we observe that the system $\dot{v} = g(w_1, x_3)$ with state $v \in \mathbb{R}^2$ and disturbance $(w_1, x_3) \in \mathbb{R}^2$ is mixed monotone with a tight decomposition function given by

$$d^g(w, \widehat{w}) = \begin{bmatrix} w_1 \\ d^{\cos}(w_2, \widehat{w}_2) \end{bmatrix}, \tag{3.74}$$

and that the system $\dot{x} = F^{\text{Mult}}(v)$ with state $x \in \mathbb{R}$ and disturbance $v \in \mathbb{R}^2$ is mixed monotone with a tight decomposition function given in closed-form by

$$d^{\text{Mult}}(v, \widehat{v}) = \begin{cases} \min\{v_1 v_2, v_1 \widehat{v}_2, \widehat{v}_1 v_2, \widehat{v}_1 \widehat{v}_2\} & \text{if } v \preceq \widehat{v}, \\ \max\{v_1 v_2, v_1 \widehat{v}_2, \widehat{v}_1 v_2, \widehat{v}_1 \widehat{v}_2\} & \text{if } \widehat{v} \preceq v, \end{cases} \tag{3.75}$$

where $d^{\cos}$ in (3.74) denotes the tight decomposition function of $\dot{x} = \cos(w)$ as introduced previously in (3.60). Theorem 2 now implies that the system (3.71) is mixed monotone with respect to

$$d_1(w, \widehat{w}) = d^{\text{Mult}}(d^g(w, \widehat{w}), d^g(\widehat{w}, w)), \tag{3.76}$$

and since d^{Mult} and d^g are both tractably computable, so is d_1. A tight decomposition function for the second element of the dynamics $F_2^{\text{Uni}}(x, w)$ is also computed using this approach, and a tight decomposition function for the third entry is trivially given by $d_3(w_2, \widehat{w}_2) = w_2$. Thus, we have

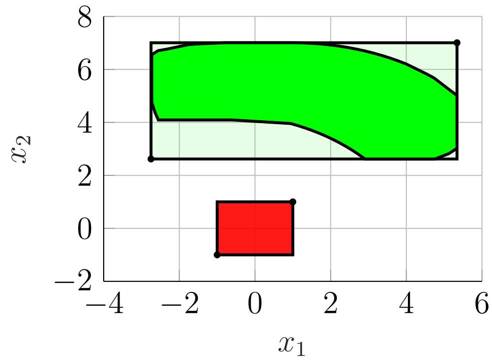


Figure 3.8: Example 14: Computing reachable sets for the 3-dimensional unicycle model (3.70) using a tight decomposition function. A hyperrectangular over-approximation of $R(6; A)$ is computed using Proposition 2 for inital set $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$ and where the disturbance space is $\mathcal{W} = [0.9, 1] \times [-0.1, 0.1]$. The inital set A is shown in red, the time-6 reachable set $R(6; A)$ is shown in dark green, and the over-approximation attained from the tight decomposition function of (14) is shown in light green.

arrived at a closed-form representation of the tight decomposition function of (3.70).

A demonstration is provided in Figure 3.8 where we apply Proposition 2 to compute a hyperrectangular over-approximation of $R(6; A)$ for inital set $A = [-1, 1]^2 \times [\frac{\pi}{3}, \frac{\pi}{2}]$ and where the disturbance space is $\mathcal{W} = [0.9, 1] \times [-0.1, 0.1]$. ■

Our previous examples mainly demonstrate the construction of tight decomposition functions for lower-dimensional systems. Indeed, we have motivated this preliminary study by showing how constructing decomposition functions for higher-dimensional systems generally requires constructing many decomposition functions for lower-dimensional systems, through the results of, *e.g.*, Lemma 3, Proposition 6 and Theorem 2. Nonetheless, when some entry of the dynamics in (3.64) is highly-nonlinear, it may be difficult to identify suitable composition functions f and g as to make the results of Theorem 2 applicable. For this reason, it may be preferable to employ, instead, the results of Proposition 6 in order to arrive at a non-tight decomposition function for (3.64), since this result is generally more applicable and can be used with non-tight decomposition functions for (3.66) and (3.67)—decomposition functions perhaps creating using Jacobian-bounds as in Proposition 3.

In the next section, we present a concluding case study where we compute a tight decomposition function for a 4-dimensional nonlinear bicycle model via the application of Theorem 2.

3.6 Case Study: Computing a Tight Decomposition Function for the Kinematic Bicycle Model

Consider the kinematic bicycle model

$$\begin{aligned} \dot{p}_x &= v\cos\left(\theta + \beta(\psi)\right) \\ \dot{p}_y &= v\sin\left(\theta + \beta(\psi)\right) \\ \dot{\theta} &= \frac{v}{l_r}\sin\left(\beta(\psi)\right) \\ \dot{v} &= a \\ \beta(\psi) &:= \tan^{-1}\left(\frac{l_r}{l_f + l_r}\tan\left(\psi\right)\right) \end{aligned} \tag{3.77}$$

as developed in [77], where $(p_x, p_y) \in \mathbb{R}^2$, $\theta \in \mathbb{R}$ and $v \in \mathbb{R}$ denote the position, heading, and velocity of the bicycle, respectively, and where $a \in \mathbb{R}$ and $\psi \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ are the linear acceleration and steering angle. The parameters, l_r and l_f denote the distances between the center of mass and the front and rear wheels, respectively, which are fixed, and $\beta(\psi)$ denotes the angle between vehicle's velocity and its heading. For notational simplicity, we represent the dynamics in (3.77) as

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = F(x, w) = \begin{bmatrix} x_4\cos(x_3 + \beta(w_1)) \\ x_4\sin(x_3 + \beta(w_2)) \\ \frac{1}{l_r}x_4\sin(\beta(w_2)) \\ w_2 \end{bmatrix} \tag{3.78}$$

where $x := (p_x, p_y, \theta, v) \in \mathbb{R}^4$ is the state and $w := (a, \psi) \in \mathbb{R} \times [-\frac{\pi}{2}, \frac{\pi}{2}]$. We construct a decomposition function in the following way:

We consider, first, the 1st entry of the dynamics

$$\dot{x}_1 = F_1(x, w) = x_4 \cos(x_3 + \beta(w_1)) \tag{3.79}$$

where now $x_1 \in \mathbb{R}$ is the state and $(x_3, x_4, w_1) \in \mathbb{R}^2 \times [-\frac{\pi}{2}, \frac{\pi}{2}]$ is viewed as the disturbance, as prescribed in Lemma 3. Next define

$$f^1(v) = v_1 \cos(v_2) \tag{3.80}$$

$$g(x_3, x_4, w_1) = \begin{bmatrix} x_4 \\ x_3 + \beta(w_1) \end{bmatrix} \tag{3.81}$$

where we observe that

$$f^1(g^1(x_3, x_4, w_1)) = F_1(x, w). \tag{3.82}$$

Since it is true that $\beta(w_1)$ is a monotonically increasing function observe that $\dot{v} = g(x_3, x_4, w_1)$ is mixed monotone with respect to

$$d^{g^1}(x_3, x_4, w_1, \widehat{x}_3, \widehat{x}_4, \widehat{w}_1) = \begin{bmatrix} x_4 \\ x_3 + \beta(w_1) \end{bmatrix} \tag{3.83}$$

and $\dot{x} = f(v)$ is mixed monotone with given in (3.76)

$$d_1^{\mathrm{Bi}}(x, w, \widehat{x}, \widehat{w}) = d_1^{\mathrm{Uni}} \left(\begin{bmatrix} x_4 \\ x_3 + \beta(w_1) \end{bmatrix}, \begin{bmatrix} \widehat{x}_4 \\ \widehat{x}_3 + \beta(\widehat{w}_1) \end{bmatrix} \right) \tag{3.84}$$

where d_1^{Uni} is the 1st entry of the tight decomposition function (3.76) for the simplified unicycle model (3.76). Using this same approach, the remaining entries of the tight decomposition function can also be formed

$$
\begin{aligned}
d_1^{\mathrm{Bi}}(x, w, \widehat{x}, \widehat{w}) &= d_1^{\mathrm{Uni}}\left(\begin{bmatrix} x_4 \\ x_3 + \beta(w_1) \end{bmatrix}, \begin{bmatrix} \widehat{x}_4 \\ \widehat{x}_3 + \beta(\widehat{w}_1) \end{bmatrix}\right) \\
d_2^{\mathrm{Bi}}(x, w, \widehat{x}, \widehat{w}) &= d_2^{\mathrm{Uni}}\left(\begin{bmatrix} x_4 \\ x_3 + \beta(w_1) \end{bmatrix}, \begin{bmatrix} \widehat{x}_4 \\ \widehat{x}_3 + \beta(\widehat{w}_1) \end{bmatrix}\right) \\
d_3^{\mathrm{Bi}}(x, w, \widehat{x}, \widehat{w}) &= d_2^{\mathrm{Uni}}\left(\begin{bmatrix} \frac{1}{l_r} x_4 \\ \beta(w_1) \end{bmatrix}, \begin{bmatrix} \frac{1}{l_r} \widehat{x}_4 \\ \beta(\widehat{w}_1) \end{bmatrix}\right) \\
d_4^{\mathrm{Bi}}(x, w, \widehat{x}, \widehat{w}) &= w_2.
\end{aligned}
\tag{3.85}
$$

In the experience of the authors, when decomposing a system with trigonometric components in the vector field, it is often required to exploit compound approached in decomposition function construction. We refer the reader to Appendix A in this work, where we tabulate several other decomposition functions for trigonometric systems, and these decomposition functions are derived using compound approaches.

3.7 Conclusion

In this chapter, we present a comprehensive framework for computing decomposition functions for mixed monotone systems. Our main result is to show that all continuous-time systems bearing a locally Lipschitz continuous vector field are mixed monotone, and we present a construction for the unique tight decomposition function that provides the tightest attainable approximations of reachable sets using the theory laid out thus far. Numerous approaches are provided for constructing (tight) decomposition functions, and we demonstrate these approaches through several examples, including a case study to a 4-dimensional nonlinear bicycle system.

3.8 Exercises

Problem 3.1: Given a system, $\dot{x} = F(x, w)$, show that the set of corresponding decomposition function for this system is a convex set, in the sense that when d^1 and d^2 are decomposition functions for $\dot{x} = F(x, w)$, it is also true that for all $\alpha \in [0, 1]$

$$d(x, w, \widehat{x}, \widehat{w}) := \alpha d^1(x, w, \widehat{x}, \widehat{w}) + (1 - \alpha) d^2(x, w, \widehat{x}, \widehat{w}) \tag{3.86}$$

is a decomposition function as well.

Problem 3.2: Consider the linear mapping

$$y = F(x) = Ax \tag{3.87}$$

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}^m$ and $A \in \mathbb{R}^{n \times m}$. Given a hyperrectangular set of inputs, $[\underline{x}, \overline{x}] \subset \mathbb{R}^n$, find a closed-form expression for $\underline{y}, \overline{y}$, so that $[\underline{y}, \overline{y}] \subset \mathbb{R}^m$ is the tightest hyperrectangle containing the image $\{y \in \mathbb{R}^m \,|\, y = Ax, x \in [\underline{x}, \overline{x}]\}$.

Problem 3.3: Consider $A \in \mathbb{R}^{n \times m}$ and $B \in \mathbb{R}^{m \times p}$. Show that both

$$[AB]^+ \;\preceq\; [A]^+[B]^+ + [A]^-[B]^- \tag{3.88}$$

and

$$[AB]^- \;\succeq\; [A]^+[B]^- + [A]^-[B]^+ \tag{3.89}$$

hold always, where now $\preceq$ and $\succeq$ are understood to apply componentwise over matrices.

Consider now the discrete-time linear system

$$x^+ = F(x) = Ax \tag{3.90}$$

with state $x \in \mathbb{R}^n$, and define by

$$R(R(A)) := \{A^2 x \,|\, x \in [\underline{x}, \overline{x}]\} \tag{3.91}$$

the 2-step reachable set of (3.90). How might one go about applying mixed monotonicity to compute the *tightest hyperrectangle* containing the 2-step reachable set? Recall that the tight decomposition function of (3.90) can not be applied directly to attain this result.

CHAPTER 4

MIXED MONOTONICITY FOR EFFICIENT REACHABILITY ANALYSIS

This chapter presents a suite of reachability analysis tools for a mixed monotone systems, and we study complex system properties beyond simple forward-time reachability. Indeed, we have shown already in Chapter 2 how the decomposition function of a mixed monotone system facilitates the efficient over-approximation of reachable sets using hyperrectangles. In this chapter, we show how this *same* decomposition can be used with broader applicability in systems' analysis.

We begin by studying a series of variants on the reachability analysis problem previously introduced in Chapter 2. Specifically, given a dynamical system, we are now interested in computing both (i) over-approximations of *backward-time reachable sets* for the inital forward-time system, and (ii) *under-approximations* forward-time reachable sets. Our approach involves constructing a decomposition function for a corresponding set of *backward-time dynamics*, however we show how such a backward-time decomposition function can be immediately identified from a decomposition function for the forward-time dynamics. In this way, one will only ever need to construct a single decomposition function to apply the tools herein.

Next, we move beyond finite-time reachability analysis and study time-invariant system properties using mixed monotonicity. A particular problem of interest involves computing *robustly forward invariant sets* for systems with disturbances; such forward invariant sets have principal use cases in safety for autonomous robotics, since they can be used to reason about system trajectories on an infinite-time horizon [17, 47–49]. Our main result is to show how robustly forward invariant sets for mixed monotone systems can be efficiently identified from the *equilibria* of the deterministic embedding system [35, 36]. Indeed, the deterministic embedding system of a mixed monotone system can induce stable, or even globally stable equilibria, and we show also how stability analysis in the embedding space can be used to reason about the attractivity of the invariant sets derived using our approach. As a final tool, we show how robustly forward invariant sets for mixed monotone systems can also be identified from closed periodic orbits in the embedding space.

This chapter is written in two main parts: The first part, Section 4.1, deals with extending the reachability analysis techniques introduced previously in Chapter 2. From the initial dynamics of a mixed monotone system, we construct a backward-time dynamical model in Section 4.1.1 and we show how forward-time reachability on the backward-time model allows for over-approximating backward-time reachable sets for the inital forward-time dynamics. This backward-time model is also employed in Section 4.1.2 for the under-approximation of forward-time reachable sets for the initial dynamics. Finally, we attempt to summarise our previous results through a cohesive theory as to how reachable sets can be efficiently under and over-approximated for mixed monotone systems using a single decomposition function for the forward-time dynamics. This summary appears in Section 4.1.3. The second part of this chapter, Section 4.2, studies how robustly forward invariant sets for mixed monotone system can be efficiently identified from invariant sets in the embedding space. Two main kinds of invariant sets for the embedding system are considered: (i) *equilibria* for the embedding system are studied in Section 4.2.1 and such equilibria can be used to identify hyperrectangular invariant sets for the initial system, and (ii) *closed periodic orbits* for the embedding system are studied in Section 4.2.3, and such periodic orbits can be used to identify invariant sets for the initial system with more complex geometries. An intermediary discussion is also provided in Section 4.2.2.

4.1 Advanced Reachability Analysis via Mixed Monotonicity

We begin by studying a series of variants on the reachability analysis problem previously introduced in Chapter 2. Specifically we are now interested in computing both (i) over-approximations of *backward-time reachable sets* for (2.1), and (ii) *under-approximations* forward-time reachable sets for (2.1). Our approach involves constructing a decomposition function for a corresponding set of *backward-time dynamics*, however we show how such a backward-time decomposition function can be immediately identified from a decomposition function for the forward-time dynamics

(2.1). In this way, one will only ever need to construct a single decomposition function to apply the tools in this section, and this task can be accomplished using the tools of Chapter 3.

4.1.1 Backward-Time Reachability Analysis for Mixed Monotone Systems

In this section, we present a result analogous to Proposition 2 for over-approximating finite-time backward reachable sets for mixed monotone systems. See Definition 10.

Definition 10. The set of initial conditions for which there exists a $\mathbf{w} : [0, t] \to \mathcal{W}$ capable of driving (2.1) to the set $A \subseteq \mathcal{X}$ in time $t \geq 0$ is given by

$$W(t; A) := \{x \in \mathcal{X} \mid \phi(t; x, \mathbf{w}) \in A \text{ for some } \mathbf{w} : [0, t) \to \mathcal{W}\} . \tag{4.1}$$

■

The set $W(t; A) \subseteq \mathcal{X}$ from (4.1) is the *time-t backward reachable set of* (2.1) *from* $A \subset \mathcal{X}$, and when A and t are clear from context, we refer to $W(t; A)$ simply as the *backward reachable set*. The remainder of this section studies means of computing hyperrectangular over-approximations of $W(t; A)$ from terminal sets A that are also a hyperrectangles, and our approach is to apply tools of mixed monotonicity to a corresponding set of *backward-time dynamics* for (2.1).

The system (2.1) induces the backward-time dynamics

$$\dot{x} = G(x, w) := -F(x, w) \tag{4.2}$$

where $x \in \mathcal{X}$ and $w \in \mathcal{W}$ retain their definitions from (2.1) as the state and disturbance and, importantly, the forward-time dynamics (2.1) and the backward-time dynamics (4.2) are related in the following way: if $x_1 = \phi(t; x_0, \mathbf{w})$ for some $\mathbf{w} : [0, t] \to \mathcal{W}$, then $x_0 = \psi(t; x_1, \mathbf{w}')$ for $\mathbf{w}'(\tau) = \mathbf{w}(t - \tau)$, and where ψ denotes the state transition function of (4.2). We depict this connection graphically in Figure 4.1. Furthermore, observe that for all $A \subseteq \mathcal{X}$,

$$W(t; A) = R^G(t; A) \tag{4.3}$$

Figure 4.1: Backward-Time Reachability Analysis for Dynamical Systems: The time-t backward reachable set of (2.1) is shown by cartoon in Figure 4.1(a). $W(t; A)$ is the set of initial system conditions which are capable of driving (2.1) to the set A in time t under some disturbance signal. We show in Figure 4.1(b) how when a trajectory $x_1 = \phi(t; x_0, \mathbf{w})$ beginning at state $x_0 \in W(t; A)$ ends at state $x_1 \in A$, it is also true that $x_0 = \psi(t; x_1, \mathbf{w}')$ for $\mathbf{w}'(\tau) = \mathbf{w}(t-\tau)$, where ψ denotes the state transition function of the backward-time dynamics (4.2). In this way, $W(t; A) = R^G(t; A)$.

holds, where $R^G(t; A)$ denotes the time-t forward reachable set of (4.2) and is given by (2.2). In this way, the backward-time reachable set $W(t; A)$ of (2.1) can be efficiently over-approximated by applying the forward-time reachability analysis procedure given in Proposition 2 with a decomposition function for the backward-time dynamics (4.2). Our main result is as follows:

Proposition 7. *Let* (4.2) *be mixed monotone with respect to* d^G*. Choose a hyperrectangular terminal set of states* $[\![a]\!] \subset \mathcal{X}$*, so that* $a \in \mathcal{T} \subset \mathbb{R}^{2n}$*. If* $\Phi^{E^G}(\tau; a) \in \mathcal{T}$ *for all* $0 \leq \tau \leq t$*, then*

$$W(t; [\![a]\!]) \subseteq [\![\Phi^{E^G}(t; a)]\!] \tag{4.4}$$

where E^G *denotes the embedding function relative to* d^G*, as prescribed in* (2.34)*, and where* $W(t; A)$ *denotes the time-t backward reachable set of* (2.1)*, as prescribed in* (4.1). ■

Since d^G is a decomposition function for (4.2), the corresponding embedding system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E^G(x, \widehat{w}) := \begin{bmatrix} d^G(x, w, \widehat{x}, \widehat{w}) \\ d^G(\widehat{x}, \widehat{w}, x, w) \end{bmatrix} \tag{4.5}$$

satisfies the natural properties laid out in Chapter 2:

- the embedding system (4.5) is monotone with respect to the southeast order,

- the upper-triangle set $\mathcal{T} := \{(\underline{x}, \overline{x}) \in \mathcal{X} \times \mathcal{X} \mid \underline{x} \preceq \overline{x}\}$ is forward invariant for (4.5), and

- the set of embedding system states whose vector field points into the southeast cone $\mathcal{S} := \{(\underline{x}, \overline{x}) \in \mathcal{T} \mid 0 \preceq_{\mathrm{SE}} E^G(\underline{x}, \overline{x})\}$ is forward invariant for (4.5), as well.

Furthermore, while it is true that a decomposition function for the backward-time system (4.2) can be computed using the theory and tools laid out in Chapter 3, we observe that it is generally possible to obtain a decomposition function for backward-time system (4.2) directly from the forward-time vector-field; see Lemma 6.

Lemma 6. If the forward-time dynamics $\dot{x} = F(x, w)$ from (2.1) are mixed monotone with respect to $d^F(x, w, \widehat{x}, \widehat{w})$, then the backward-time dynamics $\dot{x} = G(x, w)$ from (4.2) are mixed monotone with respect to $d^G(x, w, \widehat{x}, \widehat{w})$ given element-wise by

$$d_i^G(x, w, \widehat{x}, \widehat{w}) := -d_i^F(\widehat{x}_{[i:x]}, \widehat{w}, x, w). \tag{4.6}$$

Furthermore, if d^F is a tight decomposition function for (2.1), *i.e.*, d^F solves the optimization problem in (3.45), then d^G is a tight decomposition function for (4.2). ■

We demonstrate the bounding procedure from Proposition 7 in the following example.

Example 15. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x, w) = \begin{bmatrix} x_1 x_2 + w \\ x_1 + 1 \end{bmatrix} \tag{4.7}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W} = [0, \frac{1}{4}]$, which is mixed monotone with a tight decomposition function given by

$$\begin{aligned} d_1^F(x, w, \widehat{x}, \widehat{w}) &= \begin{cases} x_1 x_2 + w & \text{if } x_1 \geq 0, \\ x_1 \widehat{x}_2 + w & \text{if } x_1 < 0, \end{cases} \\ d_2^F(x, w, \widehat{x}, \widehat{w}) &= x_1 + 1. \end{aligned} \tag{4.8}$$

We first demonstrate the forward-time reachability analysis technique: we apply Proposition 2 with d^F from (4.8), in order to attain a rectangular over-approximation of $R(1; A)$ where $A = [-\frac{1}{4}, \frac{1}{4}] \times [-\frac{1}{2}, 0]$. Simulation results are provided in Figure 4.2.

Next, we consider the backward-time dynamics $\dot{x} = -F(x, w)$ of (4.7), which are given by

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = G(x, w) = \begin{bmatrix} -x_1 x_2 - w \\ -x_1 - 1 \end{bmatrix}, \tag{4.9}$$

and (4.9) is also a mixed monotone system with a tight decomposition function given by

$$\begin{aligned} d_1^G(x, w, \widehat{x}, \widehat{w}) &= \begin{cases} -x_1 x_2 - \widehat{w} & \text{if } x_1 \leq 0, \\ -x_1 \widehat{x}_2 - \widehat{w} & \text{if } x_1 > 0, \end{cases} \\ d_2^G(x, w, \widehat{x}, \widehat{w}) &= -\widehat{x}_1 - 1. \end{aligned} \tag{4.10}$$

To see this, observe that it is possible to apply Lemma 6 with d^F from (4.8) in order to arrive at the backward-time decomposition function d^G from (4.10). Furthermore, Proposition 7 now implies that the time-t backward reachable set of (4.7) is efficiently over-approximated via a simulation of the embedding system (2.34) taken with respect to d^G from (4.10). A demonstration is provided in Figure 4.2 where we apply Proposition 7 to compute a hyperrectangular over-approximation of $W(1; A)$ for the parameters taken previously. ■

In the following section, we show how a decomposition function d^G for the backward-time dynamics (4.2) has applicability beyond backward-time reachability analysis problems, and we show, specifically, how under-approximation of forward-time reachable sets for (2.1) can be computed using d^G, as well. Further applications of backward-time mixed monotonicity, pertaining to the existence of forward invariant sets for (2.1), are presented later in Section 4.2.

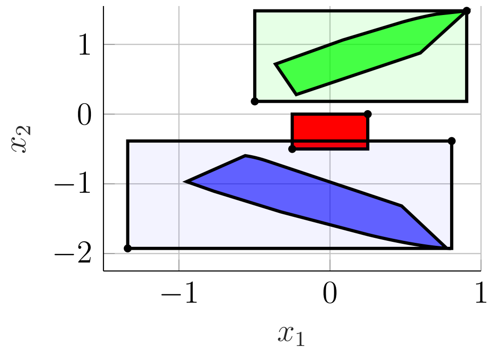


Figure 4.2: Example 15: Computing backward-time reachable sets for (4.7) by applying Proposition 7. The set $A = [-\frac{1}{4}, \frac{1}{4}] \times [-\frac{1}{2}, 0]$ is shown in red. The time-1 backward-reachable set $W(1; A)$ of (4.7) is shown in blue, and the hyperrectangular over-approximation of $W(1; A)$, derived from the application of Proposition 7, is shown in light blue. The time-1 forward-reachable set $R(1; A)$ of (4.7) is shown in green, and the hyperrectangular over-approximation of $R(1; A)$, derived from the application of Proposition 2, is shown in light green.

4.1.2 Under-Approximating Reachable Sets via Mixed Monotonicity

We next move to study how *under-approximations* of reachable sets are computed via the mixed monotonicity property. In particular, given a system (2.1), a time $t \geq 0$ and a set of initial conditions $A \subseteq \mathcal{X}$, we are interested in computing a hyperrectangle B so that $B \subseteq R(t; A)$. We show in the following Proposition how such under-approximations are computed similarly via a decomposition-function d^G for the backward-time dynamics (4.2).

Proposition 8. *Consider the forward-time dynamics* (2.1) *and the backward-time dynamics* (4.2)*. Given a decomposition function d^G for* (4.2)*, construct the backward-time dynamics of the embedding system* (2.34)*, i.e., construct the $2n$-dimensional deterministic system*

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = -E^G(x, \widehat{x}) = \begin{bmatrix} -d^G(x, \underline{w}, \widehat{x}, \overline{w}) \\ -d^G(\widehat{x}, \overline{w}, x, \underline{w}) \end{bmatrix}, \tag{4.11}$$

with state transition function Φ^{-E^G}. Choose a hyperrectangular set of inital conditions $[\![a]\!] \subseteq \mathcal{X}$, so that $a \in \mathcal{T} \subset \mathbb{R}^{2n}$. If $\Phi^{-E^G}(\tau; a) \in \mathcal{T}$ for all $0 \leq \tau \leq t$ then

$$[\![\Phi^{-E^G}(t; a)]\!] \subseteq R(t; [\![a]\!]). \tag{4.12}$$

■

Proof. Let E^G denote the embedding function relative to d^G and let Φ^{E^G} denote the state transition function of its embedding system. Then for all $a_0, a_1 \in \mathcal{T}$ and for all $t \geq 0$ we have that $a_1 = \Phi^{E^G}(t; a_0)$ if and only if $a_0 = \Phi^{-E^G}(t; a_1)$. See Figure 4.1(b).

Choose a hyperrectangular inital set $[\![a_0]\!] \subset \mathcal{X}$ so that $a_0 \in \mathcal{T}$ and choose a time $t \geq 0$. We prove Proposition 8 by showing that for all $x_1 \in [\![\Phi^{-E^G}(t; a_0)]\!]$ there exists an $x_0 \in [\![a_0]\!]$ and a disturbance input $\mathbf{w} : [0, t] \to \mathcal{W}$ so that $x_1 = \phi(t;\, x_0, \mathbf{w})$.

Define $a_1 := \Phi^{-E^G}(t; a_0)$ and choose any $x_1 \in [\![a_1]\!]$. Now $a_1 \preceq_{\mathrm{SE}} (x_1, x_1)$ holds by (2.12), and

$$a_0 = \Phi^{E^G}(t;\, a_1) \preceq_{\mathrm{SE}} \Phi^{E^G}(t;\, (x_1,\, x_1)) \tag{4.13}$$

follows from the monotonicity of the embedding system relative to E. As a result of Proposition 2, for any $\mathbf{w}' : [0,\, t] \to \mathcal{W}$ we now have that $\psi(t; x_1, \mathbf{w}') \in [\![\Phi^E(t;\, a_1)]\!] = [\![a_0]\!]$ where ψ is the state transition function of (4.2). Take $x_0 = \psi(t;\, x_0, \mathbf{w}')$ and define $\mathbf{w}(\tau) := \mathbf{w}'(t - \tau)$. Then $x_1 = \phi(t;\, x_0, \mathbf{w})$. This completes the proof. □

While (4.11) is constructed from the embedding function of the backward-time dynamics (4.2), it is important to realize that the system in (4.11) is *not* a monotone system, since it is generally true that backward-time trajectories of a monotone system do not maintain an ordering property. As such, the upper-triangular set $\mathcal{T}$ may not be forward invariant for (4.11) and the results of Proposition 8 apply so long as trajectories of (4.11) remain in $\mathcal{T}$.

Furthermore, observe from the proof above that the reachability procedure posited in Proposition 8 implicitly under-approximates the set of final system conditions which are *only* reached when the system begins in $[\![a]\!]$. That is, defining by

$$R'(t; A) := \{x_1 \in \mathcal{X} \mid \psi(t; x_1, \mathbf{w}) \in A \text{ for all } \mathbf{w} : [0, t] \to \mathcal{W}\} \tag{4.14}$$

the set of final system conditions may only be reached in time $t \geq 0$ from the initial set A, we now have

$$\llbracket \Phi^{-E^G}(t;a) \rrbracket \subseteq R'(t;\llbracket a \rrbracket) \subseteq R(t;\llbracket a \rrbracket) \subseteq \llbracket \Phi^{E^F}(t;a) \rrbracket \tag{4.15}$$

holds for all time.

As a final note, observe that a tight decomposition function d^G will provide the *largest* under-approximations of forward-time reachable sets attainable used with Proposition 8, and further discussion on this point is provided in the following section. Before this discussion, we next move to demonstrate the results of Proposition 8 through example.

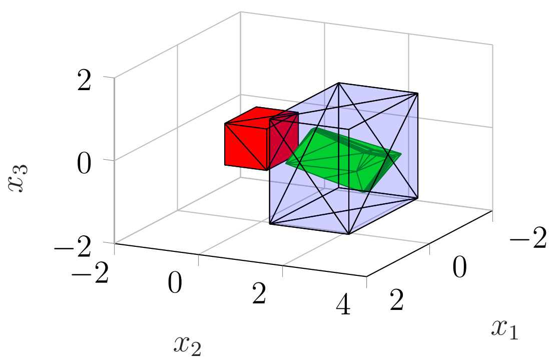
Example 16. Consider the 3-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = F(x,w) = \begin{bmatrix} w_1 x_2^2 - x_2 + w_2 \\ x_3 + 2 \\ x_1 - x_2 - w_1^3 \end{bmatrix}, \tag{4.16}$$

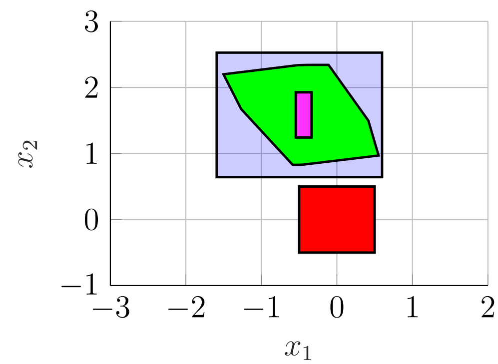
with state space $\mathcal{X} = \mathbb{R}^3$ and disturbance space $\mathcal{W} \subset \mathbb{R}^2$, which is a mixed monotone system with a tight decomposition function d^F given element-wise by

$$\begin{aligned} d_1^F(x,w,\widehat{x},\widehat{w}) &= \begin{cases} \frac{-1}{4w_1} + w_2 & \text{if } w_1 x_2 \leq \frac{1}{2} \leq w_1 \widehat{x}_2, \\ w_1 x_2^2 - x_2 + w_2 & \text{if } \frac{1}{2} \leq w_1 x_2 \leq w_1 \widehat{x}_2, \\ w_1 \widehat{x}_2^2 - \widehat{x}_2 + w_2 & \text{if } w_1 x_2 \leq w_1 \widehat{x}_2 \leq \frac{1}{2}, \end{cases} \\ d_2^F(x,w,\widehat{x},\widehat{w}) &= x_3 + 3, \\ d_3^F(x,w,\widehat{x},\widehat{w}) &= x_1 - \widehat{x}_2 - \widehat{w}_1^3. \end{aligned} \tag{4.17}$$

We first compute a hyperrectangular over-approximation of $R(\frac{1}{2};A)$ using Proposition 2 with d, where we take an initial set $A = [-\frac{1}{2},\frac{1}{2}]^3$ and where the disturbance space is $\mathcal{W} = [-\frac{1}{4},0] \times [0,\frac{1}{4}]$. Simulation results are provided in Figure 4.3.



(a) Simulation results.



(b) Projection of Figure 4.3(a) onto the x_1–x_2 plane

Figure 4.3: Example 16: Computing over- and under-approximations of reachable sets for (4.16) by applying Propositions 2 and 8. The initial set $A = [-\frac{1}{2}, \frac{1}{2}]^3$ is shown in red. The time-$\frac{1}{2}$ reachable set $R(\frac{1}{2};\, A)$ is shown in green. A hyperrectangular over-approximation of $R(\frac{1}{2};\, A)$ is computed from the embedding system (2.34) as described in Proposition 2 and is shown in light blue. A hyperrectangular under-approximation of $R(\frac{1}{2};\, A)$ is computed from (4.11) as described in Proposition 8 and is shown in pink.

Next, we consider the backward-time dynamics

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = G(x, w) = \begin{bmatrix} -w_1 x_2^2 + x_2 - w_2 \\ -x_3 - 2 \\ -x_1 + x_2 + w_1^3 \end{bmatrix} \tag{4.18}$$

as prescribed in (4.2) and we observe that, for all i, the i^{th} entry of the vector field $F_i(x, w)$ does not depend on x_i. Lemma 6 now implies that the backward-time dynamics are mixed monotone with respect to the tight decomposition function $d^G(x, w, \widehat{x}, \widehat{w}) = -d^F(\widehat{x}, \widehat{w}, x, w)$ as given by

$$\begin{aligned} d_1^G(x, w, \widehat{x}, \widehat{w}) &= \begin{cases} \frac{1}{4\widehat{w}_1} - \widehat{w}_2 & \text{if } \widehat{w}_1 \widehat{x}_2 \leq \frac{1}{2} \leq \widehat{w}_1 x_2, \\ -\widehat{w}_1 \widehat{x}_2^2 + \widehat{x}_2 - \widehat{w}_2 & \text{if } \frac{1}{2} \leq \widehat{w}_1 \widehat{x}_2 \leq \widehat{w}_1 x_2, \\ -\widehat{w}_1 x_2^2 + x_2 - \widehat{w}_2 & \text{if } \widehat{w}_1 \widehat{x}_2 \leq \widehat{w}_1 x_2 \leq \frac{1}{2}, \end{cases} \\ d_2^G(x, w, \widehat{x}, \widehat{w}) &= -\widehat{x}_3 - 3, \\ d_3^G(x, w, \widehat{x}, \widehat{w}) &= -\widehat{x}_1 + x_2 + w_1^3. \end{aligned} \tag{4.19}$$

An under-approximation of $R(\frac{1}{2}; A)$ is computed by simulating the system (4.11), here taken relative to d^G, forward in time for $t = \frac{1}{2}$ time-units. The reachable set approximations generated in this study are depicted in Figure 4.3. ■

4.1.3 Summary

In this section, we attempt to summarise our previous results through a cohesive theory as to how reachable sets can be efficiently over- and under-approximated for mixed monotone systems using a single decomposition function for the forward-time dynamics. In particular, we observe that when a forward-time system (2.1) is mixed monotone with respect to $d^F(x, w, \widehat{x}, \widehat{w})$, we also have that[1]:

- A simulation of the $2n$-dimensional deterministic system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E^F(x, \widehat{x}) = \begin{bmatrix} d^F(x, \underline{w}, \widehat{x}_{[i:x]}, \overline{w}) \\ d^F(\widehat{x}, \overline{w}, x_{[i:\widehat{x}]}, \underline{w}) \end{bmatrix} \tag{4.20}$$

  allows for computing *over-approximations* of *forward-time* reachable sets.

- A simulation of the $2n$-dimensional deterministic system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E^{-F}(x, \widehat{x}) = \begin{bmatrix} -d^F(\widehat{x}_{[i:x]}, \overline{w}, x, \underline{w}) \\ -d^F(x_{[i:\widehat{x}]}, \underline{w}, \widehat{x}, \overline{w}) \end{bmatrix} \tag{4.21}$$

  allows for computing *over-approximations* of *backward-time* reachable sets.

- A simulation of the $2n$-dimensional deterministic system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = -E^{-F}(x, \widehat{x}) = \begin{bmatrix} d^F(\widehat{x}_{[i:x]}, \overline{w}, x, \underline{w}) \\ d^F(x_{[i:\widehat{x}]}, \underline{w}, \widehat{x}, \overline{w}) \end{bmatrix} \tag{4.22}$$

[1] We abuse notation slightly in (4.20)–(4.23), where we use, for example, $d^F(x, \underline{w}, \widehat{x}_{[i:x]}, \overline{w})$ to denote the n-dimensional vector valued function whose i^{th} element is defined by $d^F_i(x, \underline{w}, \widehat{x}_{[i:x]}, \overline{w})$.

allows for computing *under-approximations* of *forward-time* reachable sets.

- A simulation of the $2n$-dimensional deterministic system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = -E^F(x, \widehat{x}) = \begin{bmatrix} -d^F(x, \underline{w}, \widehat{x}_{[i:x]}, \overline{w}) \\ -d^F(\widehat{x}, \overline{w}, x_{[i:\widehat{x}]}, \underline{w}) \end{bmatrix} \tag{4.23}$$

allows for computing *under-approximations* of *backward-time* reachable sets.

In this way, separating a system's vector field into increasing and decreasing components, through the explicit computation of a closed-form decomposition function, facilitates many different reachability analysis tools. Moreover, one can attain the tightest approximation of reachable sets, in all cases, when the initial decomposition function d^F is tight. In the next section, we study additional tools arising from forward- and backward-time decomposition functions where we present an explicit approach for computing robustly forward invariant sets for mixed monotone systems.

4.2 Computing Robustly Forward Invariant Sets for Mixed Monotone System

We show in this section how robustly forward invariant sets for mixed monotone systems can be efficiently identified from invariant sets for the embedding system (2.34).

Our approach involves viewing the state transition map of the embedding system (2.34) as a *reachability operator* for the initial system (2.1): indeed, when $t \geq 0$ is fixed and $[\![a]\!]$ viewed as an input, the set-valued map $[\![\Phi^E(t; a)]\!]$ evaluates to a hyperrectangle that contains $R(t; [\![a]\!])$. Building on this intuition, we observe that *invariant regions in the embedding space* correspond invariant regions for the initial system (2.1), and we consider two main kinds of invariant sets for the embedding system:

- *equilibria* for the embedding system, which are trivially invariant and which can be used to identify hyperrectangular invariant sets for the initial system, and

- *closed periodic orbits* for the embedding system, which can be used to identify invariant sets for the initial system with more complex geometries.

Indeed, invariant sets can be thought of as the fixed point of a reachability operator as discussed in Section 2.1, and we further explore how stability analysis in the embedding space can be used to reason about, *e.g.*, the *attractivity* of the forward invariant sets derived using this approach.

4.2.1 Computing Invariant Sets via Stability Analysis in the Embedding Space

Our first result is to show how *equilibria* for the deterministic embedding system (2.34) can be used to identify robustly forward invariant sets for the inital mixed monotone system (2.1). Indeed, unlike the symmetric embedding system (2.28), which is nondeterministic with a $2m$-dimensional input, the deterministic embedding system (2.34) can induce stable, or even globally stable equilibria, in its upper triangular set, and we show also how stability analysis in the embedding space allows one to reason about the existence for *attractive* sets for the inital system, as well.

Definition 11. A set $A \subset \mathcal{X}$ is *attractive from* $B \subset \mathcal{X}$, or simply *attractive* for (2.1), if for each solution $\phi(\,\cdot\,; x, \mathbf{w})$ to (2.1) with $x \in B$ and piecewise continuous $\mathbf{w}$ and each relatively open neighborhood $A_\epsilon \subset \mathcal{X}$ of A, there exists $\tau > 0$ such that $\phi(t; x, \mathbf{w}) \in A_\epsilon$ for all $t \geq \tau$. When $B = \mathcal{X}$, we say A is *globally attractive*. ■

We first recall from Lemma 2 that the set of embedding system states whose vector-field points into the southeast cone,

$$\mathcal{S} := \{(x, \widehat{x}) \in \mathcal{T} \,|\, 0 \preceq_{\mathrm{SE}} E(x, \widehat{x})\}. \tag{4.24}$$

is a forward invariant set for the embedding system (2.34). To interpret this result, observe that when $a \in \mathcal{S} \subseteq \mathcal{T}$,

$$a \preceq_{\mathrm{SE}} \Phi^E(t; a) \tag{4.25}$$

holds for all $t \geq 0$, since it is true that $\mathcal{S}$ is forward invariant and therefore $0 \preceq_{\mathrm{SE}} E(\underline{x}(t), \overline{x}(t))$ for all time, where $(\underline{x}(t), \overline{x}(t)) := \Phi^E(t; a)$. Now from (2.15), we have

$$[\![\Phi^E(t; a)]\!] \subseteq [\![a]\!], \tag{4.26}$$

i.e., the time-t reachable set of (2.1) from $[\![a]\!]$ will be contained inside $[\![a]\!]$ for all $t \geq 0$. Thus, $[\![a]\!] \subset \mathcal{X}$ is a robustly forward invariant set for (2.1) and, in this way, knowledge of a single embedding state $a \in \mathcal{S}$ immediately identifies a robustly forward invariant set $[\![a]\!] \subset \mathcal{X}$ for the initial system. We formalize this observation in the following Theorem where we show hyperrectangular robustly forward invariant sets for mixed monotone systems are identified using embedding states in $\mathcal{S}$.

Theorem 3. *Suppose* (2.1) *is mixed monotone with respect to* d. *Then for all* $a \in \mathcal{S}$ *the following hold:*

1. *For all* $t \geq 0$*, the set* $[\![\Phi^E(t; a)]\!] \subseteq \mathcal{X}$ *is robustly forward invariant for* (2.1).

2. $\lim_{t\to\infty} \Phi^E(t; a) =: (x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}})$ *exists and* $e(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) = 0$*, i.e.,* $(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}})$ *is an equilibrium for* (2.34).

3. *The set* $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ *is robustly forward invariant and attractive from* $[\![a]\!] \subseteq \mathcal{X}$*.* ■

Proof. Part 1. Suppose $\mathcal{S}$ is nonempty, and choose $a \in \mathcal{S}$. Then, from Lemma 2, $\Phi^E(t; a) \in \mathcal{S}$ for all $t \geq 0$. Choose $\tau \geq 0$ and let $b = \Phi^E(\tau; a) \in \mathcal{S}$. Also from Lemma 2, $b \preceq_{\mathrm{SE}} \Phi^E(t; b)$ so that $[\![\Phi^E(t; b)]\!] \subseteq [\![b]\!]$ by (2.15) for all $t \geq 0$. From Proposition 2 we have $R(t; [\![b]\!]) \subseteq [\![\Phi^E(t; b)]\!]$. Therefore $R(t; [\![b]\!]) \subseteq [\![b]\!]$ for all $t \geq 0$, *i.e.*, $[\![b]\!]$ is robustly forward invariant for (2.1). This completes the proof of the first part since $\tau \geq 0$ was arbitrary.

Part 2. This result follows from [78, Theorem 2.1] applied to the monotone embedding system. In particular, since $a \preceq_{\mathrm{SE}} \Phi^E(t; a)$ for all $t \geq 0$, and $\mathcal{T}$ is forward invariant for (2.34), we have

$$\Phi^E(t; a) \in \{(\underline{y}, \overline{y}) \in \mathcal{X} \times \mathcal{X} \mid \underline{x} \preceq \underline{y} \preceq \overline{y} \preceq \overline{x}\} \tag{4.27}$$

for all $t \geq 0$, when $a = (\underline{x}, \overline{x})$. Since $\Phi^E(t; a)$ is increasing with respect to the southeast order and is bounded, $\lim_{t\to\infty} \Phi^E(t; a) := (x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}})$ exists and $E(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) = 0$.

Part 3. Choose $x \in [\![a]\!]$ and $\mathbf{w} : [0, \infty] \to \mathcal{W}$. Then

$$(\phi(t; x, \mathbf{w}), \phi(t; x, \mathbf{w})) = \Phi^{\varepsilon}(t; (x, x), (\mathbf{w}, \mathbf{w}))$$

and

$$\Phi^E(t;a) = \Phi^\varepsilon(t;a,(\underline{w},\overline{w}))$$

hold for all $t \geq 0$. Since $a \preceq_{\mathrm{SE}} (x,x)$ and $(\underline{w},\overline{w}) \preceq_{\mathrm{SE}} (\mathbf{w}(t),\mathbf{w}(t))$ for all $t \geq 0$, we now have $\phi(t;x,\mathbf{w}) \in [\![\Phi^E(t;a)]\!]$ for all $t \geq 0$. Choose a relatively open neighborhood $\mathcal{X}_\epsilon$ of $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ and a relatively open ball $B \subset \mathcal{X} \times \mathcal{X}$ such that $(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) \in B \subset \mathcal{X}_\epsilon \times \mathcal{X}_\epsilon$. From Part 2, there must exist a $\tau \geq 0$ such that $\Phi^E(\tau;a) \in B$ and at this time $\phi(\tau;x,\mathbf{w}) \in \mathcal{X}_\epsilon$. From Part 1 we have that $[\![\Phi^E(\tau;a)]\!]$ is robustly forward invariant for (2.1) and therefore $\phi(t;x,\mathbf{w}) \in \mathcal{X}_\epsilon$ for all $t \geq \tau$. Therefore, $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ is attractive on (2.1) from $[\![a]\!]$. The fact that $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ is robustly forward invariant follows immediately from Part 1. $\square$

Theorem 3 provides a basic algorithm for identifying invariant sets; if (2.34) has an *equilibrium*, *i.e.*, there exists an $(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) \in \mathcal{T}$ such that $E(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) = 0$, then

$$A_{\mathrm{eq}} := [x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}] \tag{4.28}$$

is robustly forward invariant for (2.1). Computing equilibria for (2.34) requires one to solve a system of $2n$ nonlinear equations and, therefore, does not require excessive computation. Moreover, if a point $a \in \mathcal{S}$ is known, then one can simulate the embedding dynamics forward in time, starting from a, in order to identify an equilibrium; see Theorem 3 Part 2.

Remark 8. Very few techniques exist for *explicitly computing* robustly forward invariant sets, given a dynamical system. For example, one may consider comparing the results of Theorem 3, to the more traditional barrier function based approach for identifying forward invariant sets [57, 79, 80]. Employing traditional barrier-based reasoning involves (i) choosing a candidate subset of states and then (ii) ensuring that the system's vector field always points inward along the subset's boundary, as to verify forward invariance using a Nagumo-type argument [81, 82]. For this reason, barrier function are most naturally employed in the setting of controlled dynamical systems, without disturbances, as to increase the likelihood that the subset of interest is forward invariant under some, perhaps unknown, control policy.

A main difference of our approach is that, in general, a candidate subset need not be chosen *a priori* when employing the results of Theorem 3. Indeed, employing Theorem 3 requires only solving a system of $2n$ algebraic equations—finding an equilibrium to the embedding system—in order to identify a robustly forward invariant set. We show later in Proposition 9 that a hyperrectangular forward invariant set for (2.1) exists only when this system of algebraic equations has a solution. See also [49] for further connections and comparisons between the results of Theorem 3 and traditional barrier-based reasoning. ■

In the remainder of this section, we provide several related methods and generalizations for computing robustly forward invariant sets for mixed monotone systems. Before moving further, however, we demonstrate the application of Theorem 3 though an example.

Example 17. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x,w) = \begin{bmatrix} -x_1^3 - x_2 - w \\ x_1^2 - x_2 + w^3 \end{bmatrix} \tag{4.29}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W} = [-1, 1]$. The system (4.29) is mixed monotone and the tight decomposition function for (4.29) is given element-wise by

$$\begin{aligned} d_1(x,w,\widehat{x},\widehat{w}) &= -x_1^3 - \widehat{x}_2 - \widehat{w}, \\ d_2(x,w,\widehat{x},\widehat{w}) &= \begin{cases} x_1^2 - x_2 + w^3 & \text{if } x_1 \geq \max\{0, -\widehat{x}_1\}, \\ \widehat{x}_1^2 - x_2 + w^3 & \text{if } \widehat{x}_1 \leq \min\{0, -x_1\}, \\ -x_2 + w^3 & \text{if } x_1 \leq 0 \leq \widehat{x}_1. \end{cases} \end{aligned} \tag{4.30}$$

To compute a robustly forward invariant set for (4.29), we compute an equilibrium for the

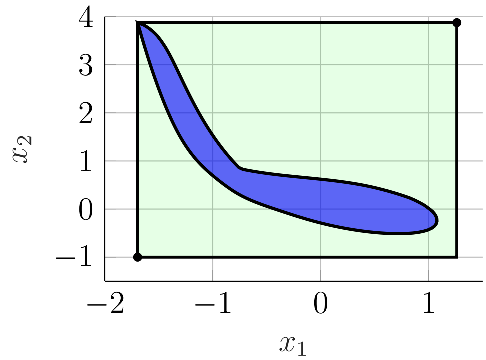


Figure 4.4: Example 15: Computing robustly forward invariant and attractive sets for (4.29) by applying Theorem 2. The green rectangle is A_{eq} from (4.31), which is robustly forward invariant and globally attractive for (4.29). The region shown in blue is globally attractive for (4.29), and no proper subset of this region is robustly forward invariant.

embedding system (2.34): we find, $E(x_{\text{eq}}, \widehat{x}_{\text{eq}}) = 0$ for

$$x_{\text{eq}} = (-1.70, -1.00), \qquad \widehat{x}_{\text{eq}} = (1.26, 3.88), \tag{4.31}$$

and $(x_{\text{eq}}, \widehat{x}_{\text{eq}}) \in \mathcal{T}$ and, therefore, from Theorem 3, we have that $A_{\text{eq}} = [x_{\text{eq}}, \widehat{x}_{\text{eq}}]$ is a robustly forward invariant set for (4.29). Furthermore, the equilibrium $(x_{\text{eq}}, \widehat{x}_{\text{eq}})$ is globally asymptotically stable for (2.34) and, therefore, the set A_{eq} is also globally attractive for (4.29). Simulation results in this study are provided in Figure 4.4. ■

We next extend Theorem 3 to leverage the backward-time dynamics (4.2). Specifically, we show that if (4.2) is mixed monotone then robustly forward invariant sets for (2.1) can be computed using a technique analogous to Theorem 3.

Theorem 4. *Let* (4.2) *be mixed monotone with respect to* d^G. *If there exists* $(\underline{x}, \overline{x}) \in \mathcal{T}$ *so that* $0 \preceq_{\text{SE}} E^G(\underline{x}, \overline{x})$ *then* $\mathcal{X} \setminus [\underline{x}, \overline{x}]$ *is robustly forward invariant for* (2.1)*, where* E^G *is the embedding function constructed from* d^G *as in* (2.34). ■

Proof. If $0 \preceq_{\text{SE}} E^G(\underline{x}, \overline{x})$ holds for $(\underline{x}, \overline{x}) \in \mathcal{T}$ then from Theorem 3 we have that $[\underline{x}, \overline{x}]$ is robustly forward invariant for (4.2). Thus, $\mathcal{X} \setminus [\underline{x}, \overline{x}]$ is robustly forward invariant for (2.1). This completes the proof. □

A second example is provided below where we now compute robustly forward invariant regions for a mixed monotone system by applying Theorems 3 and 4.

Example 18. We consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x,w) = \begin{bmatrix} -x_2 + x_1(4 - 4x_1^2 - x_2^2) + w_1 \\ x_1 + x_2(4 - x_1^2 - 4x_2^2) + w_2 \end{bmatrix} \tag{4.32}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W} = [-\frac{3}{4}, \frac{3}{4}]^2$. A tight decomposition function is formed for (4.32), and a globally asymptotically stable equilibrium for (2.34) is identified using Theorem 3 Part 2. In particular, we find $E(x_{\text{eq}}, \widehat{x}_{\text{eq}}) = 0$ for

$$x_{\text{eq}} = (-1.1, -1.1), \qquad \widehat{x}_{\text{eq}} = (1.1, 1.1), \tag{4.33}$$

and, therefore, the hyperrectangle $A_{\text{eq}} := [x_{\text{eq}}, \widehat{x}_{\text{eq}}]$ is robustly forward invariant and globally attractive for (4.32).

Next, a tight decomposition function for the backward-time dynamics (4.2) is formed and $E^G(y_{\text{eq}}, \widehat{y}_{\text{eq}}) = 0$ for

$$y_{\text{eq}} = (-0.59, -0.59), \qquad \widehat{y}_{\text{eq}} = (0.59, 0.59), \tag{4.34}$$

where E^G denotes the embedding function of the backward-time dynamics as prescribed in Theorem 4. Thus, the set $\mathcal{X} \setminus B_{\text{eq}}$ is robustly forward invariant for (4.32), where $B_{\text{eq}} := [y_{\text{eq}}, \widehat{y}_{\text{eq}}]$. Simulation results in this study are provided in Figure 4.5. ■

4.2.2 Discussion

In Section 4.2.3 of this chapter, we extend the basic theory laid out in Section 4.2.1, and we show how in robustly forward invariant sets for mixed monotone system can be identified from invariant regions for the embedding system with more complex geometries, such as, *e.g.*, periodic orbits

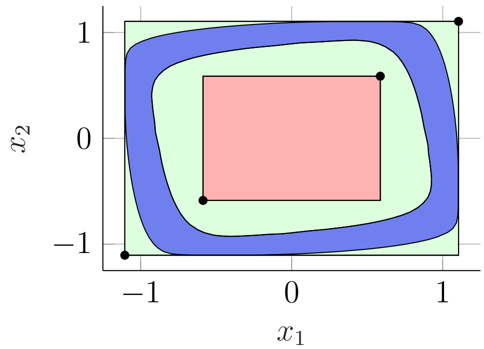


Figure 4.5: Example 18: Computing robustly forward invariant and attractive sets for (4.32) by applying Theorems 3 and 4. A_{eq} is the larger green rectangle which is robustly forward invariant and globally attractive for (4.32). B_{eq} is the smaller red rectangle, and the compliment $\mathbb{R}^2 \setminus B_{\mathrm{eq}}$ is robustly forward invariant for (4.32). The region shown in blue is attractive for (4.32), and no proper subset of this region is robustly forward invariant.

for the embedding system. Before this study, we present a brief discussion on the results previous section, which deal specifically with computing invariant sets via the identification of equilibria for (2.34).

Observe that Theorem 3 provides a sufficient condition for the existence of robustly forward invariant sets for (2.1): given a state $(x, \widehat{x}) \in \mathcal{S}$, where $\mathcal{S}$ is computed from the embedding system according to (2.38), the hyperrectangular set $[x, \widehat{x}] \subseteq \mathcal{X}$ is robustly forward invariant for (2.1). Note, however, that the set $\mathcal{S}$ from (2.38) is dependent on the choice of decomposition function for (2.1) via the embedding dynamics (2.34), and certain decomposition functions will lead to more restrictive invariant sets than others. Thus, even when $(x, \widehat{x}) \notin \mathcal{S}$, the hyperrectangular set $[x, \widehat{x}] \subseteq \mathcal{X}$ may still be forward invariant for (2.1). To address this point, we next present a necessary condition for the existence of robustly forward invariant sets for (2.1) [36].

Proposition 9. *Suppose* (2.1) *is mixed monotone with a tight decomposition function* d *satisfying* (3.45). *Then the hyperrectangular set* $[\underline{x}, \overline{x}] \subseteq \mathcal{X}$ *is robustly forward invariant for* (2.1) *if and only if* $(\underline{x}, \overline{x}) \in \mathcal{S}$, *where* $\mathcal{S}$ *is given in* (2.38) *with* E *obtained from the tight decomposition function* d. ■

Proof. (if) It follows from Theorem 3 that $[\underline{x}, \overline{x}] \subseteq \mathcal{X}$ is robustly forward invariant for (2.1) whenever $(\underline{x}, \overline{x}) \in \mathcal{S}$.

(only if) Assume there exists a $(\underline{x}, \overline{x}) \in \mathcal{T}$ so that $[\underline{x}, \overline{x}] \subseteq \mathcal{X}$ is robustly forward invariant for (2.1). Then

$$\max_{\substack{y \in [\underline{x}, \overline{x}] \\ y_i = \overline{x}_i \\ z \in [w, \widehat{w}]}} F_i(y, z) \leq 0 \leq \min_{\substack{y \in [\underline{x}, \overline{x}] \\ y_i = \underline{x}_i \\ z \in [w, \widehat{w}]}} F_i(y, z) \tag{4.35}$$

must hold for all $i \in \{1, \cdots, n\}$. To see this, suppose the first inequality does not hold for some i so that there exists a $y \in [\underline{x}, \overline{x}]$ with $y_i = \underline{x}_i$ and a $z \in \mathcal{W}$ so that $F_i(y, z) > 0$. Then, initializing at y subject to constant disturbance z, the system will leave the forward set $[\underline{x}, \overline{x}]$ for sufficiently short horizon; *i.e.*, $\phi_i(t; y, z) > \overline{x}_i$ so that $\phi(t; y, z) \notin [\underline{x}, \overline{x}]$ for t small enough. A similar argument applies if the second inequality of (4.35) does not hold for some i. Equivalently

$$d(\overline{x}, \overline{w}, \underline{x}, \underline{w}) \preceq 0 \preceq d(\underline{x}, \underline{w}, \overline{x}, \overline{w}), \tag{4.36}$$

where d is the tight decomposition for (2.1) as defined by (3.45), *i.e.*, $(\underline{x}, \overline{x}) \in \mathcal{S}$. Therefore $[\underline{x}, \overline{x}] \subseteq \mathcal{X}$ is robustly forward invariant for (2.1) if and only if $(\underline{x}, \overline{x}) \in \mathcal{S}$. $\square$

As a final consideration, we discuss *how* and *where* equilibria appear in the embedding space. Observe that when the inital system (2.1) is *deterministic*, so that, *e.g.*, $\underline{w} = \overline{w}$, the embedding system (2.34) obeys the symmetry property (2.30); in the case, if $E(x_{\text{eq}}, \widehat{x}_{\text{eq}}) = 0$ then we also have $E(\widehat{x}_{\text{eq}}, x_{\text{eq}}) = 0$, as well. For this reason, it is generally not possible to obtain *globally stable* equilibria for the embedding system when $\underline{w} = \overline{w}$, unless $x_{\text{eq}} = \widehat{x}_{\text{eq}}$, *i.e.*, the equilibrium appears on the diagonal space $(x_{\text{eq}}, \widehat{x}_{\text{eq}}) \in \Delta$. Moreover, when applying Theorem 3, it is generally only possible to obtain *globally attractive* regions for the inital system (2.1) in the instance where $\underline{w} \neq \overline{w}$. Nonetheless, we show show in the following corollary how globally attractive regions for (2.1) are identified using stability analysis in the embedding space.

Corollary 1. Suppose (2.1) is mixed monotone with respect to d. If $a \in \mathcal{T}$ is an asymptotically stable equilibrium for (2.34) with a basin of attraction $\mathcal{C} \subseteq \mathcal{X} \times \mathcal{X}$, then $[\![a]\!]$ is robustly forward invariant for (2.1) and attractive from all $[\![b]\!]$ such that $b \in \mathcal{C} \cap \mathcal{T}$. In particular, if $\mathcal{C} \supseteq \mathcal{T}$, then $[\![a]\!]$ is globally attractive and robustly forward invariant for (2.1). $\blacksquare$

Observe that the hypothesis of Corollary 1 will be satisfied only when either $\underline{w} \neq \overline{w}$ or $a_{\text{eq}} \in \Delta$. Furthermore, even in the instance where $\underline{w} \neq \overline{w}$ it can be possible for (2.34) to induce equilibria $E(x_{\text{eq}}, \widehat{x}_{\text{eq}}) = 0$ with $\widehat{x}_{\text{eq}} \preceq x_{\text{eq}}$, so that $(x_{\text{eq}}, \widehat{x}_{\text{eq}}) \notin \mathcal{T}$. In this instance, the equilibrium $(x_{\text{eq}}, \widehat{x}_{\text{eq}})$ cannot be used to reason about robustly forward invariant sets for the inital system since, *e.g.*, $[x_{\text{eq}}, \widehat{x}_{\text{eq}}] = \varnothing$ is not a valid hyperrectangle. Nonetheless, unordered equilibria can sometimes be used to reason about mixed monotone reachable set over-approximations, and we demonstrate this assertion through an example below:

Example 19. Recall from Example 4, that any linear time-invariant system $\dot{x} = Ax + Bw$ is mixed monotone with respect to $d(x, w, \widehat{x}, \widehat{w}) = A^{\text{M}+}x + A^{\text{M}-}\widehat{x} + B^{+}w + B^{-}\widehat{w}$, and that the corresponding embedding system is given by

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E^{\text{LTI}}(x, \widehat{x}) = \overline{A} \begin{bmatrix} x \\ \widehat{x} \end{bmatrix} + \overline{B} \begin{bmatrix} \underline{w} \\ \overline{w} \end{bmatrix} \tag{4.37}$$

$$\overline{A} := \begin{bmatrix} A^{\text{M}+} & A^{\text{M}-} \\ A^{\text{M}-} & A^{\text{M}+} \end{bmatrix} \quad \text{and} \quad \overline{B} := \begin{bmatrix} B^{+} & B^{-} \\ B^{-} & B^{+} \end{bmatrix}$$

As such, when $\overline{A} \in \mathbb{R}^{2n \times 2n}$ is an invertible matrix, the embedding system (4.37) always induces a unique equilibrium $E^{\text{LTI}}(x_{\text{eq}}, \widehat{x}_{\text{eq}}) = 0$ given by

$$\begin{bmatrix} x_{\text{eq}} \\ \widehat{x}_{\text{eq}} \end{bmatrix} = -(\overline{A})^{-1}\overline{B} \begin{bmatrix} \underline{w} \\ \overline{w} \end{bmatrix}. \tag{4.38}$$

Nonetheless, this equilibrium only ever identifies a forward invariant set in the specific instance where $x_{\text{eq}} \preceq \widehat{x}_{\text{eq}}$, so that, *e.g.*, $[x_{\text{eq}}, \widehat{x}_{\text{eq}}] \subseteq \mathcal{X}$ is a valid hyperrectangular subset of states.

To demonstrate a case where this condition may not hold, consider, for example, the 2-dimensional linear time-invariant system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} -2 & -1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \end{bmatrix} w \tag{4.39}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W} = [\underline{w}, \overline{w}] = [1, 2]$. The embedding system (4.37) induces an equilibrium $E^{\mathrm{LTI}}(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) = 0$ at state

$$x_{\mathrm{eq}} = \begin{bmatrix} 0.4 \\ 0.8 \end{bmatrix}, \qquad \widehat{x}_{\mathrm{eq}} = \begin{bmatrix} 0.6 \\ 0.2 \end{bmatrix}, \tag{4.40}$$

as prescribed in (4.38), however, $x_{\mathrm{eq}} \not\preceq \widehat{x}_{\mathrm{eq}}$, and thus $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ is not a robustly forward invariant set for (4.39). Nonetheless, the existence of an equilibrium *does* allow one to reason about certain system properties other than, *e.g.*, the existence of forward invariant sets for (4.39).

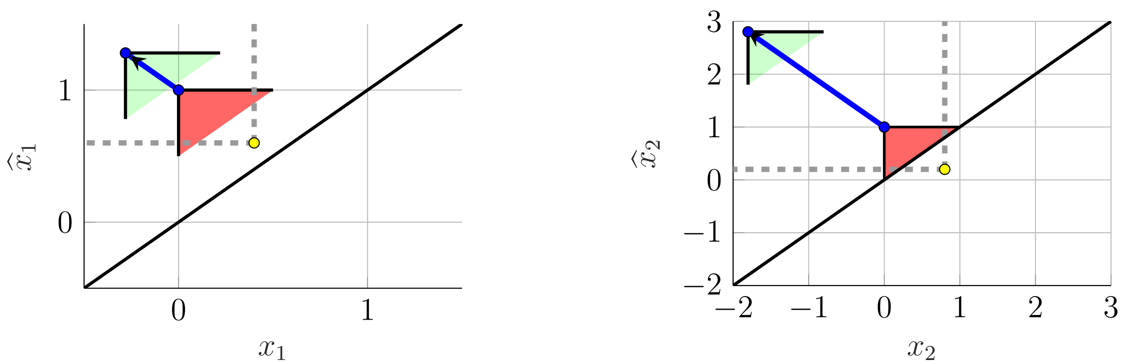
As an example, consider applying the reachability analysis given by Proposition 2 in order to over-approximate $R(t; [\![a]\!])$, the time-t forward reachable set of (4.39) from some inital set $[\![a]\!] \subseteq \mathcal{X}$. In the case where $a \preceq_{\mathrm{SE}} (x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}})$ observe that

$$\Phi^E(t; a) \preceq_{\mathrm{SE}} (x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) \tag{4.41}$$

for all time $t \geq 0$, where (4.41) follows from the monotonicity of the embedding system and holds, despite the fact that $(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) \notin \mathcal{T}$. One now can determine that, when applying the reachability analysis procedure in Proposition 2, the upper and lower reachable set bounds $(\underline{x}(t), \overline{x}(t)) := \Phi^E(t; a)$ are such that

$$\underline{x}(t) \preceq \begin{bmatrix} 0.4 \\ 0.8 \end{bmatrix} \quad \text{and} \quad \overline{x}(t) \succeq \begin{bmatrix} 0.6 \\ 0.2 \end{bmatrix}, \tag{4.42}$$

i.e., the *lower-bound* on $R(t; [\![a]\!])$ produced from the application of Proposition 2 will always be bounded-from-above by x_{eq}, and the *upper-bound* on $R(t; [\![a]\!])$ will always be bounded-from-below by $\widehat{x}_{\mathrm{eq}}$. An example is shown in Figure 4.6 where we take an initial set $[\![a]\!] = [0, 1]^2$, so that



(a) (b)

Figure 4.6: Example 19: Implications of embedding system equilibria outside of the upper-triangle $\mathcal{T}$. We consider the linear time-invariant system (4.39), and the respective embedding system (4.37) has an equilibrium $(x_{\text{eq}}, \widehat{x}_{\text{eq}}) \notin \mathcal{T}$. When applying the reachability analysis procedure in Proposition 2, to compute an over-approximation of $R(t; [\![a]\!])$ for $a \preceq_{\text{SE}} (x_{\text{eq}}, \widehat{x}_{\text{eq}})$ we have $\Phi^{E^{\text{LTI}}}(t; a) \preceq_{\text{SE}} (x_{\text{eq}}, \widehat{x}_{\text{eq}})$ holds for all time. As such, the lower-bound on $R(t; [\![a]\!])$ produced from the application of Proposition 2 will always be bounded-from-above by x_{eq}, and the upper-bound on $R(t; [\![a]\!])$ will always be bounded-from-below by $\widehat{x}_{\text{eq}}$. An example is shown in Subfigures (a) and (b), where we over-approximate $R(\frac{1}{2}; [\![a]\!])$ for $[\![a]\!] = [0, 1]^2$. The embedding system trajectory $\Phi^{E^{\text{LTI}}}(t; a)$ is shown in blue, projected onto the x_1–$\widehat{x}_1$ and x_2–$\widehat{x}_2$ planes, respectively. The equilibrium $(x_{\text{eq}}, \widehat{x}_{\text{eq}}) \notin \mathcal{T}$ is shown in yellow, and the northwest cone emanating from $(x_{\text{eq}}, \widehat{x}_{\text{eq}})$ is shown in grey. Since, $a \preceq_{\text{SE}} (x_{\text{eq}}, \widehat{x}_{\text{eq}})$ observe that $\Phi^{E^{\text{LTI}}}(t; a) \preceq_{\text{SE}} (x_{\text{eq}}, \widehat{x}_{\text{eq}})$ holds for all time.

$a \preceq_{\text{SE}} (x_{\text{eq}}, \widehat{x}_{\text{eq}})$, and where we attempt to over-approximate $R(\frac{1}{2}; [\![a]\!])$ using Proposition 2. ■

4.2.3 Computing Invariant Sets from Periodic Orbits in the Embedding Space

We have shown in Sections 4.2.1 and 4.2.2 how equilibria in the embedding space are used to reason about forward invariant sets for mixed monotone systems. Indeed, these results form special case within a more general theory as to how invariant sets can be constructed.

In particular, we observe that any *infinite* simulation of the embedding system can be used to construct a forward invariant set, in the sense that, for all $a \in \mathcal{T}$ the set $\Gamma(a) \subset \mathcal{X}$ defined by

$$\Gamma(a) := \bigcup_{\tau \in [0,\infty]} [\![\Phi^E(\tau; a)]\!] \tag{4.43}$$

is a robustly forward invariant set for the initial system (2.1), since it is true that when $x \in$

$[\![\Phi^E(\tau; a)]\!]$ for some $\tau \geq 0$ we also have $\phi(t; x, \mathbf{w}) \in [\![\Phi^E(\tau + t; a)]\!]$ for all $t \geq 0$ and all $\mathbf{w} : [0, t] \to \mathcal{W}$.

It is generally not possible, however, to apply (4.43) directly in order to arrive at a forward invariant set for (2.1), since it is true that, *e.g.*, the addition of the disturbance input w in (2.1) generally leads to embedding system trajectories that diverge. One approach for applying (4.43) is thus to identify *forward invariant sets in the embedding space*, so that, *e.g.*, that when $\Gamma_{\text{inv}} \subset \mathcal{T}$ is forward invariant for (2.34), the set $\cup_{b\in\Gamma_{\text{inv}}} [\![b]\!] \subset \mathcal{X}$ is a robustly forward invariant set for the initial system (2.1). Indeed, we have shown already how an equilibrium such as $a_{\text{eq}} \in \mathcal{T}$ is used to show that $\Gamma(a_{\text{eq}}) = [\![a_{\text{eq}}]\!]$ is a robustly forward invariant set for the initial system (2.1), and this result holds since $a_{\text{eq}} \in \mathcal{T}$ is trivially invariant with $\Phi^E(t; a_{\text{eq}}) = a_{\text{eq}}$ for all $t \geq 0$.

Building on this intuition, we next present a second method for identifying robustly forward invariant sets for mixed monotone systems, where we now use *closed periodic orbits* for the embedding system (2.34).

Theorem 5. *Assume for some $a \in \mathcal{T}$ there exist a nontrivial periodic solution $\Phi^E(\,\cdot\,; a)$ to* (2.34)*, i.e., there exists a period $\tau_{\text{p}} > 0$ so that $\Phi^E(t + \tau_{\text{p}}; a) = \Phi^E(t; a)$ holds for all $t \geq 0$. Then the set*

$$\Gamma(a, \tau_{\text{p}}) = \bigcup_{\tau\in[0,\tau_{\text{p}}]} [\![\Phi^E(\tau; a)]\!] \tag{4.44}$$

is a robustly forward invariant set for (2.1). ■

Proof. Choose $a \in \mathcal{T}$ and assume there exists a $\tau_{\text{p}} > 0$ so that $\Phi^E(t + \tau_{\text{p}}; a) = \Phi^E(t; a)$ holds for all $t \geq 0$. Define $\Gamma(a, \tau_{\text{p}})$ by (4.44) and choose $x \in \Gamma(a, \tau_{\text{p}})$. Then there exist a $\tau \in [0, \tau_{\text{p}}]$ so that $x \in [\![\Phi^E(\tau; a)]\!]$ or equivalently $\Phi^E(\tau; a) \preceq_{\text{SE}} (x, x)$. Therefore, for all $t \geq 0$

$$R(t; x) \subseteq [\![\Phi^E(t; (x, x))]\!] \subseteq [\![\Phi^E(t + \tau; a)]\!] \subseteq \Gamma(a, \tau_{\text{p}}), \tag{4.45}$$

and, thus, $\Gamma(a, \tau_{\text{p}})$ is robustly forward invariant for (2.1). □

Remark 9. Using analogous reasoning to that provided in Theorem 3 Part 3, it can additionally be shown that if $\{\Phi^E(t;a) \,|\, t \in [0, \tau_\mathrm{p}]\}$ is attractive from $\mathcal{C} \subseteq \mathcal{X} \times \mathcal{X}$ then $\Gamma(a, \tau_\mathrm{p})$ is attractive from all $[\![b]\!]$ such that $b \in \mathcal{C} \cap \mathcal{T}$. ■

In the following example, we demonstrate the application of Theorem 5, where we compute a robustly forward invariant set for 4-dimensional polynomial system via the identification of a closed periodic obit in the embedding space.

Example 20. Consider the 4-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = F(x, w) = \begin{bmatrix} -2x_1 + x_2(1 + x_1) + x_3 + w \\ -x_2 + x_1(1 - x_2) + 0.1 \\ -x_4 \\ x_3 \end{bmatrix} \tag{4.46}$$

with state space $\mathcal{X} = \mathbb{R}^4$ and disturbance space $\mathcal{W} = [-0.1, 0.1]$. The system (4.46) is mixed monotone and the tight decomposition function for (4.46) is given element-wise by

$$\begin{aligned} d_1(x, w, \widehat{x}, \widehat{w}) &= -2x_1 + l_1(x, \widehat{x}) + x_3 + w, \\ d_2(x, w, \widehat{x}, \widehat{w}) &= -x_2 + l_2(x, \widehat{x}) + 0.1, \\ d_3(x, w, \widehat{x}, \widehat{w}) &= -\widehat{x}_4, \\ d_4(x, w, \widehat{x}, \widehat{w}) &= x_3, \end{aligned} \tag{4.47}$$

where

$$\begin{aligned} l_1(x, \widehat{x}) &:= \begin{cases} \min\{x_2(1 + x_1), \widehat{x}_2(1 + x_1)\} & \text{if } x \preceq \widehat{x}, \\ \max\{x_2(1 + x_1), \widehat{x}_2(1 + x_1)\} & \text{if } \widehat{x} \preceq x, \end{cases} \\ l_2(x, \widehat{x}) &:= \begin{cases} \min\{x_1(1 - x_2), \widehat{x}_1(1 - x_2)\} & \text{if } x \preceq \widehat{x}, \\ \max\{x_1(1 - x_2), \widehat{x}_1(1 - x_2))\} & \text{if } \widehat{x} \preceq x. \end{cases} \end{aligned} \tag{4.48}$$

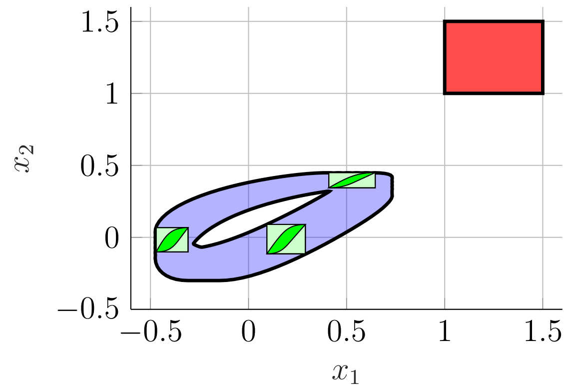


Figure 4.7: Example 20: Computing robustly forward invariant and attractive sets for (4.46) by applying Theorem 5. The robustly forward invariant and attractive set $\Gamma(a, \tau)$ is shown in blue. To demonstrate the attractiveness of $\Gamma(a, \tau)$, we compute reachable sets from $[\![b]\!] = [1, 1.5]^2 \times \{1\} \times \{0\}$ using Proposition 2. $[\![b]\!]$ is shown in red. $R(10, [\![b]\!])$, $R(12, [\![b]\!])$ and $R(14, [\![b]\!])$ are shown in green (left to right), with reachable set over-approximations derived from the application of Proposition 2 shown in light green.

Furthermore, the embedding system (2.34) induces a periodic orbit; we find $\Phi^E(t + \tau; a) = \Phi^E(t; a)$ for

$$a = (-0.03, -0.20, 0.68, -0.75, 0.16, 0.02, 0.68, -0.75) \tag{4.49}$$

and $\tau = 2\pi$. Thus, it follows from Theorem 5 that $\Gamma(a, \tau)$ is robustly forward invariant for (4.46), where $\Gamma(a, \tau)$ is given by (4.44). Moreover, $\{\Phi^E(t; a) \,|\, t \in [0, \tau]\}$ is attractive from

$$\mathcal{C} = \{(x, \widehat{x}) \in \mathcal{T} \,|\, x_3 = \widehat{x}_3, x_4 = \widehat{x}_4, x_3^2 + x_4^2 = 1\} \tag{4.50}$$

and, therefore, $\Gamma(a, \tau)$ is attractive from

$$\{x \in \mathcal{X} \,|\, x_3^2 + x_4^2 = 1\} \subset \mathcal{X}. \tag{4.51}$$

The robustly forward invariant and attractive set $\Gamma(a, \tau)$ derived in this study is shown graphically in Figure 4.7.

■

4.3 Conclusion

In this chapter we show how the decomposition function of a mixed monotone system is used to study complex system properties beyond simple forward-time reachability. In particular, we consider both forward- and backward-time reachability analysis problems, and we show how knowledge of a single decomposition function for the forward-time dynamics allows for both over- and under-approximating reachable sets in these settings. Furthermore, we present several efficient and intuitive techniques for computing robustly forward invariant sets for mixed monotone systems.

In the next chapter, we study reachability and invariance in a similar way, however, our approach is to consider, instead, the mixed monotonicity of a related set of *transformed* system dynamics. Applying mixed monotonicity via the transformed dynamics requires, now, computing a separate, second, decomposition function, and thus requires a second application of the decomposition function construction procedure laid out in Chapter 3. Nonetheless, we show how applying mixed monotonicity via the transformed dynamics enables many practical benefits in systems analysis; for example, transformations can sometimes be used to produce higher fidelity reachable set approximations than those that are attainable from the tight decomposition function for the initial dynamics with no transformation.

4.4 Exercises

Problem 4.1: Consider $\dot{x} = F(x, w)$ and suppose, for all i, the i^{th} entry F_i of the vector field does not depend on x_i. Let d^F be a tight decomposition function for $\dot{x} = F(x, w)$. First, compute the tight decomposition function for the backward-time dynamics $\dot{x} = -F(x, w)$. Now consider the four (embedding) system formulations in Section 4.1.3. What would it mean for *one* of these systems to admit an equilibrium in the upper triangle set $\mathcal{T}$?

CHAPTER 5

REDUCING CONSERVATISM IN MIXED MONOTONE REACHABLE SET APPROXIMATIONS VIA STATE-TRANSFORMATIONS

Given a tight decomposition function for some system, there will not exist another decomposition function for the same system that provides tighter reachable set approximations when used directly with the tools of Chapter 4. However, it is true that a tight decomposition function may be only provide conservative reachable set approximations and it is natural to wonder whether conservatism can be reduced using other means. To that end, in this chapter, we study *how* conservatism enters the reachability analysis procedure, and we present several general methods for reducing conservatism in reachable set approximations that can be applied without compromising the computational efficiency of the mixed monotone approach.

We have discussed already, in Chapters 2 and 3 of this work, certain tools and methodologies for assessing conservatism in mixed monotone reachable set approximations. In Section 2.2, for example, we explore the case of monotone dynamical system, for which the tightest hyperrectangle containing a reachable set can be computed via two simulations of the initial system dynamics. Even in the case of monotone dynamical systems, however, the reachable sets themselves will generally not be hyperrectangles and, for this reason, the tools of Chapter 4 cannot generally be applied to compute reachable sets *exactly*, *i.e.*, without conservatism. One instance where it is possible to compute reachable sets exactly using the theory of (mixed) monotonicity is when a dynamical system is constructed from n decoupled 1-dimensional systems; in this instance, the system's true reachable set a hyperrectangle, for all time, and a tight decomposition function can be used to attain the reachable set without conservatism. Nonetheless, the class of systems for which this approach is applicable is, indeed, very restrictive and in this chapter we focus mainly on the more general class of arbitrary nonlinear systems.

In the case of arbitrary systems, conservatism in mixed monotone reachable set approximations is a main focus of other works, including [43], where the authors show how conservatism can sometimes be reduced by considering mixed monotonicity defined with respect to an alternative partial order on the system's state space. In particular, the authors show how it is sometimes possible to construct a second mixed monotone system, via a *linear transformation* on the statespace of the initial dynamics, and how it is possible to apply the tools of mixed monotonicity to the transformed system in order to attain a *parallelotope* reachable set approximation for the inital (untransformed) dynamics. This approach has also been applied in other works, including [42, 49], in order to attain tighter reachable set approximations using the tools of mixed monotonicity.

In this chapter, we also study how state-transformations can be used to compute higher fidelity reachable set approximations via mixed monotonicity, however, we take a different approach in our analysis. We begin by studying the case where two different mixed monotone systems, with different tight decomposition functions and disturbance spaces, admit the same deterministic embedding system. In this case, the hyperrectangular reachable set approximations will be equal for both systems, for any prediction horizon, even when, *e.g.*, the true reachable set of one system contains that of the other. This analysis aids in the understanding of how conservatism enters the mixed monotone approach, and can be used to suggest whether, for some system, the application of mixed monotone systems theory will produce only overly-conservative reachable set approximations.

Following this discussion, we next apply our observations and develop tools to reduce excess conservatism in mixed monotone reachable set approximations. Motivated by [43], our approach is to apply the tools of mixed monotonicity to a new nondeterministic system, constructed via a state transformation on the inital, untransformed, dynamics. We begin by studying linear transformations on the system state space and we include an extended example where we use linear transformations in order to attain tight reachable set approximations for a 7-dimensional spacecraft system; this example is taken from [42]. Next, we extend to the case of *nonlinear* state-transformations, and we present an example where we use feedback linearization [83], together with mixed monotone systems theory, to attain tight reachable set approximations for a controlled nonlinear pendulum model with disturbances. Third, we study *time-varying transformations* on the system state, which induce a time-varying transformed system, and which are particularly useful for reducing conservatism when the initial (nonlinear) system dynamics contain an isolated linear component. We observe, further, that a time-varying transformation of an n-dimensional system can be thought of as a *state-augmentation* as to create a new $(n+1)$-dimensional system, augmented with time as a state. To that end, as final point of study, we show how it may be possible to augment a system's state vector, with redundant state variables, in order to further reduce conservatism in the approximation of reachable sets. Our approach in this matter is based on the work [68], which studies how state-augmentation can be used to reduce conservatism in interval reachability analysis based techniques.

We structure this chapter in the following way: we present a discussion on conservatism in mixed monotone reachable set approximations in Section 5.1. Our discussion is presented through a series of examples, and we revisit these examples later in the chapter where we show how sometimes conservatism can be reduced by considering an *alternative tight decomposition function* corresponding to a state-transformations of the initial system dynamics. Linear, nonlinear, and time-varying transformations are studied in Sections 5.2 , 5.4 and 5.5, respectively. Furthermore, we present an extended example in Section 5.3, where we consider a 7-dimensional nonlinear spacecraft system and where we demonstrate how a linear transformation on the dynamics allows for tighter reachable set approximations via mixed monotonicity. As a final approach, we show in Section 5.6 how it is sometimes possible to augment the state vector of a nonlinear system, with redundant state variables, in order to further reduce conservatism in the approach.

5.1 Discussion on Conservatism in Mixed Monotone Reachable Set Approximations

In this section, we present a discussion on *how* conservatism enters the reachability analysis procedure, and we focus specifically on the case where a tight decomposition function is used in the application of Proposition 2. Our discussion is presented through a series of examples, and we revisit these examples later in the chapter where we show how it is sometimes possible to attain tighter reachable set approximations by considering an *alternative tight decomposition function* corresponding to a state-transformation of the initial system dynamics in (2.1).

We begin by studying the conditions under which a system's reachable set will be *exactly equal to a hyperrectangle*, since, in this instance, the reachability analysis procedure posited by Proposition 2 can be applied to compute a system's true reachable sets exactly.

Lemma 7. Suppose (2.1) is mixed monotone with a tight decomposition function given by d, and choose a hyperrectangular inital set of states $[\![a]\!] \subset \mathcal{X}$ so that $a \in \mathcal{T}$. If the system's true reachable set $R(t; [\![a]\!])$ is exactly equal to a hyperrectangle for all $t \in [0, \tau]$, then

$$R(t, [\![a]\!]) = [\![\Phi^E(t; a)]\!] \tag{5.1}$$

for all $t \in [0, \tau]$. Equivalently, the reachable set approximation derived via the application of Proposition 2 with a tight decomposition function will be exactly equal to the system's true reachable set, and this is true for any time horizon t. ■

In particular, we observe that the reachable set of (2.1) will be exactly equal to a hyperrectangle if and only if the dynamics of (2.1) are formed from n decoupled scalar-state subsystems, so that the dynamics in (2.1) become

$$\begin{bmatrix} \dot{x}_1 \\ \vdots \\ \dot{x}_n \end{bmatrix} = F(x, w) = \begin{bmatrix} F_1(x_1, w^1) \\ \vdots \\ F_n(x_n, w^n) \end{bmatrix} \tag{5.2}$$

and where $w = (w^1, \cdots, w^n) \in \mathcal{W}_1 \times \cdots \times \mathcal{W}_n \subset \mathbb{R}^m$ is the disturbance.

Lemma 8. The reachable set of (2.1) will be exactly equal to a hyperrectangle if and only if the following hold:

- for all i, F_i does not depend on x_j for all $j \neq i$, and
- for all i, if F_i depends on w_k, then F_j does not depend on w_k. ■

We have already demonstrated the results of Lemmas 7 and 8 earlier in Chapter 3: Example 13, where we compute reachable sets for the simplified unicycle model (3.59). Even though (3.59) is not a monotone system, the application of Proposition 2 with a tight decomposition function produces the system's true reachable set exactly, and this is a result of the fact that (3.59) is a scalar-state system. See also Figure 3.7. Furthermore, we observe that in the setting of (5.2), the first n and last n coordinates of the embedding system trajectory $(\underline{x}(t), \overline{x}(t)) := \Phi^E(t; (\underline{x}_0, \overline{x}_0))$ will each correspond to true system trajectories

$$\underline{x}(t) = \phi(t; \underline{x}_0, \mathbf{w}) \quad \text{and} \quad \overline{x}(t) = \phi(t; \overline{x}_0, \mathbf{w}') \tag{5.3}$$

for some $\mathbf{w}, \mathbf{w}' : [0, t] \to \mathcal{W}$, and this is true even though (5.2) may not be monotone.

Nonetheless, the hypothesis of Lemma 8 poses a fairly restrictive assumption on the vector field or (2.1), and new tools are required to assess the conservatism of mixed monotone reachable set approximations in the more general setting of coupled state-dynamics. In the remainder of this section, we present several examples demonstrating *how* conservatism appears in this setting.

In our first example, we study the case where one or more entry of the state x or disturbance w effects more than one entry of the vector field $F(x, w)$ in (2.1). We show specifically, in this case, how the embedding function of initial system will be equal to the embedding function of a second system with more than m disturbances.

Example 21. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x, w) := \begin{bmatrix} x_2^2 + w \\ x_1 - w \end{bmatrix} \tag{5.4}$$

with state $x = \mathbb{R}^2$ and scalar disturbance $w \in [\underline{w}, \overline{w}] \subset \mathbb{R}$. We are interested in computing an over-approximation of the system's time-t reachable set $R(t; A)$.

As a first example, we apply Proposition 2 with a tight decomposition function d for (5.4) in order to attain a rectangular over-approximation of $R(1; x_0)$, for $x_0 = (1, 1)$ and $\mathcal{W} = [0, 1]$. We denote by E the embedding function of d, and the rectangular reachable set over-approximation $B := [\![\Phi^E(1;(x_0,x_0))]\!] \subset \mathcal{X}$ derived in this study is shown graphically in Figure 5.1. In the setting of this example, we observe that the application of Proposition 2 with d produces a generally conservative over-approximation of $R(1;x_0)$.

As a means of understanding why Proposition 2 may lead to conservative reachable set over-approximations in the setting of (5.4), we consider next a second system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F'(x,w) = \begin{bmatrix} x_2^2 + w_1 \\ x_1 - w_2 \end{bmatrix} \tag{5.5}$$

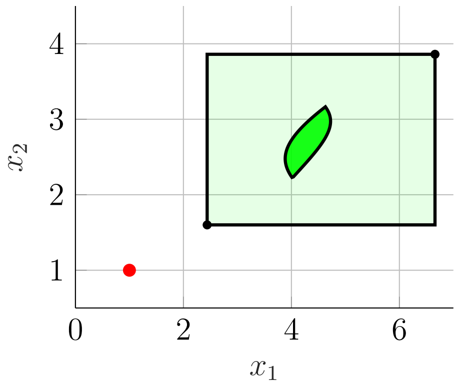
with statespace $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W}' = \mathcal{W} \times \mathcal{W} \subset \mathbb{R}^2$. Since it is true that $F(x,w) = F'(x,(w,w))$ for all $w \in \mathcal{W}$, observe that any trajectory $\phi(t;x,\mathbf{w})$ of (5.4) uniquely identifies a trajectory $\phi'(t;x,(\mathbf{w},\mathbf{w})) := \phi(t;x,\mathbf{w})$ of (5.5), and in this way

$$R(t;A) \subseteq R'(t;A) \tag{5.6}$$

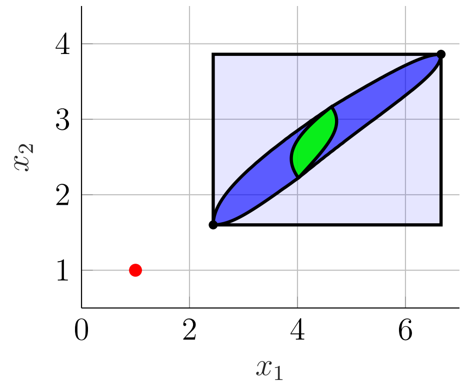
holds always, where $R'(t;A)$ denotes the time-t reachable set of (5.5). To demonstrate this assertion we show also in Figure 5.1 the time-1 reachable set $R'(1;x_0)$ of (5.5) and the rectangular reachable set over-approximation $B' := [\![\Phi^{E'}(1;(x_0,x_0))]\!] \subset \mathcal{X}$ for (5.5) derived via the application of Proposition 2 with a tight decomposition function d' for (5.5).

While it is true that the systems (5.4) and (5.5) admit *different* tight decomposition functions—since, *e.g.*, w is 1-dimensional in (5.4) and 2-dimensional in (5.5)—we observe that d and d' admit the *same* deterministic embedding system (2.34) since it is true that $\mathcal{W}' = [\underline{w}, \overline{w}]^2$; see Remark 3. Stated another way, we observe that $E(x,\widehat{x}) = E'(x,\widehat{x})$ holds always, and therefore $B = B'$, even though d and d' are tight decomposition functions for different systems. Furthermore, since the reachable set of (5.4) is a strict subset of (5.5), we additionally have that

$$R(t;x_0) \subseteq R'(t;x_0) \subseteq B. \tag{5.7}$$



(a)



(b)

Figure 5.1: Example 21: Comparing two reachable set approximations derived from applying Proposition 2 and where the systems of interest are (5.4) and (5.5). Subfigures: (a) Computing reachable sets using a tight decomposition function for (5.4) and where $\mathcal{W} = [0,1]$. The initial state $x_0 = (1,1)$ is shown in red, the time-1 reachable set $R(1;x_0)$ is shown in green, and the rectangular reachable set over-approximation $B \subset \mathbb{R}^2$ is shown in light green. (b) Computing reachable sets using a tight decomposition function for (5.5) and where $\mathcal{W}' = [0,1]^2$. The initial state $x_0 = (1,1)$ is shown in red, the time-1 reachable set $R'(1;x_0)$ is shown in blue, and the rectangular reachable set over-approximation $B' \subset \mathbb{R}^2$ is shown in light blue. While it is true that the systems (5.4) and (5.5) admit different tight decomposition functions, observe that $B = B'$ and this is a result of the fact that decomposition functions are computed elementwise. Furthermore, observe that $R(t;x_0) \subseteq R'(t;x_0) \subset B$ and, for this reason, it can be difficult to attain a tight reachable set approximations for (5.4) when applying Proposition 2 with a tight decomposition function.

For this reason, it can be difficult to attain a tight reachable set approximations for (5.4) when applying Proposition 2 with a tight decomposition function. In particular, we observe that the reachability analysis procedure treats w as though it may take different values in $F_1(x,w)$ and $F_2(x,w)$, and this is a result of the fact that (tight) decomposition functions are computed elementwise; see Lemma 3 and Theorem 1. ■

In Example 21, we show how the tight decomposition function of a mixed monotone system may produce overly-conservative reachable set approximations when some entry of the state x or disturbance w effects more than one entry of the vector field $F(x,w)$ in (2.1). Our approach is to show how, in this instance, the embedding function of the inital mixed monotone system will be equal to the embedding function of a second mixed monotone system with more than m disturbances.

We study the same problem setting in our next example, however, we take a different approach in our analysis. Specifically, we show in Example 22 how, if some entry of the disturbance w effects both entries of the dynamics in (2.1), then it may be possible to extend the disturbance space of (2.1) and attain the same reachable set over-approximation via an application of Proposition 2.

Example 22. Consider the linear time-invariant system

$$\dot{x} = F(x, w) := Ax + Bw \tag{5.8}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W}^{\mathrm{rect}} = [-1, 1] \times [1, 2] \subset \mathbb{R}^2$, and where $A = \left[\begin{smallmatrix} -2 & 1 \\ 1 & -2 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right]$. We are interested in over-approximating reachable sets for (5.8) and, as a first demonstration, we apply Proposition 2 with a tight decomposition function d for (5.8) in order to arrive at a rectangular over-approximation of $R(1; x_0)$ for $x_0 = (2, 1)$. This over-approximation is denoted

$$C^{\mathcal{W}} := [\![\Phi^E(1; (x_0, x_0))]\!] \subset \mathbb{R}^2 \tag{5.9}$$

and we show $C^{\mathcal{W}}$ graphically in Figure 5.2.

We next explore a second, natural, method of computing over-approximations of reachable sets for (5.8): we consider the system

$$\dot{x} = F'(x, v) := Ax + v \tag{5.10}$$

where $x \in \mathcal{X}$ is the state and

$$v \in \mathcal{V}^{\mathrm{par}} := \{Bw \in \mathbb{R}^2 \,|\, w \in \mathcal{W}\} \tag{5.11}$$

is the disturbance. Observe that the reachable set $R'(t; x_0)$ of (5.10) is equal to $R(t; x_0)$, since it is true that each $w \in \mathcal{W}^{\mathrm{rect}}$ identifies a unique $v = Bw \in \mathcal{V}^{\mathrm{par}}$ so that $F(x, w) = F'(x, v)$. While it is true that the disturbance space $\mathcal{V}^{\mathrm{par}}$ of (5.10) is a *parallelogram* in this setting, it is indeed possible to over-approximate $R'(t; x_0)$ by applying Proposition 2 with a *rectangular over-approximation* of the disturbance space

$$\mathcal{V}^{\text{rect}} := [B^+\underline{w} + B^-\overline{w}, B^-\underline{w} + B^+\overline{w}] \supset \mathcal{V}^{\text{par}}. \tag{5.12}$$

To that end, we apply Proposition 2 with a tight decomposition function d' for (5.10) in order to attain a rectangular over-approximation of $R'(1; x_0) = R(1; x_0)$ and this over-approximation is denoted

$$C^{\mathcal{V}} := [\![\Phi^{E'}(1; (x_0, x_0))]\!] \subset \mathbb{R}^2. \tag{5.13}$$

In the setting of this example, we find that $C^{\mathcal{V}} = C^{\mathcal{W}}$ since it is true that $E(x, \widehat{x}) = E'(x, \widehat{x})$. Furthermore, since it is true that $R'(t; x_0) = R(t; x_0)$ for all $v \in \mathcal{V}^{\text{rect}}$, we now have that $R(t; x_0) \subseteq C^{\mathcal{W}}$ for (5.8), and this is true even when the disturbance set of (5.8) is considered to be

$$\mathcal{W}^{\text{par}} = \{w \in \mathbb{R}^2 \,|\, Bw \in \mathcal{V}^{\text{rect}}\}, \tag{5.14}$$

i.e., $\mathcal{W}^{\text{par}} \supset \mathcal{W}^{\text{rect}}$ is a parallelogram. ■

Our previous examples provide a basic theory as to how conservatism enters the reachability analysis procedure, Proposition 2. Our main observations are as follows:

- A tight decomposition function can be applied to compute a system's reachable set, without conservatism, when the initial system dynamics are comprised of n-decoupled scalar-state systems: see Lemmas 7 and 8.

- In the case of coupled state dynamics, the application of Proposition 2 will produce a generally conservative reachable set over-approximation. The hyperrectangular over-approximation derived in this case can sometimes be viewed as

  - a reachable set over-approximation for a *different* system with more than m disturbances, or also

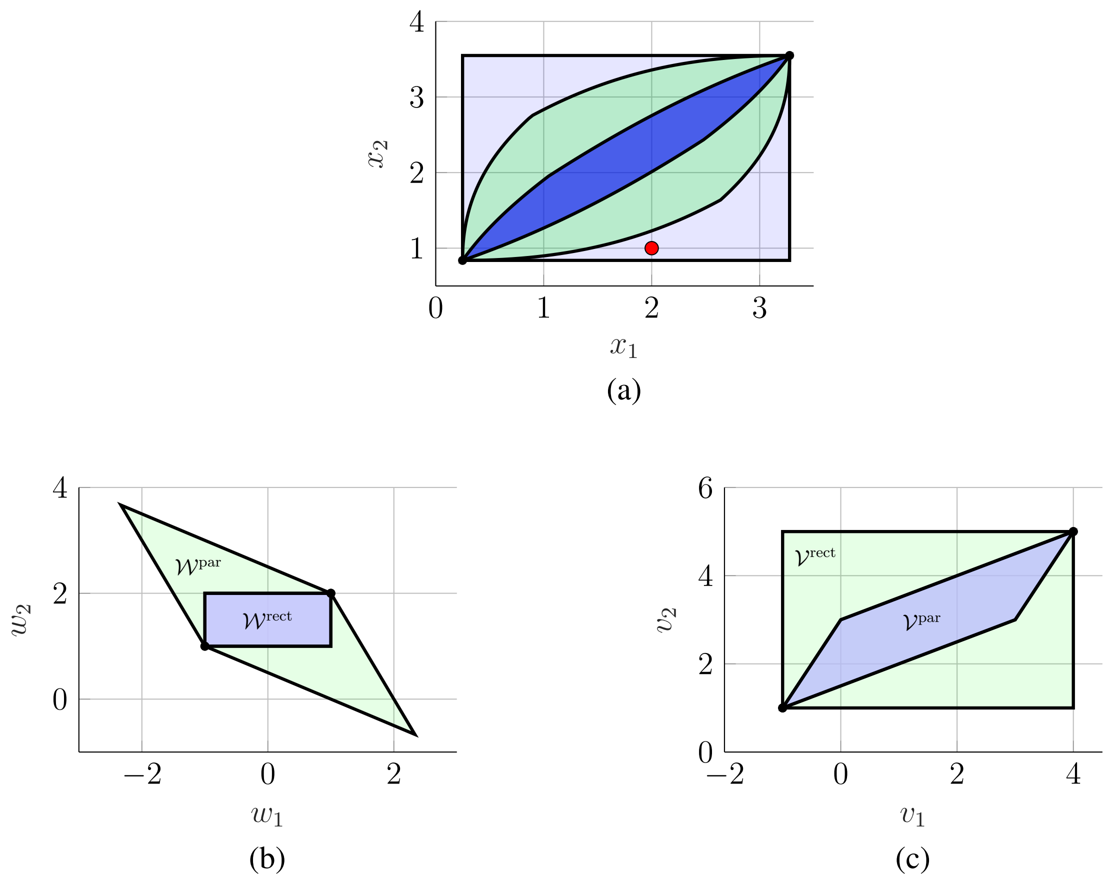


Figure 5.2: Example 22: Comparing reachable sets for (5.8) when the disturbance space is $\mathcal{W}^{\text{rect}}$ and $\mathcal{W}^{\text{par}}$. Subfigures: (a) the inital state $x_0 = (2, 1)$ is shown in red. The time-1 reachable set $R(1; x_0)$ of (5.8) is shown in blue, where $\mathcal{W}^{\text{rect}}$ is the disturbance space. Observe that $R'(1; x_0) = R(1; x_0)$ where $R'(1; x_0)$ denotes the time-1 reachable set (5.10) and where the disturbance space $\mathcal{V}^{\text{par}}$ is a parallelogram. The time-1 reachable set $R(1; x_0)$ of (5.8) is shown in green, where $\mathcal{W}^{\text{par}}$ is the disturbance space. Observe that $R'(1; x_0) = R(1; x_0)$ where $R'(1; x_0)$ denotes the time-1 reachable set (5.10) and where the disturbance space $\mathcal{V}^{\text{rect}}$. The rectangular reachable set approximation $C^{\mathcal{W}} = C^{\mathcal{V}} \supset R(1; x_0)$ is shown in green. (b) The sets $\mathcal{W}^{\text{rect}}$ and $\mathcal{W}^{\text{par}}$ are shown in blue and green respectively. Observe that while it is possible to apply Proposition 2 with a tight decomposition function for (5.8) and show that $R(t; x_0) \subset B$ when the disturbance space is $\mathcal{W}^{\text{rect}}$, we also have $R(t; x_0) \subset B$ when the disturbance space is $\mathcal{W}^{\text{par}}$. (c) The sets $\mathcal{V}^{\text{par}}$ and $\mathcal{V}^{\text{rect}}$ are shown in blue and green respectively.

– a reachable set over-approximation for the *same* system, with an augmented disturbance space.

In the remaining sections of this chapter, we present several general methods for reducing conservatism in mixed monotone reachable set approximations. Our approach is to consider a state-transformation of the initial system dynamics in (2.1), and we show how a decomposition function for the transformed dynamics may be used to approximate reachable sets for the initial untransformed dynamics with reduced conservatism. In particular, such a transformation may be used to reduce coupling within a system's vector field and, in the experience of the authors, it is often possible to transform the initial (nonmonotone) dynamics in (2.1) to monotone dynamics. Numerous examples are provided to demonstrate these assertions.

5.2 Linear Transformations for Parallelotope Reachable Set Approximations with Reduced Conservatism

We consider, first, a *linear transformation* on the state space of (2.1), formed by

$$x := Ty \quad \sim \quad y := T^{-1}x \tag{5.15}$$

where $x \in \mathcal{X}$ is the state of (2.1) and $T \in \mathbb{R}^{n\times n}$ is a nonsingular transformation matrix. Under the transformation (5.15), the dynamics of y become

$$\begin{aligned} \dot{y} &= F_T(y, w) \\ &:= T^{-1}F(Ty, w) \end{aligned} \tag{5.16}$$

where $y \in \mathcal{Y}$ is the state, $w \in \mathcal{W}$ is the disturbance and where F and $\mathcal{W}$ retain their definitions from (2.1). Furthermore, the system (2.1) and (5.16) are related in the following way: for all $x \in \mathcal{X}$, all time $t \geq 0$, and all piecewise continuous $\mathbf{w} : [0, t] \to \mathcal{W}$, we have

$$\phi(t; x, \mathbf{w}) = T\psi(t; T^{-1}x, \mathbf{w}) \tag{5.17}$$

and where we now use ψ to denote the state transition function of (5.16).

Our main observation is that hyperrectangular sets in the state space of (5.16) correspond to *parallelotopes* in the state space of (2.1). Given $(\underline{y}, \overline{y}) \in \mathcal{T}$ and a nonsingular transformation matrix $T \in \mathbb{R}^{n\times n}$, recall that

$$[\underline{y}, \overline{y}]_T := \{x \in \mathcal{X} \mid T^{-1}x \in [\underline{y}, \overline{y}]\} \tag{5.18}$$

denotes the n-dimensional parallelotope defined by the endpoints $\underline{y}$ and $\overline{y}$ and the shape matrix T, and $[\![a]\!]_T := [\underline{y}, \overline{y}]_T$ when $a = (\underline{y}, \overline{y}) \in \mathcal{T}$. Furthermore, observe that when $y \in [\![a]\!]_T$ we also have that $x = Ty \in [\![a]\!]$. In this way, one can apply the reachability analysis procedure given in Proposition 2 to the transformed system (5.16) in order to arrive a parallelotope over-approximation of $R(t; A)$ for (2.1). Our main result is as follows:

Proposition 10 ([43], Theorem 1)**.** *For some nonsingular $T \in \mathbb{R}^{n\times n}$, let* (5.16) *be mixed monotone with respect to d. Choose a parallelotope set of inital conditions $[\![a]\!]_T \subseteq \mathcal{X}$, so that $a \in \mathcal{T}$. Then*

$$R(t; [\![a]\!]_T) \subseteq [\![\Phi^E(t; a)]\!]_T, \tag{5.19}$$

where $R(t; [\![a]\!]_T)$ is the reachable set of the original dynamics (2.1) *as defined in* (2.2) *and Φ^E is the state transition function of the embedding system constructed from d as defined in* (2.34). ■

Before moving to demonstrate the application of Proposition 10, a few remarks are in order:

It is true that Proposition 2 forms a special case of Proposition 10 attained by considering T to be the $n \times n$ identity matrix. Nonetheless, the unique benefit of Proposition 10 becomes apparent when considering transformations other than $T = I$. We show specifically in this section how such transformations may be used to reduced conservatism in reachable set approximations, in comparison to, *e.g.*, applying Proposition 2 with a tight decomposition function for (2.1) in order to attain a hyperrectangular reachable set approximation. Furthermore, this reduction in conservatism is possible even when the initial set of interest is a hyperrectangle.

Indeed, an initial set $A \subset \mathcal{X}$ of any geometry can always be *over-approximated* by a parallelotope with shape matrix T as to make the hypothesis of Proposition 10 applicable. Regardless, to best demonstrate the unique benefit of applying Proposition 10 in this section, we mainly consider the problem of over-approximating a system's reachable set $R(t;x)$ from an *initial state* $x \in \mathcal{X}$.

Remark 10. When attempting to approximate a reachable set $R(t,x)$ from an initial state $x \in \mathcal{X}$, it is always possible to apply Proposition 10 with any transformation and without the need to over-approximate the inital set. This is due to the fact that any singleton set $A = \{x\}$ is trivially a parallelotope with respect to any shape matrix T, since it is true that $A = [T^{-1}x, T^{-1}x]_T \subset \mathcal{X}$ always. ■

We next demonstrate the application of Proposition 10 through example, where we show how considering the mixed monotonicity of the transformed system (5.16) may allow for computing reachable set over-approximations with reduced conservatism in comparison to, *e.g.*, applying Proposition 2 with a tight decomposition function.

Example 23. Consider the 2-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = F(x,w) = \begin{bmatrix} x_1 - 2x_2 + x_2^3 + w \\ x_1 - 2x_2 \end{bmatrix} \tag{5.20}$$

with state space $\mathcal{X} = \mathbb{R}^2$ and disturbance space $\mathcal{W} = [-1,1]$. As a first demonstration, we compute an over-approximation of $R(1;x_0)$ using Proposition 2, *i.e.*, Proposition 10 with $T_1 = I$, where now the inital set is an *initial state* $x_0 = (1,0)$ and where a tight decomposition function for (5.20) is used in the approach. The rectangular reachable set approximation derived in this study is denoted $A_1 \subset \mathcal{X}$ and we show this approximation graphically in Figure 5.3.

Next, we consider a transformation on the statespace of (5.20), $x = T_2 y$ as prescribed in (5.16), where the transformation matrix is taken to be $T_2 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. In this case, the dynamics of y become

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \end{bmatrix} = F_{T_2}(y,w) = \begin{bmatrix} y_2^3 + w \\ y_1 - y_2 \end{bmatrix}, \tag{5.21}$$

with $y \in \mathcal{Y} = \mathbb{R}^2$ and $w \in [-1,1]$ and we observe that (5.21) is a monotone system as defined in Definition 3. As such, one can apply Proposition 10 with the tight decomposition function

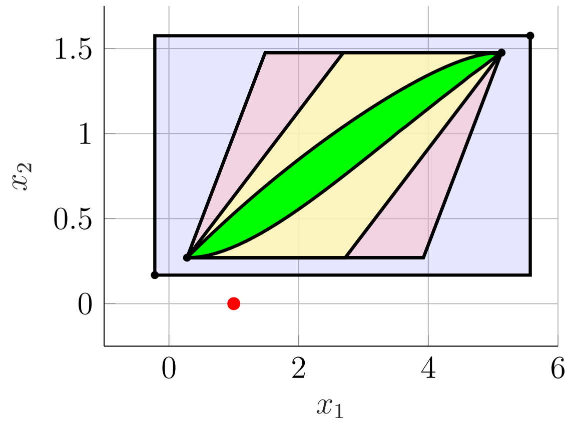


Figure 5.3: Example 23: Computing tight parallelogram reachable set over-approximations for (5.20) by applying Proposition 10. The inital state x is shown in red and the time-1 reachable set $R(1; x)$ is shown in green. We compute three over-approximations of $R(1; x)$ as follows: (i) the rectangular over-approximation A_1 derived from the application of Proposition 2 (Proposition 10 with $T_1 = I$) is shown in blue, (ii) the parallelogram over-approximation A_2 derived from the application of Proposition 10 with $T_2 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ is shown in red, and (ii) the parallelogram over-approximation A_3 derived from the application of Proposition 10 with $T_3 = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ is shown in red. While T_2 induces monotone dynamics (5.16) and no rectangular subset of A_2 contains $R(1; x_0)$, observe that A_3 provides a less-conservative approximation of $R(1; x_0)$.

$d^2(y, w, \widehat{y}, \widehat{w}) = F_{T_2}(y, w)$ in order to attain *the tightest parallelogram with shape matrix* T_2 that contains $R(1; x_0)$. An example is shown in Figure 5.3 where we apply Proposition 10 with T_2 to approximate $R(1; x_0)$ for the parameters taken previously, and this approximation is denoted $A_2 \subset \mathcal{X}$.

Observe in Figure 5.3 how the application of Proposition 10 in this setting produced a significantly tighter approximation of $R(1; x_0)$ than the initial Proposition 2 with a tight decomposition function. Moreover, while A_1 is not the tightest rectangle containing $R(1; x_0)$, the set A_2 is the tightest parallelogram with shape matrix T_2 that contains $R(1; x_0)$ and it is even true that no *rectangular* subset of A_2 contains $R(1; x_0)$. This observation highlights a main benefit in Proposition 10; for correctly chosen T, the application Proposition 10 may provide significant tighter approximation of $R(t; A)$ than, for example, the application of Proposition 2 for a rectangular reachable set approximation.

Furthermore, even though it is true that (5.20) is transformable to a monotone system via T_2, there indeed exists other transformations capable of producing monotone transformed dynamics and some of these transformations produce *even tighter* approximations of $R(1;x_0)$. We observe, for example, that under the transformation $T_3 = \left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right]$, the dynamics of $y = T_3^{-1}x$ are given by

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \end{bmatrix} = F_{T_3}(y,w) = \begin{bmatrix} (1-a)y_1 + y_2^3 - y_2(a^2 - 3a + 2) + w \\ y_1 + (a-2)y_2 \end{bmatrix} \tag{5.22}$$

and (5.22) is a monotone system for all $a \in [1,2]$. Thus, as a final demonstration, we over-approximate $R(1;x_0)$ using Proposition 10 with $T_3 = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$, *i.e.*, $a = 2$, and in this case

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \end{bmatrix} = F_{T_3}(y,w) = \begin{bmatrix} -y_1 + y_2^3 + w \\ y_1 \end{bmatrix}. \tag{5.23}$$

The parallelotope over-approximation of $R(1;x_0)$ derived in this case is denoted $A_3 \subseteq \mathcal{X}$ and we observe that $A_3 \subset A_2$; that is, the parallelotope approximation derived from the application Proposition 10 with $T_3 = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ is the tightest parallelotope with shape matrix T_3 that contains $R(t;x_0)$ and A_3 is a strict subset of A_2. See Figure 5.3. ■

Example 23 demonstrates how, in certain instances, transformations on the state space of (2.1) can be used to reduce conservatism in mixed monotone reachable set approximations. As a particular approach, we observe that it is sometimes possible to transform the system (2.1) to a *monotone* system via (5.16) and, in this case, the parallelotope over-approximation of $R(t;[\![a]\!]_T)$ derived via the application of Proposition 10 will be the tightest parallelotope with shape matrix T that contains $R(t;[\![a]\!]_T)$. While, in general, it can be difficult to identify a suitable transformation T so the (5.16) is monotone, there do exists certain special cases for when there is a natural choice of transformation; see Example 24.

Example 24. Consider the linear time-invariant system

$$\dot{x} = F^{\mathrm{LTI}}(x) = Ax, \tag{5.24}$$

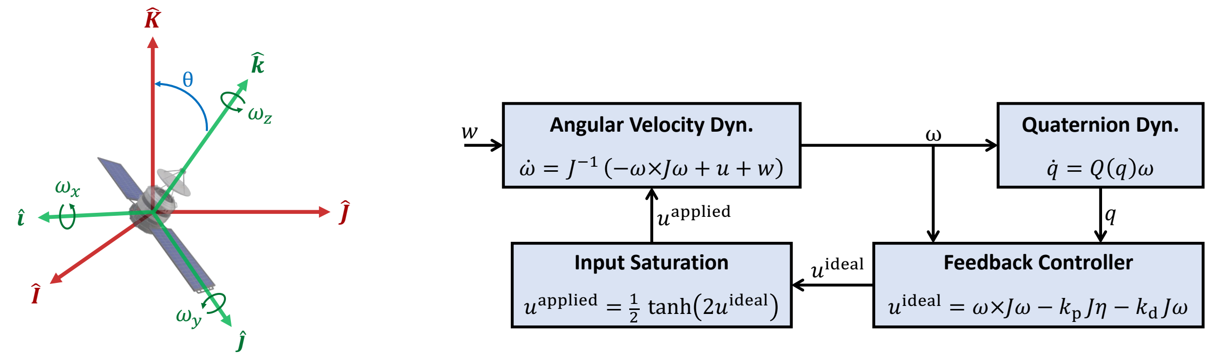
as previously studied in Example 3, where $x \in \mathbb{R}^n$ is the state and where we now omit the disturbance input so that $B = 0$. In the special instance where A admits only real eigenvalues, it is always possible to transform (5.24) to a monotone system via a Jordan decomposition. That is, when there exists a matrix $V \in \mathbb{R}^{n\times n}$ and a block diagonal matrix $\Lambda \in \mathbb{R}^{n\times n}$ so that $AV = V\Lambda$, it is always possible to choose $x = Vy$ so that

$$\dot{y} = \Lambda y, \tag{5.25}$$

and Λ is Metzler. In this case the n columns of $T^{-1} = V$ are the n (generalized) eigenvectors of A and the diagonal of Λ is comprised of the corresponding real eigenvalues. A related approach is demonstrated later in Example 25, where we consider a nonlinear system with inputs.

Furthermore, observe that when inputs are added so that $\dot{x} = Ax + Bu$, we have now that the transformation V leads to a transformed system $\dot{y} = \Lambda x + V^{-1}Bu$. While this new transformed system will not be a monotone system—unless $V^{-1}B$ is a positive matrix—we observe that it is generally possible to apply the approach from Example 22 in order to attain tight rectangular reachable sets for the transformed system, via the consideration of a transformed input space. ■

For general nonlinear systems it is usually difficult to identify a suitable transformation T so that (5.16) is monotone, and this is true even when there exist many such transformations. Regardless, there may, indeed, exist other natural choices for T such that (5.16) is not monotone but that reduce conservatism in mixed monotone reachable set approximations via the application of Proposition 10. We present a case study in the next section demonstrating this assertion, where we compute reachable sets for a 7-dimensional nonlinear spacecraft system and where we show how conservatism is reduced by considering a linear transformation on the system state space.



(a) (b)

Figure 5.4: Case Study of Section 5.3: Depiction of the spacecraft system. Subfigures: (a) The inertially-fixed reference frame $\mathcal{F}_{\text{I}}$ is shown in red and the body-fixed reference frame $\mathcal{F}_{\text{B}}$ is shown in green. The line-of-sight angle, which is the angle made between the $\widehat{k}$ and $\widehat{K}$ directions is given by (5.30) and is shown in blue. Note that the vectors ω, u, and w are all taken with respect to $\mathcal{F}_{\text{B}}$. (b) Depiction of the closed-loop spacecraft dynamics, (5.26) under (5.28), as an interconnection amongst subsystems.

5.3 Case Study: Reducing Conservatism in Mixed Monotone Reachable Set Approximations via Linear Transformations

In this section, we present demonstration where we show how linear transformations on the dynamics can be used to significantly reduce conservatism in the approximation of reachable sets:

We consider a 7-dimensional torque-controlled spacecraft in unconstrained rotational motion. The spacecraft is modeled with state $x = (q, \omega) \in \mathbb{R}^7$, control input $u \in \mathbb{R}^3$ and disturbance input $w \in \mathbb{R}^3$, where the orientation of the spacecraft is captured by the quaternion vector $q \in \mathbb{H} \subset \mathbb{R}^4$ and the angular velocity is captured by $\omega \in \mathbb{R}^3$. The quaternion vector $q = (q_0, q_1, q_2, q_3)$ defines the orientation of a body-fixed reference frame $\mathcal{F}_{\text{B}}$ with respect to an inertial frame $\mathcal{F}_{\text{I}}$, as depicted in Figure 5.4(a), and the components of $\omega = (\omega_x, \omega_y, \omega_z)$, $u = (u_1, u_2, u_3)$ and $w = (w_1, w_2, w_3)$ are expressed in the body frame $\mathcal{F}_{\text{B}}$. We denote also by $J \in \mathbb{R}^{3\times 3}$ the inertia matrix of the spacecraft, taken with respect to $\mathcal{F}_{\text{B}}$.

The dynamics of the spacecraft are described as the interconnection of subsystems and feedback controllers, as shown graphically in Figure 5.4(b). We consider the dynamical model

$$\begin{aligned}\dot{q} &= Q(q)\omega \\ \dot{\omega} &= J^{-1}(-\omega \times J\omega + u + w)\end{aligned} \tag{5.26}$$

where $\times$ denotes the cross product operator and where $Q(q) \in \mathbb{R}^{4\times 3}$ denotes the quaternion kinematic matrix,

$$Q(q) := \frac{1}{2}\begin{bmatrix} -q_1 & -q_2 & -q_3 \\ q_0 & -q_3 & q_2 \\ q_3 & q_0 & -q_1 \\ -q_2 & q_1 & q_0 \end{bmatrix}. \tag{5.27}$$

We consider also the stabilizing feedback controller

$$u(x) := \sigma\left(\omega \times J\omega - k_{\mathrm{p}} J\eta(q) - k_{\mathrm{d}} J\omega\right) \tag{5.28}$$

for suitable controller gains $k_{\mathrm{p}} > 0$, $k_{\mathrm{d}} > 0$, where

$$\eta(q) := \begin{bmatrix} 2(q_2 q_3 + q_0 q_1) \\ 2(q_0 q_2 - q_1 q_3) \\ 0 \end{bmatrix} \tag{5.29}$$

and where $\sigma(u) := \frac{1}{2}\tanh(u)$ is a saturation function. The goal of this study is to over-approximate the reachable set of the spacecraft (5.26) using mixed monotone systems theory and we show specifically how a linear transformation of the dynamics can allow for reduced conservatism in the approach. For ease of comparison, we introduce also a nonlinear output function

$$\theta(x) = \arccos\left(1 - 2q_1^2 - 2q_2^2\right), \tag{5.30}$$

that describes the orientation of a boresight sensor, and we attempt to over-approximate

$$R^{\theta}(t;x_0) := \{\theta(x_1) \in \mathbb{R} \,|\, x_1 \in R(t;x_0)\}\,, \tag{5.31}$$

which is the reachable set of spacecraft in the space of line-of-sight angles. We observe, in particular, that the controller posited in (5.28) stabilizes the system (5.26) to $\theta = 0$ when the model is considered deterministic, *i.e.*, $w = 0$.

As a first demonstration, we compute a decomposition function for the closed-loop dynamics (5.26) under (5.28), and then over-approximate $R^{\theta}(t;x_0)$ via an application of Proposition 2. In this setting, the highly nonlinear and nonconvex dynamics posited in (5.26)–(5.28) prevent the authors from attaining a tight decomposition function in closed-form. Nonetheless, we are able to attain a decomposition by applying the compound approach posited in Section 3.5: tight decomposition functions are constructed for the angular velocity and quaternion subsystems in (5.26), and we construct also an inclusion function for the feedback controller given in (5.28); a decomposition function for the composite system is then constructed via Proposition 6. Further details are provided in [42]. We observe, in particular, that while the individual decomposition functions used in the approach are tight for their respective subsystems, the resulting composite decomposition function is a non-tight decomposition function for the interconnection (5.26)–(5.28).

Denoting by d the decomposition function formed in this case, and by E the respective embedding function, we have that

$$R^{\theta}(t;x_0) \subseteq \Theta(\llbracket \Phi^{E}(t;x_0) \rrbracket) \tag{5.32}$$

where $\Theta : 2^{\mathcal{X}} \to 2^{\mathbb{R}}$ is an inclusion function for $\theta(x)$, and is given by $\Theta([\underline{x},\overline{x}]) := [\Theta(\underline{x},\overline{x}), \Theta(\overline{x},\underline{x})]$ for

$$\Theta(\underline{x},\overline{x}) := \arccos\Big(1 - 2g(\underline{q}_1,\overline{q}_1) - 2g(\underline{q}_2,\overline{q}_2)\Big), \tag{5.33}$$

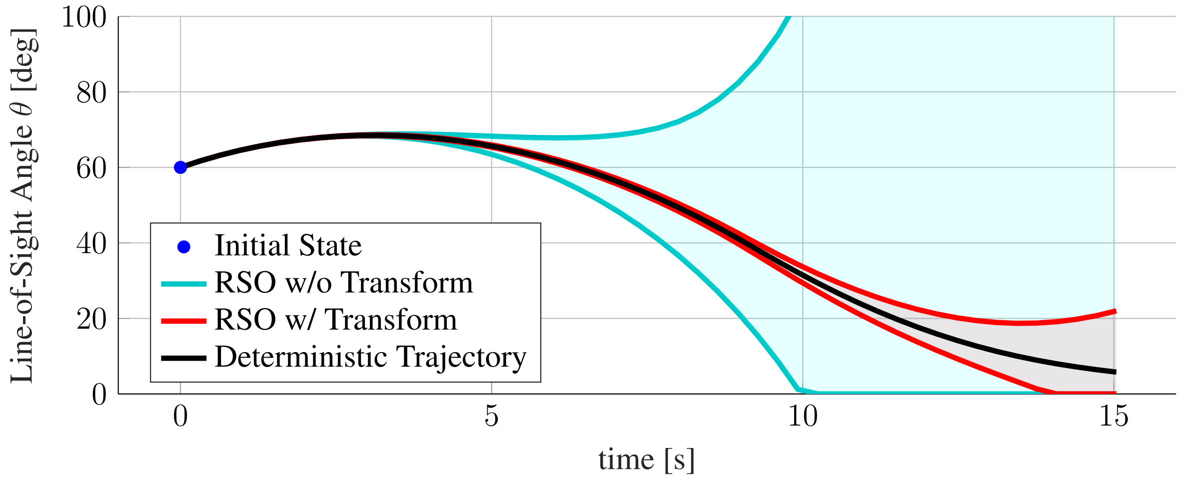


Figure 5.5: Case Study of Section 5.3: Computing reachable sets for the closed-loop spacecraft dynamics (5.26) under (5.28), by applying (5.32). Two hyperrectangular over-approximations of $R^{\theta}(t;x_0)$ are computed, with initial state $x_0 = (q_0, \omega_0)$ given by (5.35). The over-approximation of $R^{\theta}(t;x_0)$ attained from applying (5.32) with a decomposition function for the untransformed dynamics (5.26) is shown in blue. The over-approximation of $R^{\theta}(t;x_0)$ attained from applying (5.32) with a decomposition function for the transformed system (5.36) is shown in red. The initial state $x_0 = (q_0, \omega_0)$ given by (5.35) is shown in blue, and the deterministic trajectory $\theta(\phi(t;x_0,0))$, arising from the case with no disturbances, is shown in black.

$$g(q,\widehat{q}) := \begin{cases} q^2 & \text{if } q \geq 0 \text{ and } q \geq -\widehat{q}, \\ \\ \widehat{q}^2 & \text{if } \widehat{q} \leq 0 \text{ and } q < -\widehat{q}, \\ \\ 0. \end{cases} \tag{5.34}$$

An example is shown in Figure 5.5 where we apply (5.32) with the inclusion function (5.33) to compute an over-approximation of $R^{\theta}(t;x_0)$ on the time interval $t \in [0,15]$, where $x_0 = (q_0, \omega_0)$ with

$$q_0 = (\sqrt{3}/2,\, 0.5,\, 0,\, 0) \;\text{ and }\; \omega_0 = (0.1,\, 0.1,\, 0.1), \tag{5.35}$$

the disturbance bound is $\mathcal{W} = [-5\times 10^{-3}, 5\times 10^{-3}]^3$, the controller gains are $k_{\mathrm{p}} = 0.6$ and $k_{\mathrm{d}} = 2.25$, and the inertia matrix is given by $J = \left[\begin{smallmatrix} 17.5 & -0.8 & 0.3 \\ -0.8 & 14.9 & 0.4 \\ 0.3 & 0.4 & 20.8 \end{smallmatrix}\right]$. Observe also that $\theta(x_0) = 60°$.

In the setting of this example, we find that the application of (5.32) with a decomposition function for (5.26)–(5.28) provides a generally conservative approximation of $R^{\theta}(t; x_0)$. Excess conservatism can be attributed to coupling withing the vector field of (5.26); we observe, in particular, that $J^{-1}u$ appears in the dynamics and, using analogous reasoning to that provided in Example 22, we can reason that the decomposition function formed in this setting is considering, instead, an augmented space of control inputs at each time.

To remedy this issue, we next consider a linear transformation on the angular velocity $\Omega = J\omega$, so that the dynamics in (5.26)–(5.28) become

$$\begin{aligned} \dot{q} &= Q(q)J^{-1}\Omega \\ \dot{\Omega} &= -J^{-1}\Omega \times \Omega + u(x') + w \\ u(x') &:= \sigma\left(J^{-1}\Omega \times \Omega - k_{\mathrm{p}}J\eta(q) - k_{\mathrm{d}}\Omega\right) \end{aligned} \tag{5.36}$$

with state $x' = (q, \Omega)$ and where $w \in \mathcal{W}$ retains its definition from (5.26). A decomposition function is formed for the transformed system (5.36), using individual tight decomposition function for the rotation q and angular velocity Ω subsystems and using an inclusion function for the control policy $u(x')$. We then apply (5.32) in order to over-approximate $R^{\theta}(t; x_0)$ for the parameters taken previously. We show in Figure 5.5 how the application of (5.32) with a decomposition function for (5.36) provides a significantly tighter approximation of $R^{\theta}(t; x_0)$ in this setting. This reduction in conservatism and be attributed to the fact that, now, $u(x')$ appears directly in the dynamics of (5.36), rather than $J^{-1}u(x)$, *i.e.*, coupling is reduced.

5.4 Nonlinear Transformations for Reduced Conservatism in Mixed Monotone Reachable Set Approximations

The previous part of this chapter deals mainly with *linear* transformations on the state of (2.1), and we show how such transformations may allow one to compute reachable sets with reduced conservatism via the application of Proposition 10. In this section, we discuss a similar approach for reducing conservatism in mixed monotone reachable set approximations, involving a *nonlinear* transformation of the dynamics.

Indeed, many canonical nonlinear transformations appear in literature for the analysis of dynamical systems: for example, the polar coordinate transformation of linear time-invariant systems [83, 84], the transverse coordinate transformation of nonlinear systems [85], the center manifold transformation [86], and the so called feedback linearization transformation [87]. In our work, we observe that it is generally possible to apply the tools of mixed monotonicity to these transformed systems, in order to deduce time-domain properties of the initial system (2.1).

We consider a general nonlinear transformation $T : \mathcal{Y} \to \mathcal{X}$ on the statespace of (2.1), and we assume also that T is a bijection, so that

$$x = T(y) \quad \sim \quad y = T^{-1}(x). \tag{5.37}$$

In this instance, the dynamics of y are

$$\dot{y} = \frac{\partial T^{-1}}{\partial x}(T(y))F(T(y)), \tag{5.38}$$

and one can now apply Proposition 2 to the transformed dynamics in (5.38) in order to compute over-approximations reachable sets for the initial untransformed dynamics. In particular, for any initial set $A \subset \mathcal{X}$ so that

$$A \subseteq [\![b]\!]_{T(\cdot)} := \{x \in \mathcal{X} \,|\, T^{-1}(x) \in [\![b]\!]\} \tag{5.39}$$

we have that

$$R(t; A) \subseteq [\![\Phi^E(t; b)]\!]_{T(\cdot)} := \{x \in \mathcal{X} \,|\, T^{-1}(x) \in [\![\Phi^E(t; b)]\!]\}. \tag{5.40}$$

A particular transformation worth studying is that of *feedback linearization*, which can be used to transform the dynamics of a generally nonlinear system to a monotone dynamical system in certain instances.

Proposition 11 ([83]). *Consider the affine-in-control dynamical system*

$$\dot{x} = F(x,u) = f(x) + g(x)u \tag{5.41}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$ is the system state and now $u \in \mathbb{R}^m$ is considered as a control input.

Assume there exists a scalar valued function $h : \mathcal{X} \to \mathbb{R}$, so that both

- $L_g L_f^k h(x) = 0$ *for all $k \in \{1, \cdots, n-2\}$, and*
- $L_g L_f^{n-1} h(x) \neq 0$,

hold for all $x \in \mathcal{X}$. In this case, the function h is said to have relative degree n and the system (5.41) *is said to be feedback linearizable. In particular, it is the case that an invertible transformation*

$$y = T(x) = \begin{bmatrix} h(x) \\ L_f h(x) \\ \vdots \\ L_f^{n-1} h(x) \end{bmatrix}, \qquad \dot{y} = \begin{bmatrix} L_f h(x) \\ L_f^2 h(x) \\ \vdots \\ L_f^n h(x) + L_g L_f^{n-1} h(x) u \end{bmatrix} \tag{5.42}$$

exists so that

$$\begin{bmatrix} \dot{y}_1 \\ \vdots \\ \dot{y}_{n-1} \\ \dot{y}_n \end{bmatrix} = \begin{bmatrix} y_2 \\ \vdots \\ y_n \\ v \end{bmatrix}, \tag{5.43}$$

where

$$v(x,u) = L_f^n h(x) + L_g L_f^{n-1} h(x) u. \tag{5.44}$$

Furthermore, the system (5.43) *is a monotone control system with respect to the input v.* ■

Employing the feedback linearization approach posited Proposition 11 requires choosing $h(x)$ so that u appears in $\frac{\partial^n h}{\partial t^n}$, and a similar approach can sometimes be employed when disturbances are added. An example is provided below, where we consider a 2-dimensional nonlinear pendulum model with disturbances, where we compute invariant parallelotope regions for the pendulum through the use of feedback linearization and a linear transformation.

Example 25. Consider a torque-controlled pendulum, as shown graphically in Figure 5.6(a). The pendulum is modeled by the dynamical system

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -\frac{g}{L}\sin(x_1) + u + w \end{aligned} \tag{5.45}$$

where $x_1 \in \mathbb{R}$ is the orientation of the pendulum, $x_2 \in \mathbb{R}$ is the angular velocity, $L > 0$ is the length, $g = 9.81\mathrm{m/s}^2$ is the gravitational constant, $u \in \mathbb{R}$ is the control input and $w \in [\underline{w}, \overline{w}] \subset \mathbb{R}$ denotes actuator noise. Even though the system is nondeterministic, due to the disturbance input w, we are interested designing a stabilizing feedback controller as to ensure the forward invariance of some neighborhood of the origin.

To design such a controller, we consider a transformation on the input

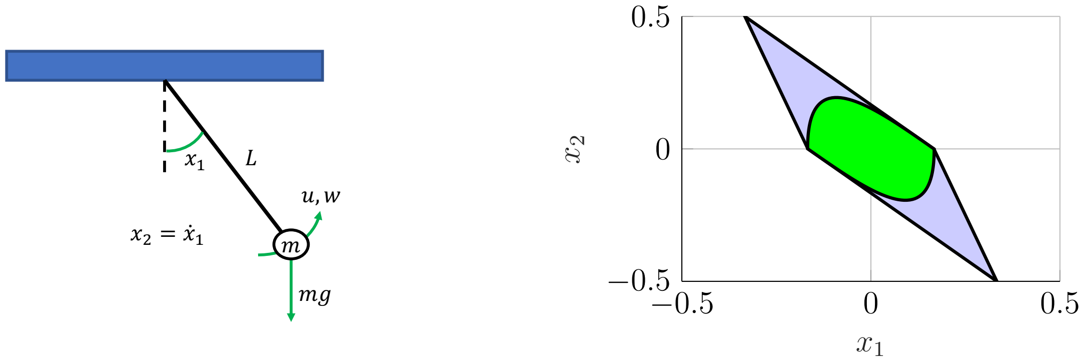
$$u(x) = -k_{\mathrm{p}}x_1 - k_{\mathrm{d}}x_2 + \frac{g}{L}\sin(x_1) \tag{5.46}$$

for controller gains $k_{\mathrm{p}}, k_{\mathrm{d}} \geq 0$, and in this case the dynamics in (5.45) become

$$\dot{x} = \begin{bmatrix} 0 & 1 \\ -k_{\mathrm{p}} & -k_{\mathrm{d}} \end{bmatrix} x + \begin{bmatrix} 0 \\ 1 \end{bmatrix} w. \tag{5.47}$$

The controller in (5.46) can be thought of as a trivial instantiation of the procedure in Proposition 11, where $h(x) = x_1$ and where the parameters $k_{\mathrm{p}}, k_{\mathrm{d}}$ are included for PD control. Furthermore, we observe that $A = \left[\begin{smallmatrix} 0 & 1 \\ -k_{\mathrm{p}} & -k_{\mathrm{d}} \end{smallmatrix}\right]$ admits negative real eigenvalues any time $k_{\mathrm{d}}^2 \geq 4k_{\mathrm{p}}$.

For the remainder of this example, we fix $k_{\mathrm{p}} = 3$ and $k_{\mathrm{d}} = 4$, however, we observe that (5.47) does not induce a stable embedding system for any decomposition function. This is due to the fact that $\left[\begin{smallmatrix} A^{\mathrm{M}+} & A^{\mathrm{M}-} \\ A^{\mathrm{M}-} & A^{\mathrm{M}+} \end{smallmatrix}\right]$ admits a positive real eigenvalue, even though A is stable. For this reason, we next consider a linear transformation $y = Tx$ on the dynamics of (5.47), where the columns of T are



(a) (b)

Figure 5.6: Example 25: Computing invariant regions for the torque-controlled pendulum model (5.45). Subfigures: (a) graphical depiction of the pendulum system, as modeled by (5.45). A stabilizing feedback controller is designed using the feedback linearization approach given in Proposition 11. (b) The forward invariant parallelotope $[\underline{y}, \overline{y}]_T$ attained from applying (5.49) with $[\underline{w}, \overline{w}] = [-\frac{1}{2}, \frac{1}{2}]$ is shown in blue, and this region is also globally attractive. The true smallest attractive region for (5.45) was computed via exhaustive simulation and shown in green.

the two real eigenvectors of A. In this case, the dynamics of $y \in \mathbb{R}^2$ become

$$\dot{y} = \begin{bmatrix} -3 & 0 \\ 0 & -1 \end{bmatrix} y + \begin{bmatrix} 1.5 \\ -0.5 \end{bmatrix} w. \tag{5.48}$$

See Example 24. Furthermore, one can now apply (4.38) from Example 19 to show that $[\underline{y}, \overline{y}] \subset \mathbb{R}^2$ is invariant and globally attractive for (5.48), when the disturbance space is $\mathcal{W} = [\underline{w}, \overline{w}]$, and where

$$\underline{y} = \frac{1}{2} \begin{bmatrix} \underline{w} \\ -\overline{w} \end{bmatrix} \qquad \overline{y} = \frac{1}{2} \begin{bmatrix} \overline{w} \\ -\underline{w} \end{bmatrix}. \tag{5.49}$$

In this way, $[\underline{y}, \overline{y}]_T$ is invariant and globally attractive for (5.47). An example is shown in Figure 5.6(b) where we apply (5.49) with $[\underline{w}, \overline{w}] = [-\frac{1}{2}, \frac{1}{2}]$ to compute an invariant and attractive region for (5.47). Excess conservatism in the approach can be attributed to the fact that the disturbance input w effects both entries of the vector-field in (5.48) and, in this way, the set $[\underline{y}, \overline{y}]$ is also invariant for an alternative system to (5.48) containing an augmented disturbance vector: see Example 21. ■

In Example 25, we consider a trivial instantiation of the feedback linearization approach, where the transformation posited in Proposition 11 effects only the control input. Indeed, a main difficulty in applying nonlinear transformations with mixed monotonicity is in inverting the nonlinear transformation in (5.40). Observe that the reachable set over-approximation derived from (5.40) is equal to the image of T when evaluated over a hyperrectangular set. Furthermore, we observe that general theory posited in this chapter for attaining tighter reachable set approximations via nonlinear transformations is useful mainly when the transformation is simple there exists some linear structure to the transformed system.

In the following section, we present a related approach for reducing conservatism in mixed monotone reachable set approximations, via the use of time-varying transformations on the statespace of (2.1).

5.5 Time-Varying Transformations for Reduced Conservatism in Mixed Monotone Reachable Set Approximations

Another related approach for reducing conservatism in mixed monotone reachable set approximations involves considering a *time-varying* transformation on the statespace of (2.1). Such a transformation generally leads to a time-varying set of transformed dynamics, and while have not yet discussed mixed monotonicity in the context of time-varying systems, this topic is a focus of other works, including [34].

As an initial point of of study, we consider the time-varying system

$$\dot{x} = F(t; x, w) \tag{5.50}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$ is the state, $w \in \mathcal{W} \subset \mathbb{R}^m$ is the disturbance and the vector field F now has explicit dependence on time. We denote by $\phi(t; x, \mathbf{w})$ the state of (5.50) reached at time $t \geq 0$ when beginning at state $x \in \mathcal{X}$ at time $t = 0$ and evolving subject to the piecewise-continuous disturbance input $\mathbf{w} : [0, t] \to \mathcal{W}$, and we denote by $R(t; A)$ the time-t reachable set as given by (2.2). Mixed monotonicity in the context of (5.50) is defined as follows:

Definition 12. The time-varying system (5.50) is mixed monotone with respect to $d(t; x, w, \widehat{x}, \widehat{w})$ if for all $x, \widehat{x} \in \mathcal{X}$, all $w, \widehat{w} \in \mathcal{W}$ and all $t \in \mathbb{R}$, the following hold:

- $d(t; x, w, x, w) = F(t; x, w)$,
- $\frac{\partial d_i}{\partial x_j}(t; x, w, \widehat{x}, \widehat{w}) \geq 0$ holds for all i, j with $i \neq j$,
- $\frac{\partial d_i}{\partial \widehat{x}_j}(t; x, w, \widehat{x}, \widehat{w}) \leq 0$ holds for all i, j, and
- $\frac{\partial d_i}{\partial w_k}(t; x, w, \widehat{x}, \widehat{w}) \geq 0$ and $\frac{\partial d_i}{\partial \widehat{w}_k}(t; x, w, \widehat{x}, \widehat{w}) \leq 0$ hold for all i and all k. ■

In this setting, one can think of a decomposition function $d(t; x, w, \widehat{x}, \widehat{w})$ as a decomposition function for a related time-invariant system with an augmented state vector; in particular,

$$d(t; x, w, \widehat{x}, \widehat{w}) := d_t((x, t), w, (\widehat{x}, t), \widehat{w}) \tag{5.51}$$

where $d_t\left((x, t), w, \left(\widehat{x}, \widehat{t}\right), \widehat{w}\right)$ is a decomposition function for the time-augmented system

$$\begin{bmatrix} \dot{x} \\ \dot{t} \end{bmatrix} = F_t((x, t), w) := \begin{bmatrix} F(x, w) \\ 1 \end{bmatrix} \tag{5.52}$$

and where the state of (5.52) is taken to be time-augmented vector $(x, t) \in \mathcal{X} \times \mathbb{R}$. We discuss this connection further in the next section where we show how *augmenting* the statespace of (2.1) can sometimes also be used to reduce conservatism in mixed monotone reachable set approximations.

As was the case in the time-invariant setting of (2.34), we apply a decomposition function d through a corresponding time-varying monotone embedding system

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = E(t; x, \widehat{x}) := \begin{bmatrix} d(t; x, \underline{w}, \widehat{x}, \overline{w}) \\ d(t; \widehat{x}, \overline{w}, x, \underline{w}) \end{bmatrix}, \tag{5.53}$$

and reachable sets of (5.50) can be efficiently computed using

$$R(t; [\![a]\!]) = [\![\Phi^E(t; a)]\!]. \tag{5.54}$$

Similar reachability analysis tools to those presented in Chapter 4 can also be constructed to attain, *e.g.*, over- and under-approximations of forward- and backward-time reachable sets for (5.50), and also robustly forward invariant sets, however, for ease of exposition in this section we do not present formal generalizations of these results here.

Indeed, the main reachability analysis tools presented in this thesis pertain to time-invariant setting of $\dot{x} = F(x, w)$. However, we show in the following how it is sometimes possible to transform the initial time-invariant system $\dot{x} = F(x, w)$ to form a time-varying mixed monotone system and how how reachable sets for the initial time invariant dynamics can be over-approximate using this approach. In this work, we mainly consider *linear* time-varying transformations, although it is true that more general nonlinear time-varying transformations are possible using the theory presented in Section 5.4.

To that end, consider a time-varying system $\dot{x} = F(t; x, w)$ as in (5.50), and consider also a time-varying linear transformation $T : \mathbb{R} \to \mathbb{R}^{n\times n}$ where we assume that $T(0) = I$, $T(t)$ is nonsingular for all t, and that $\frac{\partial T}{\partial t}$ exists for all t. Under the transformation $T(t)$, the dynamics of $y(t) := T(t)^{-1}x(t)$ become

$$\begin{aligned} \dot{y} &= F_T(t; y, w) \\ &:= T(t)^{-1} \Big(F\left(t; T(t)y, w\right) - \dot{T}(t)y \Big) \end{aligned} \tag{5.55}$$

where $y \in \mathcal{Y} \subset \mathbb{R}^{n\times n}$ is the state, $w \in \mathcal{W} \subset \mathbb{R}^m$ is the disturbance, and where F and $\mathcal{W}$ maintain their definitions from (5.50). We show next how the reachable set of (5.50) is efficiently over-approximated using a decomposition function for the transformed system (5.55):

Proposition 12. *Choose $T : \mathbb{R} \to \mathbb{R}^{n\times n}$ so that $T(0) = I$ and $T(t)$ is nonsingular for all t, and let* (5.55) *be mixed monotone with respect to d. For any hyperrectangular set of inital conditions*

$[\![a]\!] \subseteq \mathcal{X}$ *with* $a \in \mathcal{T}$*, we have*

$$R(t; [\![a]\!]) \subseteq [\![\Phi^E(t; a)]\!]_{T(t)}, \tag{5.56}$$

where $R(t; [\![a]\!])$ *denotes the reachable set of the original dynamics* (5.50) *as defined in* (2.2) *and* Φ^E *denotes the state transition function of the embedding system constructed from* d. ■

Observe that the application of Proposition 12 will produce a parallelotope over-approximation of $R(t; [\![a]\!])$ and that the shape matrix of the over-approximation is $T(t)$, and thus time-varying. While we specialize to the case of, *e.g.*, hyperrectangular initial sets $[\![a]\!]$ in Proposition 12, we observe also that it is generally possible to choose the inital set to be a parallelotope $[\![a]\!]_{T(0)}$ for some $T(0) \neq I$ so that $R(t; [\![a]\!]_{T(0)}) \subseteq [\![\Phi^E(t; a)]\!]_{T(t)}$. Furthermore, while the reachable set over-approximation attained via the application of Proposition 12 is a parallelotope $[\![\Phi^E(t; a)]\!]_{T(t)}$ we observe that it is always possible to produce a hyperrectangular over-approximation using the inclusion function

$$[\![a]\!]_{T(t)} \subseteq [\![T^{\mathrm{M}}(t)a]\!] \qquad \text{where} \qquad T^{\mathrm{M}}(t) := \begin{bmatrix} [T(t)]^+ & [T(t)]^- \\ [T(t)]^- & [T(t)]^+ \end{bmatrix}. \tag{5.57}$$

While the results of Proposition 12 are applicable to the more general setting of time-varying systems as in $\dot{x} = F(t; x, w)$, we show next through example how, even for time-invariant systems as in $\dot{x} = F(x, w)$, it is sometime possible to attain significantly tighter reachable set approximations using Proposition 12, than are attainable by either using Propositions 2 and 10.

Example 26. Consider the linear time-invariant system

$$\dot{x} = F^{\mathrm{LTI}}(x, w) = Ax + Bw, \tag{5.58}$$

where the state is $x \in \mathbb{R}^n$ and $w \in \mathcal{W}$ is the disturbance. We are interested in computing an over-approximation of the time-t reachable set $R(t; [\![a]\!])$, where $[\![a]\!] \subset \mathcal{X}$ is a hyperrectangle of initial conditions. Indeed, we have shown already in Example 3 how such over-approximations can be computed via Proposition 2 with, *e.g.*, the tight decomposition function provided in (2.24). In this example, we take a different approach and show how time-varying transformations can be used to attain tight parallelotope reachable set over-approximations for (5.58).

To that end, consider a time-varying transformation $T(t) = e^{At}$ on the state space of (5.58), so that the dynamics of $y(t) = T(t)^{-1}x(t)$ are

$$\dot{y} = e^{-At}Bw. \tag{5.59}$$

The system (5.59) is mixed monotone and its tight decomposition function is given by

$$d(w, \widehat{w}) = [e^{-At}B]^{+}w + [e^{-At}B]^{-}\widehat{w}, \tag{5.60}$$

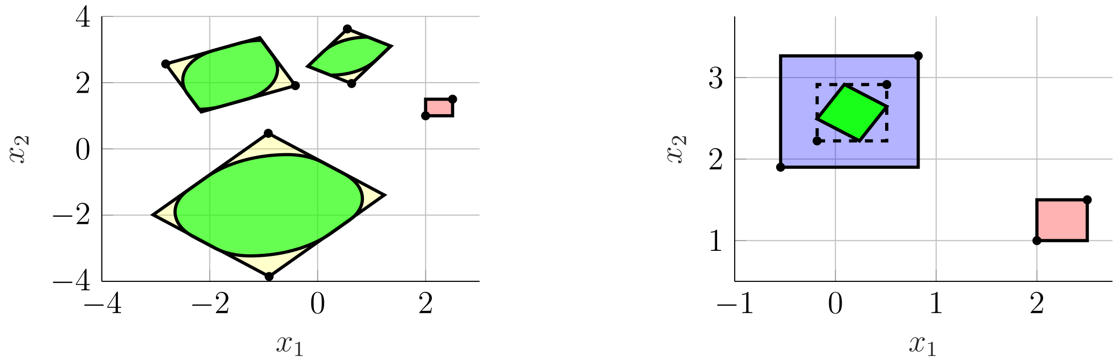
where we observe that for any fixed t, the transformed system (5.59) is linear time-invariant. Proposition 12 now implies that the reachable set of (5.58) is now efficiently over-approximated using a simulation of the time-varying embedding system (5.53), and we demonstrate this result in Figure 5.7 where we over-approximate $R(t; [\![a]\!])$ for

$$\dot{x} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} x + \begin{bmatrix} 1 \\ 0 \end{bmatrix} w \tag{5.61}$$

with $x \in \mathbb{R}^2$, $w \in [0, 1] \subset \mathbb{R}$, and $[\![a]\!] = [2, 2.5] \times [1, 1.5]$. Observe in Figure 5.7 how $[\![\Phi^E(t; a)]\!]_{T(t)}$ is the tightest parallelotope containing $R(t; [\![a]\!])$ in this case, and the shape matrix of the approximation changes with time.

As a second demonstration, consider the case where $B = 0$, so that $\dot{x} = Ax$ is a deterministic system, and in this case the transformed system in (5.59) becomes $\dot{y} = 0$. Observe that d from (5.60) is now given by $d(\,\cdot\,) = 0$ and applying Proposition12 we now have

$$R(t; [\![a]\!]) \subseteq [\![a]\!]_{e^{At}} \tag{5.62}$$



(a) (b)

Figure 5.7: Example 26: Computing tight parallelotope reachable set approximations for (5.58) using time-varying transformations. Subfigures: (a) Computing reachable sets for (5.61) where $w \in [0, 1]$. The initial set $\llbracket a \rrbracket$ is shown in red. We show $R(1, \llbracket a \rrbracket)$, $R(2, \llbracket a \rrbracket)$, and $R(4, \llbracket a \rrbracket)$ in green (top to bottom), and their respective parallelotope reachable set approximations derived via the application of Proposition 12 are shown in yellow. (b) Computing reachable sets for (5.58) where $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$. The initial set $\llbracket a \rrbracket$ is shown in red. We show $R(1, \llbracket a \rrbracket)$ in green, and observe that $R(1, \llbracket a \rrbracket) = \llbracket \Phi^E(1; a) \rrbracket_{T(1)}$. To further contrast the results of Propositions 2 and 12, we compute also a hyperrectangular over-approximation of $R(1, \llbracket a \rrbracket)$ using Propositions 2 with the tight decomposition function for (5.58) and this approximation is shown in blue. Finally, we compute a hyperrectangular reachable set over-approximation from $\llbracket \Phi^E(1; a) \rrbracket_{T(1)}$ by applying (5.57), and this region is outlined with black dashes.

where we observe that $a = \Phi^E(t; a)$ for all $t \geq 0$ and all $a \in \mathcal{T}$. Moreover, we observe that *every state $a \in \mathcal{T}$ is an equilibrium for the embedding system* (5.53) for all time. In this way, the application of Proposition 12 implicitly equates *forward invariant sets* for the transformed system (5.55) with *reachability tubes* for the initial system $\dot{x} = Ax$. Furthermore since the initial system $\dot{y} = 0$ is deterministic, observe that the diagonal space is invariant for the embedding system (2.34), and since the diagonal trajectories correspond to initial system trajectories we have that the true reachable set of $\dot{x} = Ax$ is *exactly equal to a* $\llbracket a \rrbracket_{e^{At}}$. To see this another way, observe that $\phi(t; x) = e^{At}x$ for linear time-invariant systems, and therefore $R(t; \llbracket a \rrbracket) = \{e^{-At}x \mid x \in \llbracket a \rrbracket\}$, *i.e.*, at any fixed time, the reachable set can be computed a using a linear transformation over the hyperrectangular initial set. As a final observation, we note that since the eigenvalues of A in (5.61) are imaginary, there does not exist a time-invariant linear transformation capable of producing a monotone system via (5.16). ∎

As a second demonstration of the approach, we next present an example where we apply Proposition 12 to a nonlinear system with an isolated linear component.

Example 27. Reconsider the 4-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = F(x,w) = \begin{bmatrix} -2x_1 + x_2(1+x_1) + x_3 + w \\ -x_2 + x_1(1-x_2) + 0.1 \\ -x_4 \\ x_3 \end{bmatrix} \tag{5.63}$$

as previously considered in Example 20, where $x \in \mathbb{R}^4$ is the state and $w \in \mathcal{W} = [-0.1, 0.1]$ is the disturbance. In Example 20, we compute a robustly forward invariant set for (5.63) via the application of Theorem 5; this invariant set is formed from a periodic solution $\Phi^E(t; (\underline{x}, \overline{x}))$ to the embedding system and we use a tight decomposition function in the approach. Nonetheless, in the setting of Example 20, we find that periodic orbits to the embedding system (2.34) exist only when $\underline{x}_3 = \overline{x}_3$ and $\underline{x}_4 = \overline{x}_4$.

In the setting of this example, we observe that the dynamics of (x_3, x_4) form an isolated linear subsystem of the dynamics in (5.63). For this reason, we consider a time-varying transformation

$$T(t) = \begin{bmatrix} I_2 & 0_{2\times 2} \\ 0_{2\times 2} & e^{\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]t} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(t) & -\sin(t) \\ 0 & 0 & \sin(t) & \cos(t) \end{bmatrix} \tag{5.64}$$

on the dynamics of (5.63) so that the dynamics of $y := T(t)^{-1}x$ in this setting become

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \\ \dot{y}_4 \end{bmatrix} = F_T(y,w) = \begin{bmatrix} -2y_1 + y_2(1+y_1) + \cos(t)y_3 + \sin(t)y_4 + w \\ -y_2 + y_1(1-y_2) + 0.1 \\ 0 \\ 0 \end{bmatrix}. \tag{5.65}$$

The transformed dynamics in (5.65) are mixed monotone with a tight decomposition function d' given by

$$
\begin{aligned}
d'_1(x,w,\widehat{x},\widehat{w}) &= -2x_1 + l_1(y,\widehat{y}) + l_3(y,\widehat{y}) + w \\
d'_2(x,w,\widehat{x},\widehat{w}) &= -x_2 + l_2(y,\widehat{y}) + 0.1, \\
d'_3(x,w,\widehat{x},\widehat{w}) &= 0 \\
d'_4(x,w,\widehat{x},\widehat{w}) &= 0,
\end{aligned}
\tag{5.66}
$$

where $l_1(\,\cdot\,)$ and $l_2(\,\cdot\,)$ are defined in (4.48), and

$$
l_3(y,\widehat{y}) := [\cos(t)]^+ y_3 + [\cos(t)]^- \widehat{y}_3 + [\sin(t)]^+ y_4 + [\sin(t)]^- \widehat{y}_4. \tag{5.67}
$$

We then compute an infinite-time simulation of the embedding system relative to d'; see (4.43). We find that $\Phi^{E'}(t;a)$ approaches a periodic orbit for

$$
a = (1,1,1,0,1.5,1.5,1.5,0.5) \tag{5.68}
$$

and this periodic orbit establishes a robustly forward invariant set for the initial untransformed dynamics in (5.63), as well. See Figure 5.8. ■

As discussed previously in (5.52), the procedure introduced in this section for constructing time-varying transformations effectively acts as a state-augmentation of the inital system dynamics in (2.1). We explore state-augmentation further in the next section, where we show how it is sometimes possible augment the state of (2.1) using redundant state variables in order to further reduce conservatism in mixed monotone reachable set approximations.

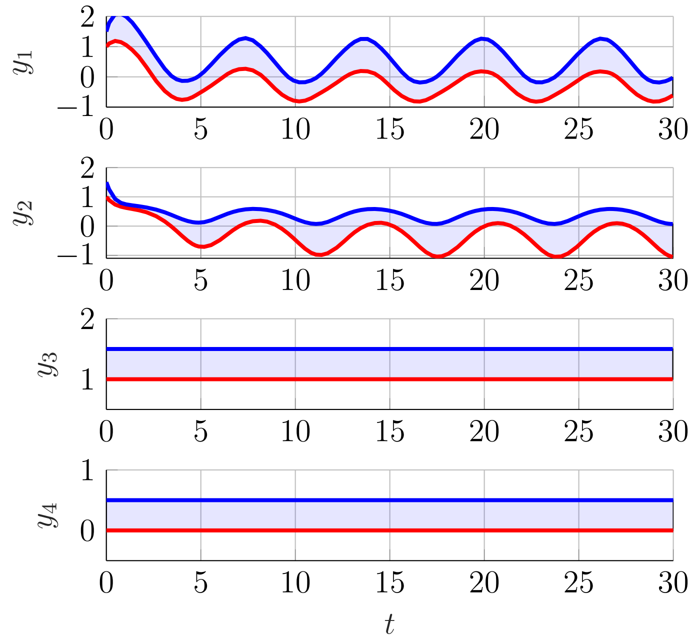


Figure 5.8: Example 27: Computing robustly invariant and attractive sets for (5.63) via the identification of a periodic orbit in the embedding space of (5.66). We conduct an infinite-time simulation of the embedding system relative to (5.66), and find that $\Phi^{E'}(t;a)$ approaches a periodic orbit. This periodic orbit then establishes a robustly forward invariant and attractive set for (5.65), shown in light blue above, and can be used to establish a robustly forward invariant set for (5.63), as well.

5.6 State-Augmentation for Reduced Conservatism in Mixed Monotone Reachable Set Approximations

As a final tools for reducing conservatism in mixed monotone reachable set approximations, in this section, we discuss a related approach involving a *state-augmentation* of the initial system dynamics in (2.1). Indeed, state-augmentation has been shown to provide many useful analysis tools for systems as in (2.1), with applications outside of reachability, *e.g.*, optimization theory [88, 89]. In our work, we study augmenting the state vector of an initial n-dimensional system with redundant state variables, formed via, *e.g.*, linear combinations of the entries of x. We then apply the tools of mixed monotonicity with a decomposition function for the augmented system, which contains more than n states, in order to attain reachable set approximations for the initial system with reduced conservatism.

To facilitate discussion in this section, we begin with an example based on [68, Example 1].

In particular, the work [68] studies conservatism in the approximation of reachable sets using interval readability analysis [66, 67], and the authors show how the interval arithmetic approach, when applied to an augmented system to that of (2.1) can be used to increase the fidelity of the approximations derived.

Example 28. Consider the 3-dimensional polynomial system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = F^1(x) = \begin{bmatrix} -x_1x_2 + x_3 \\ 2x_1x_2 \\ x_1 + x_2 \end{bmatrix} \tag{5.69}$$

with state space $\mathcal{X} = \mathbb{R}^3$. The system (5.69) is mixed monotone with a tight decomposition function given by

$$\begin{aligned} d_1(x, \widehat{x}) &= \begin{cases} -x_1x_2 + x_3 & \text{if } x_1 \leq 0, \\ -x_1\widehat{x}_2 + x_3 & \text{if } x_1 \geq 0, \end{cases} \\ d_2(x, \widehat{x}) &= \begin{cases} 2x_1x_2 & \text{if } x_2 \geq 0, \\ 2\widehat{x}_1x_2 & \text{if } x_2 \leq 0, \end{cases} \\ d_3(x, \widehat{x}) &= x_1 + x_2. \end{aligned} \tag{5.70}$$

Proposition 2 now implies that the reachable set of (5.69) from $[\![a^1]\!]$ is approximated via a simulation of the embedding system (2.34) and, since d from (5.70) is a tight decomposition function for (5.69), no other decomposition function for (5.69) will produce a tighter approximation of $R^{F^1}(t; [\![a^1]\!])$. Nonetheless, d produces conservative approximations of reachable sets, and a demonstration of this fact is provided in Figure 5.9 where we take an initial set $[\![a^1]\!] = [0, 1]^3$ and where we approximate $R(\frac{1}{2}; [\![a^1]\!])$ for (5.69) by applying Proposition 2.

We consider, next, a redundant state variable $x_4 = x_1 + x_2$, so that the dynamics of (5.69) become

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = F^2(x) = \begin{bmatrix} -x_1x_2 + x_3 \\ 2x_1x_2 \\ x_4 \\ x_1x_2 + x_3 \end{bmatrix}. \tag{5.71}$$

Indeed, for all $x_1, x_2, x_3 \in \mathbb{R}$ and all $i \in \{1, 2, 3\}$

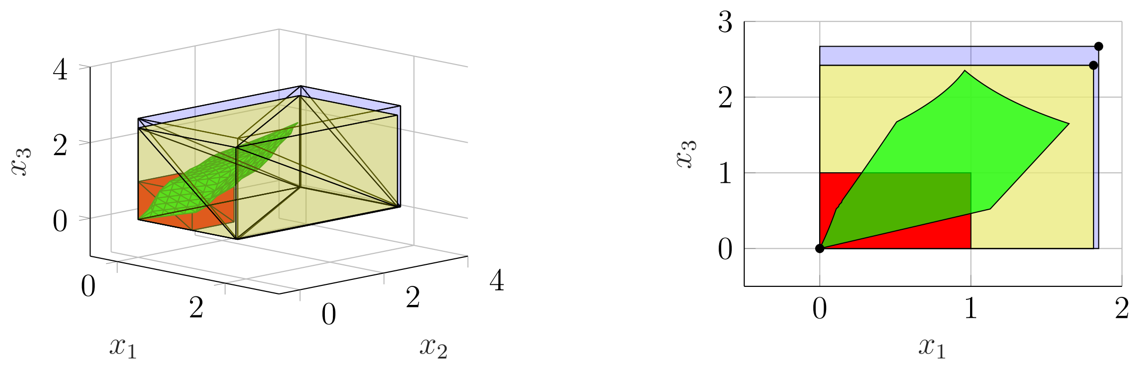
$$\phi_i^1(t; (x_1, x_2, x_3)) = \phi_i^2(t; (x_1, x_2, x_3, x_1 + x_2)) \tag{5.72}$$

and, thus, reachable sets of (5.69) can be approximated by applying the mixed monotonicity procedure to the system (5.71). An example is shown in Figure 5.9 where we approximate $R(\frac{1}{2}; [\![a^1]\!])$ using a tight decomposition function for (5.71). In this case, the embedding system relating to (5.71) is simulated forward in time $\frac{1}{2}$ time-units from the initial state $a^2(0) = (0, 0, 0, 0, 1, 1, 1, 2)$, and a rectangular over-approximation of $R(\frac{1}{2}, [\![a^1]\!])$ is formed by $[a^2_{1:3}(t), a^2_{5:7}(t)]$. Note that applying Proposition 2 to the redundant system (5.71), allows for tighter approximations of $R(\frac{1}{2}; [\![a^1]\!])$ than when used with (5.69). As a final point, observe that it is also possible to exploit the 4^{th} and 8^{th} coordinates of the $a^2(\frac{1}{2})$ in order to produce bounds on $x_4(\frac{1}{2}) = x_1(\frac{1}{2}) + x_2(\frac{1}{2})$, *i.e.*, half-plane regions containing the reachable set of (5.69). ■

Following our example above, we next move to formalize the theory of how state-augmentations allow for reducing conservatism in mixed monotone reachable set approximations. For ease of discussion, we consider the addition of a single state, defined as a linear combination

$$x_{n+1} = Tx = T_1x_1 + T_2x_2 + \cdots + T_nx_n \tag{5.73}$$

for $T \in \mathbb{R}^{1\times n}$. Indeed, there may be many ways of representing the dynamics of the augmented state vector $y := (x, x_{n+1})$; see [68] where the authors show how certain dynamics choices for y may lead to tighter reachable set approximations that others when a tight decomposition function is used. In our characterization, we observe that it is generally preferable to choose an augmented



(a) (b)

Figure 5.9: Example 28: Computing tight reachable set approximations via state-augmentation. Subfigures: (a) $[\![a^1]\!]$ is shown in red. $R^{F^1}(0.5; [\![a^1]\!])$ is shown in green with over-approximations derived from the application of Proposition 2 with (5.69) and (5.71) shown in blue and yellow, respectively. Note that applying Proposition 2 with a tight decomposition function for (5.71) allows for tighter approximations of $R^{F^1}(0.5; [\![a^1]\!])$ then when a tight decomposition function for (5.69) is used. (b) Projection of Figure 5.9(a) onto the x_1–x_3 plane.

dynamical system $\dot{y} = F^y(y, w)$ so that F^y reduces coupling in comparison to F or induces monotone transformed dynamics. See Examples 21 and 22.

We observe further that, when choosing $x_{n+1} = Tx$, it is important that $\frac{\partial T}{\partial x}(x) \geq 0$ for all x, *i.e.*, T is a positive row vector. In the case where this statement does not hold, observe that it may be possible to obtain augmented dynamics $\dot{y} = F^y(y, w)$ that are monotone, but where the resulting reachable set approximation derived from the augmented dynamics does not recover the tightest hyperrectangle containing the reachable set of $\dot{x} = F(x, w)$.

5.7 Conclusion

In this chapter, we study conservatism in mixed monotone reachable set approximations and we present new tools for reducing conservatism via transformations of the initial system state space. In particular, we study *how* conservatism enters the reachability analysis procedure, and we present several general methods for reducing conservatism in reachable set approximations. Our approach in this matter is to consider an *alternative tight decomposition function* corresponding to a state-transformations of the initial system dynamics. Linear transformations, nonlinear transformations, time-varying transformations, and state-augmentations are all considered. We present also an extended example, where we consider a 7-dimensional nonlinear spacecraft system and where we demonstrate how a linear transformation on the dynamics allows for tighter reachable set approximations via mixed monotonicity.

CHAPTER 6

MIXED MONOTONICITY FOR SAFETY AND VERIFICATION OF COMPLEX DYNAMICAL SYSTEMS

In this section, we present two case studies, where we apply the theoretical framework of mixed monotonicity in order to verify and enforce safety properties on complex dynamical systems.

We study safe-by-construction controllers whose safety guarantees are certified online via in-the-loop reachability analysis using mixed monotonicity. This approach is referred to in literature as Run Time Assurance (RTA), which provides an elegant and highly-adaptable methodology for assured autonomy [56] and where current research and applications are being conducted in the domains of, *e.g.*, spacecraft systems [90–92]. Given a desired control policy, an assurance mechanism will *filter* the desired input online in such a way that preserves system safety while also ensuring that the desired control input is passed to the system when it is safe to do so. In this way, the addition of an RTA works to decouple the task of enforcing safety constraints from all other objectives of the controller and allows a designer to sidestep the common trade-off between performance and safety. Canonical examples of RTA mechanisms include the Simplex architecture [93–96], which switches to a backup control scheme when necessary, and control barrier functions (CBFs) [57, 97, 98], which adjust desired control actions in a minimally invasive way to ensure forward invariance of a predetermined safe subset of the state space.

In this chapter, we present two basic run time assurance mechanism, and case studies, where RTA controllers are constructed using mixed monotone systems theory and in-the-loop reachability analysis. We first present a CBF-based run time assurance architecture, and a numerical example where we enforce inter-agent distance constraints on a platoon of three networked vehicles using this construction. Second, we present a case study where we develop a Simplex Architecture based run time assurance mechanism, using mixed monotonicity, and we demonstrate the real-word applicability of our construction via a hardware demonstration on the Autonomous Spacecraft Testing of Robotic Operations in Space (ASTROS) platform, at the Georgia Institute of Technology; see Figure 6.4, later. A video of this experiment is available at `https://youtu.be/g1-zMepDm1I`.

6.1 Online Reachability Analysis for Enforced System Safety with Barrier Functions and Applications to Vehicle Platoons

Controllers whose safety guarantees are derived through the online enforcement of constraints are referred to in literature as *run time assurance architectures* (RTA) [99] or *active set invariance filters* (ASIF) [100, 101]. In this setting, system safety is posed as an invariance constraint, requiring that a system avoid some unsafe region of the statespace for all time. Specifications of this class are often used to describe real-word safety specifications due to the fact that the definition of real-world safety often is presented as the ability to avoid unsafe scenarios during deployment.

Numerous mechanisms exist for enforcing invariance constraints within the control-loop, and in particular, control barrier functions (CBFs) are well suited for this task. CBF-based run time assurance architectures modify a suggested desired input at run time to create a safe forward invariant region in the state space. This is a main idea of [57, 80] where the resulting controller is formulated as a quadratic program for systems with no disturbances, and this idea is extended in [79] to the setting with disturbances. A limitation of these approaches is the need to verify a controlled forward invariant region *a priori* and in general this region should be large as to enable the satisfaction of performance criteria; this problem can also be formulated as the search for a backup strategy with a corresponding controlled forward invariant region [102, 103]. The authors of [100, 101] present a CBF-based run time assurance architecture that uses look-ahead methods within the control-loop in order to allow the system to leave a safe invariant region when a backup strategy is verified to return the system to this region. In this way size of the safe set is effectively increased and, thus, this approach eases the problem of verifying a large forward invariant region *a priori*. These works do not consider systems with disturbances, however, numerous impressive hardware experiments [104] have been performed demonstrating the real-world applicability of the

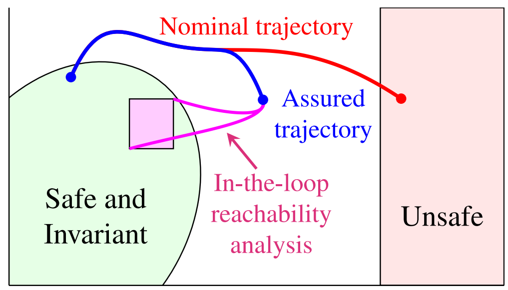


Figure 6.1: Case Study of Section 6.1: Run time assurance approach. Reachable sets are computed within the control-loop using mixed monotonicity, and these predictions are used in order to certify a safe backup strategy.

approach. See also [105].

In this case study, we use mixed monotonicity based reachability methods, together with control barrier functions, in order to design a run time assurance architecture for controlled dynamical systems with disturbances. Given a safe forward invariant region and a verified backup strategy, the RTA performs online reachability analysis using mixed monotone systems theory in order to ensure that is always possible reach the forward invariant region without violating a safety constraint. Control decisions within the RTA are determined using a modified control barrier formulation, where the barrier constraint is evaluated over the system's reachable set. In this way, the RTA will allow the system to leave the invariant region when safe backup strategy is available, and therefore our construction similarly avoids necessity for a large invariant safe set at the onset of analysis.

The results and tools generated in this study are demonstrated though a concluding example where we synthesize a safe controller for a vehicle platoon model using mixed monotonicity and control barrier functions. See also [47, 48] where the authors perform real-world experiments using teams of unmanned aerial vehicles, and where the same mixed monotone CBF approach is employed in the run time assurance mechanism.

6.1.1 Problem Formulation and Motivation

We consider, in this study, a controlled dynamical system

$$\dot{x} = f(x) + g_1(x)u + g_2(x)w \tag{6.1}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^m$ is the control input, and $w \in \mathcal{W} = [\underline{w}, \overline{w}] \subset \mathbb{R}^p$ is the disturbance input. We denote by $\phi(t; x, \mathbf{u}, \mathbf{w})$ the state of (6.1) reached at time $t \geq 0$, when beginning at an initial state x at time 0 and evolving subject to a feedback controller $\mathbf{u} : \mathbb{R}^n \to \mathbb{R}^m$ and the disturbance signal $\mathbf{w} : [0, t] \to \mathcal{W}$. Further, we assume that f, g_1, and g_2 are Lipschitz continuous functions and that $\mathbf{w}$ is piecewise-continuous in time so that $\phi(t; x, \mathbf{u}, \mathbf{w})$ is unique when it exists.

The primary focus of this study is in designing safe controllers for the system (6.1): the system (6.1) is paired with an *unsafe* subset of the system statespace $\mathcal{X}_{\mathrm{u}} \subset \mathbb{R}^n$, and we say that a controller $\mathbf{u} : \mathbb{R}^n \to \mathbb{R}^m$ is *safe with respect to state* x if $\phi(t; x, \mathbf{u}, \mathbf{w}) \in \mathbb{R}^n \setminus \mathcal{X}_{\mathrm{u}}$ for all $t \geq 0$ and for all $\mathbf{w} : [0, t] \to \mathcal{W}$. We extend this notation to sets as well so that $\mathbf{u}$ is *safe with respect to* $\mathcal{S} \subset \mathbb{R}^n$ if $\mathbf{u}$ is safe with respect x for all $x \in \mathcal{S}$.

Indeed, one way to establish safety is through invariance. Consider

$$\mathcal{S} = \{x \in \mathbb{R}^n \,|\, h(x) \geq 0\} \subset \mathbb{R}^n \setminus \mathcal{X}_{\mathrm{u}} \tag{6.2}$$

for some continuously differentiable $h : \mathbb{R}^n \to \mathbb{R}$ and consider also the pointwise-defined controller

$$\mathbf{u}^{\mathrm{CBF}}(x) = \underset{u \in \mathbb{R}^m}{\arg\min} ||u - \mathbf{u}^{\mathrm{d}}(x)||_2^2 \tag{6.3}$$

$$\text{s.t. } \frac{\partial h}{\partial x}(x)(f(x) + g_1(x)u + g_2(x)w) \geq -\alpha(h(x)) \tag{6.4}$$

$$\forall w \in \mathcal{W}$$

where $\alpha : \mathbb{R} \to \mathbb{R}$ is a given locally Lipschitz class-$\mathcal{K}$ function and $\mathbf{u}^{\mathrm{d}}(x)$ is some given controller. In the instance where the set of u satisfying the constraint (6.4) is nonempty for all x, we have also that $\mathcal{S}$ is robustly forward invariant for (6.1) and in this way $\mathbf{u}^{\mathrm{CBF}}$ is safe with respect to $\mathcal{S}$. Furthermore, in this instance, we say that h is a *control barrier function* (CBF) for (6.1), as developed in [80]. Now applying $\mathbf{u}^{\mathrm{CBF}}$ from (6.3)–(6.4) guarantees system safety for all time and, as a second practical benefit, $\mathbf{u}^{\mathrm{CBF}}$ will evaluate to $\mathbf{u}^{\mathrm{d}}$ whenever possible. Thus, when the controller $\mathbf{u}^{\mathrm{d}}$ is chosen to satisfy performance criteria, the controller posited by $\mathbf{u}^{\mathrm{CBF}}$ will retain these performance advantages while also ensuring safety.

To that end, we assume knowledge of a backup controller which is safe with respect to some subset of the statespace by virtue of a robustly invariant backup region. We say that the pair $(\mathbf{u}^{\mathrm{b}}, S_{\mathrm{b}})$ with $\mathbf{u}^{\mathrm{b}} : \mathbb{R}^n \to \mathbb{R}^m$ and $S_{\mathrm{b}} = \{x \in \mathbb{R}^n \mid h(x) \geq 0\}$ is a *backup control policy* if:

1. S_{b} is compact and $S_{\mathrm{b}} \cap \mathcal{X}_{\mathrm{u}} = \varnothing$,

2. h is concave on $\mathbb{R}^n$,

3. $\frac{\partial h}{\partial x} \neq 0$ on the boundary of S_{b}, and

4. there exists a class-$\mathcal{K}$ function $\alpha : \mathbb{R} \to \mathbb{R}$ such that

$$\frac{\partial h}{\partial x}(x)\left(f(x) + g_1(x)\mathbf{u}^{\mathrm{b}}(x) + g_2(x)w\right) \geq -\alpha(h(x)) \tag{6.5}$$

   holds for all $x \in S_{\mathrm{b}}$ and for all $w \in \mathcal{W}$.

In particular, the last condition above implies S_{b} is robustly forward invariant for (6.1) under $\mathbf{u}^{\mathrm{b}}$ via the CBF conditions discussed above and therefore $\mathbf{u}^{\mathrm{b}}$ is safe with respect to S_{b} by virtue of the first condition [79]. In this case, $\mathbf{u}^{\mathrm{b}}$ is called a *backup controller* and S_{b} its *backup region*.

While the existence of a backup strategy ensures system safety, there are two primary reasons why applying such a policy is generally not preferable: (i) backup controllers are typically designed without considering performance objectives and it may be the case where there exists some other controller $\mathbf{u}^{\mathrm{d}}$ that outperforms $\mathbf{u}^{\mathrm{b}}$ in application, and (ii) $\mathbf{u}^{\mathrm{b}}$ may be safe with respect to a set larger than S_b, and it is possible that S_b is too conservative to satisfy certain performance objectives. We have already discussed how CBFs provide a solution to the first problem; however, traditional CBF based controllers are still subject to the limitations of the second problem. A solution to the second problem is presented in [100, 101] for deterministic systems, where the authors effectively increase the size of the safe region through the use of look-ahead methods.

In the next section, we present a controller architecture, which is designed with knowledge of $\mathbf{u}^\mathrm{b}$ but which also allows the system to leave the, perhaps conservative, safe set S_b. In particular, we assume a system of form (6.1), an unsafe set $\mathcal{X}_\mathrm{u} \subset \mathbb{R}^n$, a backup control policy $(\mathbf{u}^\mathrm{b},\ S_\mathrm{b})$, and a desired controller $\mathbf{u}^\mathrm{d}$ that satisfies some performance objective but is perhaps not safe with respect to S_b; our objective is to is to design an *assured controller* $\mathbf{u}^\mathrm{ASIF}$ such that $\mathbf{u}^\mathrm{ASIF}$ is safe with respect to S_b and such that $\mathbf{u}^\mathrm{ASIF}(x)$ evaluates to $\mathbf{u}^\mathrm{d}(x)$ when it is safe to do so. As stated above, we particularly aim for an assured controller that need not render S_b forward invariant; it may be the case, for instance, that for certain initial conditions $x \in S_\mathrm{b}$, the system (6.1) will be driven out of S_b by $\mathbf{u}^\mathrm{ASIF}$ and may not return. Regardless, safety is assured via knowledge of $\mathbf{u}^\mathrm{b}$, and thus $\mathbf{u}^\mathrm{ASIF}$ is safe with respect to S_b.

6.1.2 Mixed Monotonicity based Active Set Invariance

In this section, we design a controller architecture which both allows the system to leave S_b and ensures that the system never enters $\mathcal{X}_\mathrm{u}$. The proposed controller uses a modified CBF formulation, where we now use mixed monotonicity based reachability methods to assess the nondeterminism in the system model.

We assume a system of the form (6.1), an unsafe set $\mathcal{X}_\mathrm{u} \subset \mathbb{R}^n$, a backup controller $\mathbf{u}^\mathrm{b}$ with a compact backup region $S_\mathrm{b} = \{x \in \mathbb{R}^n \,|\, h(x) \geq 0\}$, and a desired controller $\mathbf{u}^\mathrm{d}$. We denote by

$$\dot{x} = F^\mathrm{b}(x, w) := f(x) + g_1(x)\mathbf{u}^\mathrm{b}(x) + g_2(x)w \tag{6.6}$$

the closed-loop dynamics of (6.1) under $\mathbf{u}^{\mathrm{b}}$ and we let

$$\phi^{\mathrm{b}}(t; x, \mathbf{w}) := \phi(t; x, \mathbf{u}^{\mathrm{b}}, \mathbf{w}) \tag{6.7}$$

denote the state transition function of this system. Thus, h is a CBF for (6.6) and $\mathbf{u}^{\mathrm{b}}$ is safe with respect to S^{b}. Additionally, we denote by

$$S_{\mathrm{b}}^{+}(t) := \left\{ x \in \mathbb{R}^n \,\middle|\, \phi^{\mathrm{b}}(t; x, \mathbf{w}) \in S_{\mathrm{b}} \text{ for all } \mathbf{w} : [0, t] \to \mathcal{W} \right\} \tag{6.8}$$

the time-t basin of attraction of S_{b}, which is the set of states that are guaranteed to enter S_{b} along trajectories of (6.6) within the time-horizon $[0, t]$. Observe that since S_{b} is robustly forward invariant for (6.6), we additionally have that $S_{\mathrm{b}}^{+}(t)$ is robustly forward invariant for (6.6) for all $t \geq 0$.

As in [100], the RTA formulation presented in this study allows the system to leave the safe set S_{b} in instances where the backup control policy is known to return the system to S_{b} on some finite time-horizon. For this reason, we associate the backup control policy $(\mathbf{u}^{\mathrm{b}},\, S_{\mathrm{b}})$ with a fixed backup time T_{b}, where we assume that the T_{b}-second basin of attraction of S_{b} under the backup dynamics (6.6) does not intersect the unsafe set, *i.e.*,

$$S_{\mathrm{b}}^{+}(T_{\mathrm{b}}) \cap \mathcal{X}_{\mathrm{u}} = \varnothing. \tag{6.9}$$

To verify the condition in (6.9) holds, one can over-approximate backward reachable sets of S_{b} under (6.6) and check for intersection with the unsafe set $\mathcal{X}_{\mathrm{u}}$. Many techniques allow for such an over-approximation, and in the example provided at the end of this study we use mixed monotone systems theory and Proposition 7 in order to compute these backward-time over-approximations.

Given a state x, possibly with $x \notin S^{\mathrm{b}}$, our goal is to determine a suitable value $\mathbf{u}^{\mathrm{ASIF}}(x)$; as suggested by the problem statement, $\mathbf{u}^{\mathrm{ASIF}}(x)$ should be equal or close to $\mathbf{u}^{\mathrm{d}}(x)$ if it is safe to do so. One method to determine whether or not $\mathbf{u}^{\mathrm{ASIF}}(x)$ should be equal to $\mathbf{u}^{\mathrm{d}}(x)$ is to assess the safety of the backup controller with respect to x, *i.e.*, if $R_{\mathrm{b}}(t;x) \subseteq S^{\mathrm{b}}$ for some $t < T_{\mathrm{b}}$ then $\mathbf{u}^{\mathrm{ASIF}}(x) = \mathbf{u}^{\mathrm{d}}(x)$ is allowed, where we let $R_{\mathrm{b}}(t;x)$ denote the time-t forward reachable set of (6.6) as in (2.2). We next present a family of functions that, for given $x \in \mathbb{R}^n$, can be used to assess whether or not $R_{\mathrm{b}}(t;x) \subseteq S^{\mathrm{b}}$ for some $t < T_{\mathrm{b}}$, and these functions exploit the mixed monotonicity of (6.6).

Assume that the backup dynamics (6.6) are mixed monotone with respect to d, and denote by Φ^E the transition function of its respective embedding system. Define

$$\gamma^{\mathrm{ideal}}(t;x) := \inf_{z \in [\![\Phi^E(t;x)]\!]} h(z) = \min_{z \in \langle\!\langle \Phi^E(t;x) \rangle\!\rangle} h(z), \tag{6.10}$$

where the second equality comes from the concavity on h. Further observe that, for any x and any $t \geq 0$, the statement $x \in S_{\mathrm{b}}^{+}(t)$ holds when $\gamma^{\mathrm{ideal}}(t;x) \geq 0$. Next define

$$\Psi^{\mathrm{ideal}}(x) := \sup_{0 \leq \tau \leq T_{\mathrm{b}}} \gamma^{\mathrm{ideal}}(\tau;x). \tag{6.11}$$

If $\Psi^{\mathrm{ideal}}(x) \geq 0$ for some $x \in \mathcal{X}$, then applying the backup control policy starting from x at time 0 ensures that there exists a time $\tau \leq T_{\mathrm{b}}$ such that $R_{\mathrm{b}}(t;x) \subseteq S_{\mathrm{b}}$ for all $t \geq \tau$. In this case, we also have that $\mathbf{u}^{\mathrm{b}}$ is safe with respect to x. In particular, note that the set

$$S_{\Psi}^{\mathrm{ideal}} := \{x \in \mathcal{X} \mid \Psi^{\mathrm{ideal}}(x) \geq 0\} \tag{6.12}$$

is robustly forward invariant on (6.6), and $S_{\Psi}^{\mathrm{ideal}} \subseteq S_{\mathrm{b}}^{+}(T_{\mathrm{b}})$. Thus, any controller that renders $S_{\Psi}^{\mathrm{ideal}}$ robustly forward invariant will be safe with respect to x. CBFs are well suited for this task when the relevant functions are differentiable, however, γ^{ideal} and Ψ^{ideal} are generally not differentiable due to the $\min$ construction in (6.10).

To that end, we next present a novel soft-min construction of γ^{ideal} and Ψ^{ideal} which ensures differentiability and allows for incorporating these functions with a CBF-based run time assurance architecture. We first recall the *Log-Sum-Exponential* function

$$\text{LSE}(\mathcal{S}, p) = -\frac{1}{p} \log \sum_{s \in \mathcal{S}} \exp(-p \cdot s) \tag{6.13}$$

where $\mathcal{S} \subset \mathbb{R}$ is a finite set and $p > 0$ is a fixed parameter. The Log-Sum-Exponential has several useful properties: namely, LSE$(\mathcal{S}, p)$ is differentiable with respect to the elements of $\mathcal{S}$, and LSE$(\mathcal{S}, p)$ approximates $\min \mathcal{S}$, *i.e.*,

$$\min \mathcal{S} - \frac{n}{p} \log 2 \leq \text{LSE}(\mathcal{S}, p) < \min \mathcal{S} \tag{6.14}$$

for all $p > 0$, and this approximation can be made arbitrarily tight by choosing p large enough.

For fixed $p > 0$, define now

$$\gamma(t; x) := \text{LSE}(\, \{h(z) \mid z \in \langle\!\langle \Phi^E(t;\, x) \rangle\!\rangle \,\} \,,\, p), \tag{6.15}$$

$$\Psi(x) := \sup_{0 \leq \tau \leq T_\text{b}} \gamma(\tau, x), \tag{6.16}$$

and likewise $S_\Psi := \{x \in \mathcal{X} \mid \Psi(x) \geq 0\}$. Importantly, $\Psi(x)$ is differentiable with

$$\frac{\partial \Psi}{\partial x}(x) = \frac{\partial \gamma}{\partial x}(\tau^*(x), x) \tag{6.17}$$

where $\tau^*(x)$ is the maximizer from (6.16), *i.e.*, $\tau^*(x)$ satisfies $\Psi(x) = \gamma(\tau^*(x), x)$, and this is a result of [106, Theorem 1]. In practice, $\frac{\partial \Psi}{\partial x}(x)$ is computed as follows: First, $\Phi^E(t, x)$ is computed for t in the interval $[0, T_\text{b}]$ via simulation, and the simulated trajectory is used to identify the minimizer $\tau^*(x)$ for (6.16). Next, $\frac{\partial \Phi^E}{\partial x}(\tau^*(x), x)$ is computed numerically; for example, n additional simulations of horizon $\tau^*(x)$ can be used to approximate the n columns of the Jacobian matrix $\frac{\partial \Phi^E}{\partial x}$. Lasty, $\frac{\partial \gamma}{\partial x}(\tau^*(x), x)$ is obtained via the chain rule using prior computations.

Observe that S_Ψ is a strict under-approximation of S_Ψ^ideal, *i.e.*, $S_\Psi \subset S_\Psi^\text{ideal}$. We recall that S_Ψ^ideal is robustly forward invariant for (6.6), however, S_Ψ may not be. Further, S_Ψ may not be robustly

Algorithm 1 Mixed-Monotone-CBF-Based Run Time Assurance Mechanism

input : Desired control policy $\mathbf{u}^{\mathrm{d}} : \mathcal{X} \to \mathbb{R}^m$.
: Current State $x \in \mathcal{X}$.
: Class-$\mathcal{K}$ function $\alpha : \mathbb{R} \to \mathbb{R}$.
output: Assured control input $\mathbf{u}^{\mathrm{ASIF}}(x) \in \mathbb{R}^m$.

function $\mathbf{u}^{\mathrm{ASIF}}(x) =$ASIF($\mathbf{u}^{\mathrm{d}}$, x, α)
Compute:
$u^* = \arg\min_{u \in \mathbb{R}^m} ||u - \mathbf{u}^{\mathrm{d}}(x)||_2^2$
s.t. $\frac{\partial \Psi}{\partial x}(x)(f(x) + g_1(x)u + g_2(x)w) \geq -\alpha(\Psi(x))$
$\forall w \in \langle\!\langle \underline{w}, \overline{w} \rangle\!\rangle$
if Program feasible **then return** u^*
else return $\mathbf{u}^{\mathrm{b}}(x)$

forward invariant under any control policy, even though it is true that if $\Psi(x) \geq 0$ for some x, then applying $\mathbf{u}^{\mathrm{b}}$ will still result in eventually entering S_{b} within horizon T_{b}. This is because it is no longer the case that applying $\mathbf{u}^{\mathrm{b}}$ will keep $\Psi(x)$ from decreasing sometime before x enters S_{b}. Thus, even though a natural barrier-function-based reasoning might lead one to choose an input such that

$$\frac{d\Psi}{dt}(x(t)) \geq -\alpha(\Psi(x(t))) \tag{6.18}$$

for some class-$\mathcal{K}$ function $\alpha : \mathbb{R} \to \mathbb{R}$ for all time, this may not be possible when $\Psi(x)$ is close to zero, and in particular, it may be the case that choosing $\mathbf{u}^{\mathrm{b}}$ violates (6.18). However, due to the fact that $S_\Psi \subset S_\Psi^{\mathrm{ideal}}$, if for some $x \in S_\Psi$ we have that $\mathbf{u}^{\mathrm{b}}$ violates (6.18), then $\mathbf{u}^{\mathrm{b}}$ is safe with respect to x, and thus it is acceptable to immediately switch to the backup control policy to retain safety.

Following the discussion above, we next present an assured controller for nondeterministic control systems of the form (6.1). This controller is presented in Algorithm 1 and control actions are chosen point-wise in time. Letting $\phi^{\mathrm{ASIF}}(t; x, \mathbf{w})$ denote the state transition function of (6.1) when inputs are chosen using Algorithm 1, we now have that For all initial conditions $x \in S_{\mathrm{b}}$ and any Lipschitz continuous controller $\mathbf{u}^{\mathrm{d}} : \mathcal{X} \to \mathbb{R}^m$, the controller $\mathbf{u}^{\mathrm{ASIF}}$ from Algorithm 1 is such that $\Phi^{\mathrm{ASIF}}(T; x, \mathbf{w}) \notin \mathcal{X}_{\mathrm{u}}$ for all $T \geq 0$. We refer the reader to [17] for a more formal proof of this result.

In summary, the assured controller $\mathbf{u}^{\mathrm{ASIF}}$ defined by Algorithm 1 (i) evaluates to the desired control input whenever possible, (ii) allows the system (6.1) to leave the safe region S_{b}, and (iii) ensures the system never enters the unsafe set $\mathcal{X}_{\mathrm{u}}$. Moreover, the optimization problem posed in Algorithm 1 contains only a finite number of affine constraints and, thus, the proposed assured controller can be computationally amenable to real-world applications. We demonstrate this assertion in the next section, where we employ Algorithm 1 to assure safety for a vehicle platoon model.

6.1.3 Numerical Example: Enforcing Inter-Agent Distance Constraints on a Vehicle Platoon

Consider a platoon of 3 vehicles, whose velocity dynamics are given as

$$\dot{x}_i = \beta x_i + a_i + w_i, \tag{6.19}$$

where $x_i \in \mathbb{R}$ denotes the velocity of the i^{th} vehicle, a_i denotes the acceleration of the vehicle, which is controlled, $\beta = -1$ denotes a friction coefficient and $w \in [-0.1, 0.1]^3$ denotes a bounded additive noise term. Control decisions are made after referencing the relative displacements of vehicles in the platoon. In particular, there are two available displacement measures

$$z_1 = x_2 - x_1 \quad \text{and} \quad z_2 = x_3 - x_2, \tag{6.20}$$

so that letting

$$A^{\mathsf{T}} = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}, \tag{6.21}$$

we have $\dot{z} = A^{\mathsf{T}} x$. The platoon dynamics then become

$$\begin{bmatrix} \dot{x} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} \beta I & 0 \\ A^{\mathsf{T}} & 0 \end{bmatrix} \begin{bmatrix} x \\ z \end{bmatrix} - \begin{bmatrix} A \\ 0 \end{bmatrix} \mathbf{u}(z) + \begin{bmatrix} w \\ 0 \end{bmatrix} \tag{6.22}$$

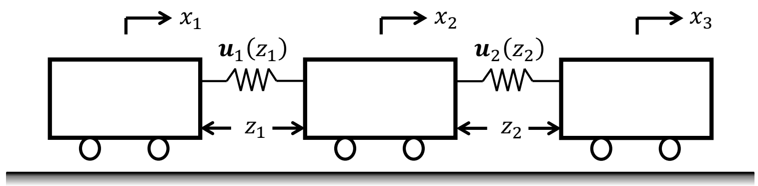


Figure 6.2: Case Study of Section 6.1: Problem setting. $x_1,\ x_2,\ x_3$ are the vehicle velocities, and $z_1,\ z_2$ are the inter-agent distances when connectivity is given by (6.21). The control inputs $\mathbf{u}_1,\ \mathbf{u}_2$ effectively pull (push) the vehicles toward (away from) one another.

with control input $\mathbf{u}(z) = [\,\mathbf{u}_1(z_1),\ \mathbf{u}_2(z_2)\,]^\mathsf{T}$. This problem setting is shown in Figure 6.2.

We aim to enforce inter-agent distance constraints on (6.22) by applying the ASIF controller presented in Algorithm 1. Specifically, we take an unsafe set

$$\mathcal{X}_\mathrm{u} = \left\{(x, z) \in \mathbb{R}^5 \,\middle|\, |z_1| \geq 8 \ \text{ or } \ |z_2| \geq 8\right\}, \tag{6.23}$$

and we ignore vehicle collisions so that z_1, z_2 are allowed to change sign over trajectories of (6.22).

We choose a backup controller

$$\mathbf{u}^\mathrm{b}(z) = (\ \kappa \tanh(\sigma z_1),\ \kappa \tanh(\sigma z_2)\ ), \tag{6.24}$$

with $\kappa = 2$ and $\sigma = \frac{1}{2}$. Roughly speaking, (6.24) acts as two identical nonlinear springs which *pull* the carts together when applied to (6.22); by this description, κ describes the maximum force which the springs apply before saturation, and σ describes the distance at which the springs saturate.

The closed-loop dynamics of (6.22) under $\mathbf{u}^b$ are mixed monotone with respect to

$$d\left(\begin{bmatrix} x \\ z \end{bmatrix},\ w,\ \begin{bmatrix} \widehat{x} \\ \widehat{z} \end{bmatrix},\ \widehat{w}\right) = \begin{bmatrix} \beta x - A^- \mathbf{u}^\mathrm{b}(z) - A^+ \mathbf{u}^\mathrm{b}(\widehat{z}) + w \\ (A^+)^\mathsf{T} x + (A^-)^\mathsf{T} \widehat{x} \end{bmatrix} \tag{6.25}$$

where A^+ and A^- denote the non-negative and and non-positive parts of A, respectively.

To construct a backup region S_b, we consider a local linearization of (6.6) at $(x, z) = 0$. The linearization is asymptotically stable to the origin and is certified by the quadratic Lyapunov function $V(x,z) = (x,z)^\mathsf{T} P(x,z)$ for

$$P = \begin{bmatrix} \kappa\sigma + AA^\mathsf{T} & -\beta A \\ -\beta A^\mathsf{T} & (\kappa^2\sigma^2 + \beta^2)I + \kappa\sigma A^\mathsf{T} A \end{bmatrix}. \tag{6.26}$$

Thus, we consider an invariant safe set

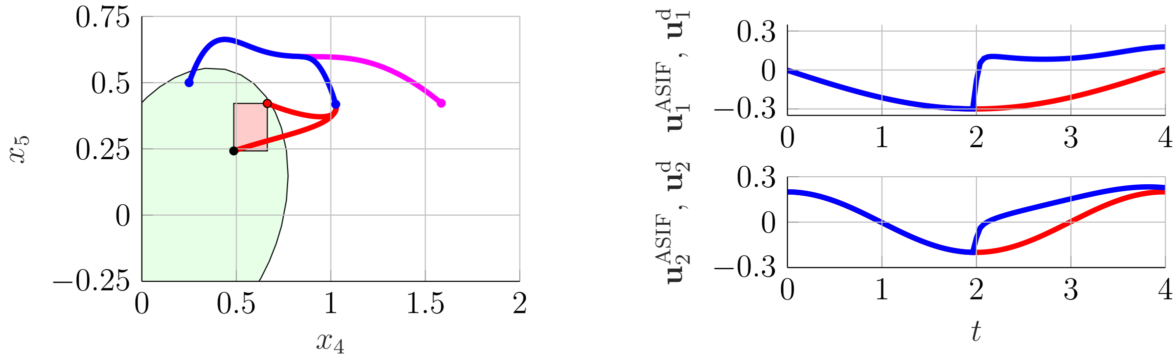
$$S_\mathrm{b} = \{(x,z) \in \mathbb{R}^5 \,|\, V(x,z) \leq \delta\} \tag{6.27}$$

for appropriate $\delta \geq 0$. For the parameters taken in this study, S_b from (6.27) is verified to be robustly forward invariant for the backup dynamics when $\delta = \frac{9}{4}$ and, using an approach whereby backward reachable sets of S_b are over-approximated using Proposition 7, it is additionally shown that $S_\mathrm{b}^+(T_\mathrm{b}) \cap \mathcal{X}_\mathrm{u} = \varnothing$ for $T_\mathrm{b} = 1$.

We construct an ASIF to assure the system (6.22), where we take the backup controller (6.24), safe set (6.27), and backup time $T_\mathrm{b} = 1$. In this case, γ is given by (6.15) where we fix $p = 1000$ and Φ^E is taken in reference to d. Now an assured controller is given by Algorithm 1. For the purpose of this study, we hypothesize an open-loop desired control input

$$\mathbf{u}^\mathrm{d}(t) = \begin{bmatrix} -\frac{3}{10}\sin(\frac{\pi}{4}t) \\ \frac{1}{5}\cos(\frac{\pi}{2}t) \end{bmatrix} \tag{6.28}$$

and simulate the system (6.22) under the ASIF controller Algorithm 1, where we let $\alpha(\psi) = 1000\psi^3$. A 4-second simulation is conducted using MATLAB 2020a and simulation results are provided in Figure 6.3. In the simulation the assured controller $\mathbf{u}^\mathrm{ASIF}$ drives the system (6.22) out of the safe set; however, the system remains in $S_\mathrm{b}^+(1)$ and all points along the system trajectory are safe with respect to $\mathbf{u}^\mathrm{b}$. The code that accompanies this example study, and that generates the figures in this section, is publicly available through the GaTech FACTS Lab Github: `https://github.com/gtfactslab/Abate_CDC2020`.



(a) (b)

Figure 6.3: Case Study of Section 6.1: Employing mixed monotonicity and control barrier functions to enforce safety on the vehicle platoon model (6.22). The vehicles begin with an initial velocity state $x_0 = (-\frac{1}{4}, 0, \frac{1}{2})$ and an initial displacement state $z_0 = (\frac{1}{4}, \frac{1}{2})$. A random disturbance $\mathbf{w} : [0, 4] \to \mathcal{W}$ is also chosen. Subfigures: (a) Cart displacement trajectory on time interval $[0, 4]$. The nominal trajectory $\phi(\,\cdot\,; (x_0, z_0), \mathbf{u}^{\mathrm{d}}, \mathbf{w})$ is shown in pink. The assured trajectory $\phi^{\mathrm{ASIF}}(\,\cdot\,; (x_0, z_0), \mathbf{w})$ is shown in blue. Bounds on the safe backup trajectory are computed via the decomposition function d, and are shown in red. S^{b} is shown in green at time $T = 4$. (b) Control input signals vs. time. The desired control input $\mathbf{u}^{\mathrm{d}}$ from (6.28) is shown in red. The applied input, which is chosen via Algorithm 1, is shown in blue.

6.1.4 Conclusion

This study presents a control barrier function-based run time assurance mechanism for nondeterministic systems, where the nondeterminism in the system model is specifically addressed using mixed monotone reachability methods. The proposed assured controller computes an optimization problem containing only a finite number of affine constraints, and we demonstrate the applicability of our construction through an example pertaining to vehcile platoons.

6.2 Hardware Demonstration for Spacecraft Safety: a Mixed Monotonicity Based Approach

The recent proliferation of commercial and government space missions, particularly in low-Earth orbit, has motivated the need for increased autonomy capabilities for the control of space vehicles. Such advancements in autonomy can save on costs and risks associated with human-in-the-loop operations while improving vehicle reliability and performance.

In this study, we present the development and testing of a run time assurance mechanism for a torque-controlled spacecraft in free rotational motion, subject to a line-of-sight constraint. A nondeterministic dynamical model is considered for the spacecraft, and mixed monotonicity based reachability methods are employed within the control-loop in order to assure safe behavior. Unlike the run time assurance approach presented in Section 6.1, however, where we use control barrier functions together with mixed monotone systems theory in order to ensure the satisfaction of the safety constraint, in this study, we employ a *Simplex Architecture* [93–96]. This approach is employed in order to facilitate the inclusion of actuation constraints within the system's safety specification.

Our proposed algorithm is as follows. We first suppose existence of a backup control policy that is verified *a priori* to render a given subset of the state space robustly forward invariant. Motivated by applications where such subsets are generally conservative, our objective is to allow the system to safely evolve beyond this initial verified subset. To do so, we propose computing an over-approximation of the system's reachable set under the backup control law. This is used to guarantee safety of states outside of the verified subset by proving that the backup controller provides a safe trajectory that returns to the verified subset. Specifically, if the reachable set becomes fully contained within the verified safe subset at some time along the prediction horizon, and it does not intersect with the set of states where the line-of-sight constraint is violated before that time, then a safe return trajectory is ensured. We construct this assurance mechanism in the following way.

We begin by computing a safe backup control policy and corresponding safe subset of the state space. The backup controller is designed to drive trajectories to the backup set while saturating to adhere to input constraints. Consequently, these actuation constraints on the backup controller prevent the explicit knowledge of a large robust forward invariant set *a priori*, further motivating the approach proposed in this study where conservative-but-verified safe subset is coupled with reachable set computations to achieve safety beyond the verified subset.

The practicality of the approach is demonstrated in with an application on a hardware testbed: the Autonomous Spacecraft Testing of Robotic Operations in Space (ASTROS) platform, at the Georgia Institute of Technology. The experimental setup is shown later in Figure 6.4, and a video of the experiment is available at `https://youtu.be/g1-zMepDm1I`. In the experiment, unsafe primary control actions are chosen by a human operator via a joystick, with a controller update rate of 10 Hz. A $t_{\mathrm{p}} = 0.6$ second reachable set computation is conducted under the performance controller, followed by a $t_{\mathrm{b}} = 15$ second reachability computation under the backup controller. Reachable set computations are conducted in 1 ms. Furthermore, when necessary to avoid collisions, the assurance mechanism applies the backup controller to the system in order to guarantee system safety on an infinite time-horizon.

6.2.1 Problem Statement for Obstacle Avoidance Case Study

Our problem setting is similar to that of Section 5.3. We study a rotating rigid body model of a spacecraft

$$\dot{\omega} = J^{-1}(-\omega \times J\omega + u + w) \tag{6.29}$$

where $\omega = (\omega_x, \omega_y, \omega_z) \in \mathbb{R}^3$ is a vector of spacecraft angular rates, $u \in \mathcal{U} \subset \mathbb{R}^3$ is a vector of applied torque inputs, and $w \in \mathcal{W} \subset \mathbb{R}^3$ is a vector of disturbance torques. The set $\mathcal{U}$ incorporates actuation constraints and $\mathcal{W}$ accommodates known disturbance bounds, and we further assume that $\mathcal{U}$ and $\mathcal{W}$ are both hyperrectangles. As was the case in Section 5.3, the components of ω describe the rotation of a body-fixed reference frame $\mathcal{F}_{\mathrm{B}}$ with respect to an inertial frame $\mathcal{F}_{\mathrm{I}}$, and we refer the reader back to Figure 5.4 for a depiction of the frames. Furthermore, the matrix $J \in \mathbb{R}^{3\times 3}$ in (6.29) is the inertia matrix for the spacecraft, which is symmetric and positive-definite.

There are many possible ways to represent the attitude (orientation) dynamics of a rotating body; see [107] for a short review. Indeed, in case study of Section 5.3, we employed a 4-dimensional quaternion vector representation of the spacecraft's attitude. For reasons that will become clear in Section 6.2.3, in this work, we choose a two-parameter representation of the attitude that describes, only, the orientation of the body-fixed $\widehat{k}$-axis with respect to the inertially fixed $\widehat{K}$-axis[1]; this parameterization is derived in [108], and its utility for control design problems is ex-

[1]The general theory posited in this section for parameterizing attitude extends naturally to other orientation definitions, as well, so that one may choose to represent orientation using, *e.g.*, the body-fixed $\widehat{\imath}$-axis and the inertially fixed $\widehat{J}$-axis. Moreover, the particular parameterization used in this work, which uses $\widehat{k}$ and $\widehat{K}$, is chosen without loss of

emplified in [109, 110]. In particular, we describe the spacecraft attitude using $\rho = (\rho_1, \rho_2) \in \mathbb{R}^2$, where the time-evolution of ρ is described by

$$\begin{aligned} \dot{\rho}_1 &= \omega_z \rho_2 + \omega_y \rho_1 \rho_2 + \frac{\omega_x}{2}(1 + \rho_1^2 - \rho_2^2), \\ \dot{\rho}_2 &= -\omega_z \rho_1 + \omega_x \rho_1 \rho_2 + \frac{\omega_y}{2}(1 + \rho_2^2 - \rho_1^2). \end{aligned} \tag{6.30}$$

Following the findings of [108], observe that the *line-of-sight angle* of the spacecraft, which is the angle made between the $\widehat{k}$ and $\widehat{K}$ directions is given by

$$\theta(x) = \arccos\left(\frac{1 - \rho_1^2 - \rho_2^2}{1 + \rho_1^2 + \rho_2^2}\right), \tag{6.31}$$

i.e., $\rho = 0$ when $\widehat{k}$ points in the $\widehat{K}$-direction.

Now, combining the orientation dynamics (6.30) with the rotational velocity dynamics (6.29), we have that the full spacecraft dynamics are given by

$$\begin{bmatrix} \dot{\rho}_1 \\ \dot{\rho}_2 \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} \omega_z \rho_2 + \omega_y \rho_1 \rho_2 + \frac{\omega_x}{2}(1 + \rho_1^2 - \rho_2^2) \\ -\omega_z \rho_1 + \omega_x \rho_1 \rho_2 + \frac{\omega_y}{2}(1 + \rho_2^2 - \rho_1^2) \\ J^{-1}(-\omega \times J\omega + u + w) \end{bmatrix} \tag{6.32}$$

which we hereafter denote as

$$\dot{x} = f(x, u, w) \tag{6.33}$$

with state $x = (\rho, \omega) \subset \mathcal{X} = \mathbb{R}^5$ and where $u \in \mathcal{U} \subset \mathbb{R}^3$ and $w \in \mathcal{W} \subset \mathbb{R}^3$ retain their definitions from (6.29). In the following, we say that a control policy $\mathbf{u} : \mathbb{R} \times \mathcal{X} \to \mathbb{R}^3$ is *admissible on set* $A \subset \mathcal{X}$ when $\mathbf{u}(t; x) \in \mathcal{U}$ for all $x \in A$ and all $t \geq 0$. We denote by $\phi(t; x, \mathbf{u}, \mathbf{w})$ the state of (6.33) reached at time t when beginning from state $x \in \mathcal{X}$ at time 0 and evolving subject to the feedback control input $\mathbf{u}(t; x)$ and the disturbance signal $\mathbf{w}(t)$. The time-t reachable set of (6.33) from A under $\mathbf{u}$ is denoted $R(t; A, \mathbf{u})$, which is the set of states reachable from A at time $t \geq 0$ under some disturbance signal.

generality and serves only for ease of exposition.

Safety for the spacecraft system (6.33) is formalized via a line-of-sight constraint: we say that a state $x \in \mathcal{X}$ is safe when $\theta(x) \leq \theta_{\max}$ where $\theta(x)$ is given by (6.31) and where $\theta_{\max}$ is a parameter describing the maximum allowable line-of-sight angle and which is fixed *a priori*. To assess the safety of states, we employ a safety constraint function

$$\varphi(x) := (1 + \rho_1^2 + \rho_2^2)\left(\cos\left(\theta(x)\right) - \cos\left(\theta_{\max}\right)\right) \tag{6.34}$$

or, equivalently,

$$\varphi(x) := (1 - \cos(\theta_{\max})) - (1 + \cos\left(\theta_{\max}\right))\left(\rho_1^2 + \rho_2^2\right) \tag{6.35}$$

where we observe that $\varphi(x) \geq 0$ only when x is safe and $\varphi(x) < 0$ otherwise. The set of all safe states, *i.e.*, states $x \in \mathcal{X}$ that satisfy $\varphi(x) \geq 0$, is referred to as the *constraint set* and is denoted by

$$\mathcal{C}_{\mathrm{A}} := \{x \in \mathcal{X} \mid \varphi(x) \geq 0\}. \tag{6.36}$$

Thus, the goal of this study to construct a controller $\mathbf{u}$ that ensures $\phi(t; x_0, \mathbf{u}, \mathbf{w}) \in \mathcal{C}_{\mathrm{A}}$ for all time $t \geq 0$ and for all disturbance signals $\mathbf{w} : [0, \infty) \to \mathcal{W}$. A feedback control policy $\mathbf{u}$ is said to be safe for (6.33) when there exists a set A so that A is forward invariant for (6.33) under $\mathbf{u}$ and $A \subseteq \mathcal{C}_{\mathrm{A}}$. Applying $\mathbf{u}$ to (6.33) then ensures $\theta(x) \leq \theta_{\max}$ for all time so long as $x(0) \in A$.

6.2.2 Run Time Assurance Solution

We are interested in designing feedback controllers that ensure the satisfaction of the safety constraint (6.35) along trajectories of (6.33), and we show next how knowledge of a single safe control policy for (6.33) facilitates the online *enforcement* of safety constraints through the use of a run time assurance mechanism. Unlike the run time assurance approach presented in Section 6.1, where we use control barrier functions together with mixed monotone systems theory in order to ensure the satisfaction of the safety constraint, in this study, we employ a *Simplex Architecture* based run time assurance mechanism. Our construction is as follows:

We consider, first, a desired control policy $\mathbf{u}^{\mathrm{d}}(t; x)$ for the system (6.33). The desired controller is assumed to satisfy some performance control objective, but is not directly applicable to (6.33) due to the fact that (i) $\mathbf{u}^{\mathrm{d}}$ may not be safe, *i.e.*, applying $\mathbf{u}^{\mathrm{d}}$ may cause the system to leave $\mathcal{C}_{\mathrm{A}}$, and (ii) $\mathbf{u}^{\mathrm{d}}$ may not be admissible, *i.e.*, there may exist a state $x \in \mathcal{C}_{\mathrm{A}}$ so that $\mathbf{u}^{\mathrm{d}}(t;x) \notin \mathcal{U}$ at some time t. Next, we suppose knowledge of a backup control policy $\mathbf{u}^{\mathrm{b}}(x)$ for (6.33) which is certified safe via an explicitly defined forward invariant set $\mathcal{C}_{\mathrm{b}} \subseteq \mathcal{C}_{\mathrm{A}}$ and is also admissible, *i.e.*, $\mathbf{u}^{\mathrm{b}}(x) \in \mathcal{U}$ for all $x \in \mathcal{X}$. Applying $\mathbf{u}^{\mathrm{b}}(x)$ to (6.33) now ensures that state trajectories remain in $\mathcal{C}_{\mathrm{b}} \subseteq \mathcal{C}_{\mathrm{A}}$ and guarantees system safety for all time. However, applying such a backup controller may not be preferable; backup controllers are typically designed without considering performance objectives and may be the case that, *e.g.*, $\mathcal{C}_{\mathrm{b}}$ is too small to allow for satisfaction of performance criteria.

To address the limitations of the backup controller, the RTA will select as its output either $\mathbf{u}^{\mathrm{d}}(t,x_0)$ or $\mathbf{u}^{\mathrm{b}}(x_0)$, depending on whether $\mathbf{u}^{\mathrm{d}}(t;x_0)$ is safe. To determine whether it is safe to apply $\mathbf{u}^{\mathrm{d}}(t;x_0)$, at each timestep, the RTA computes an over-approximation of the system's reachable set $\mathcal{X}_{\mathrm{p}} \supseteq R(t_{\mathrm{des}};x_0,\mathbf{u}^{\mathrm{d}})$ for some constant $t_{\mathrm{des}} > 0$. Next, the RTA computes an over-approximation under the backup controller $\mathcal{X}_{\mathrm{b}} \supseteq R(t_{\mathrm{b}};\mathcal{X}_{\mathrm{p}},\mathbf{u}^{\mathrm{b}})$ at discrete time steps over a finite time-horizon. We let the notation X_k^{b} refer to $\mathcal{X}_{\mathrm{b}}$ evaluated at the k^{th} timestep and let k^* denote the number of points in the horizon. In the special instance where $\varphi(x) \geq 0$ for all $x \in \mathcal{X}_k^{\mathrm{b}}$ with $k \in \{1,\cdots,k^*\}$ and $\mathcal{X}_{k^*}^{\mathrm{b}} \subseteq \mathcal{C}_{\mathrm{b}}$, the desired input is allowed to pass to the system unaltered. If, instead, the above constraints are not met, the backup controller is applied to the system. In this way the RTA acts to *filter* the desired control input online, and this approach guarantees system safety while also ensuring that the desired control input is passed to the system when it is safe to do so. A second benefit of this approach, as we shall see later, is that it allows system trajectories leave the backup set $\mathcal{C}_{\mathrm{b}}$ when it is verified online that the current system state can return to $\mathcal{C}_{\mathrm{b}}$ on a finite time-horizon. In this way, employing an RTA mechanism eases the task of computing a large forward invariant set $\mathcal{C}_{\mathrm{b}}$ a priori and offloads computation to online reachability analysis.

6.2.3 Computing a Robustly Forward Invariant Safe Set and Backup Controller

In this section, we construct a stabilizing backup control policy for the spacecraft system (6.33), and we compute an associated safe forward invariant set.

Our choice of controller is by hypothesis. We consider

$$\mathbf{u}^{\mathrm{b}}(x) = \sigma(\omega \times J\omega + Kx) \tag{6.37}$$

where $K \in \mathbb{R}^{3\times 5}$ is the controller gain matrix and where $\sigma : \mathbb{R}^3 \to \mathbb{R}^3$ is an saturation function that is understood to apply componentwise. Observe that when input saturation is not present, so that, *e.g.*, $\sigma(u) = u$, the controller posited in (6.37) linearizes on the closed-loop rotational velocity dynamics so that, in this case, $\dot{\omega} = J^{-1}Kx + w$. Regardless, hardware limitations generally make it so that actuator constraints cannot be avoided in real-world control system design, and in this study we consider a *hard-clamping* saturation function, given by

$$\sigma_i(u_i) = \begin{cases} \overline{u}_i & \text{if } u_i \geq \overline{u}_i, \\ u_i & \text{if } u_i \in [\underline{u}_i, \overline{u}_i], \\ \underline{u}_i & \text{if } u_i \leq \underline{u}_i, \end{cases} \tag{6.38}$$

for $\mathcal{U} = [\underline{u}, \overline{u}]$. We denote by

$$\dot{x} = F(x, w) = f(x, u^{\mathrm{b}}(x), w) \tag{6.39}$$

the closed loop dynamics of (6.33) under the backup control policy (6.37).

To identify a suitable controller gain matrix K and invariant safe set $\mathcal{C}_{\mathrm{b}}$, we employ a sum-of-squares optimization problem. We consider the control law (6.37) and, based on hardware constraints of the ASTROS platform, we choose an an inertia matrix $J = \left[\begin{smallmatrix} 17.5 & -0.8 & 0.3 \\ -0.8 & 14.9 & 0.4 \\ 0.3 & 0.4 & 20.8 \end{smallmatrix}\right] \mathrm{kg\,m^2}$, an admissible set $\mathcal{U} = [-2.0, 2.0] \times [-0.8, 0.8]^2$ N m, and a disturbance space $\mathcal{W} = [-0.02, 0.02]^3$ N m.

Via the optimization problem, we identify a suitable controller gain matrix

$$K = 10^{-2} \times \begin{bmatrix} 100.0 & -0.4 & 467.3 & 3.5 & -1.4 \\ 0.3 & 70.6 & 5.1 & 330.8 & 4.2 \\ 1.4 & -5.9 & 4.0 & -20.0 & 99.8 \end{bmatrix} \tag{6.40}$$

and a safe set

$$\mathcal{C}_{\mathrm{b}} := \{x \in \mathcal{X} \,|\, \gamma - x^{\mathsf{T}} P x \geq 0\} \tag{6.41}$$

for

$$P = \begin{bmatrix} 20.0 & 2.1 & 6.5 & 1.1 & -1.5 \\ 2.1 & 26.7 & 1.1 & 10.0 & -2.4 \\ 6.5 & 1.1 & 323.3 & 17.6 & -2.8 \\ 1.1 & 10.0 & 17.6 & 378.5 & -4.4 \\ -1.5 & -2.4 & -2.8 & -4.4 & 288.1 \end{bmatrix} \quad \text{and} \quad \gamma = 17.1. \tag{6.42}$$

In particular, we show that $\mathcal{C}_{\mathrm{b}}$ is a robustly forward invariant for the closed-loop backup dynamics (6.39), and we show also that $\varphi(x) \geq 0$ for all $x \in \mathcal{C}_{\mathrm{b}}$, *i.e.*, $\mathcal{C}_{\mathrm{b}} \subset \mathcal{C}_{\mathrm{A}}$. Thus, we have arrived at a suitable backup control policy and robustly forward invariant safe set. We refer the reader also to [44], where the parameters provided in this section are derived in greater detail.

6.2.4 Constructing a Decomposition Function for the Closed-Loop Backup Dynamics

The next step in the construction of the RTA mechanism involves computing a decomposition function for the closed-loop backup dynamics in (6.39). Our approach in this matter is similar that of Section 5.3, where individual decomposition functions are constructed for the attitude and rotational velocity subsystems and then combined to form a decomposition function for the interconnected system using Proposition 6.

As before, we consider a linear transformation on the rotational velocity dynamics, $\Omega := J\omega$, so that the closed-loop backup dynamics become

$$\begin{bmatrix} \dot{\rho}_1 \\ \dot{\rho}_2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(1+\rho_1^2-\rho_2^2) & \rho_1\rho_2 & \rho_2 \\ \rho_1\rho_2 & \frac{1}{2}(1+\rho_2^2-\rho_1^2) & -\rho_1 \end{bmatrix} J^{-1}\Omega \tag{6.43}$$

$$\dot{\Omega} = -\, J^{-1}\Omega \times \Omega + \mathbf{u}^{\mathrm{b}}(x) + w \tag{6.44}$$

$$\mathbf{u}^{\mathrm{b}}(x) := \sigma\left(J^{-1}\Omega \times \Omega + K \begin{bmatrix} I_2 & 0 \\ 0 & J^{-1} \end{bmatrix} \begin{bmatrix} \rho \\ \Omega \end{bmatrix} \right) \tag{6.45}$$

Tight decomposition functions are constructed for the individual subsystems in (6.43) and (6.44), and a tight inclusion function is constructed for the control input mapping in (6.45). These functions are then used to form a decomposition for the 5-dimensional composite system using Proposition 6. Hereafter, we denote by d the decomposition formed for (6.43)–(6.45) and we denote by Φ^E the state transition function of the resulting embedding system when $\mathcal{W} = [-0.02, 0.02]^3$ Newton-Meters.

At each time step, the RTA developed in this study will apply Proposition 10 with d in order to attain a parallelotope over-approximation of the reachable set of (6.33). First, the RTA computes a t_{des}-second simulation of the embedding system of (6.43)–(6.43), where the backup control input in (6.45) is replaced by knowledge of the human operator's desired control action. Next, the RTA computes an over-approximation under the backup controller at discrete time-steps over a finite time-horizon $[t_{\mathrm{des}}, t_{\mathrm{des}} + t_{\mathrm{p}}]$. The reachable set approximations derived in this step are then applied within the RTA mechanism in two main ways:

First, we check that there exists a time $t \in [0, t_{\mathrm{des}} + t_{\mathrm{b}}]$ so that the reachable set approximation $[\![\Phi^E(t; x_0)]\!]$ is contained completely within the safe region $\mathcal{C}_{\mathrm{b}}$. This step is achieved using an inclusion function for $h(x) := \gamma - x^{\mathsf{T}} P x$. In particular, we define by

$$H(t; x_0) := \min\left\{ \gamma - x^{\mathsf{T}} \left[\begin{smallmatrix} I_2 & 0 \\ 0 & J^{-1} \end{smallmatrix}\right] P \left[\begin{smallmatrix} I_2 & 0 \\ 0 & J^{-1} \end{smallmatrix}\right] x \,\middle|\, x \in \langle\!\langle \Phi^E(t; x_0) \rangle\!\rangle \right\} \tag{6.46}$$

the minimum valuation of $h(x)$ over the t-second reachable set approximation $[\![\Phi^E(t;x)]\!]$. When the system is at state $x = (\rho, \Omega)$ at some time, the RTA computes $H(t;x)$ for all $t \in [0, t_{\text{des}} + t_{\text{b}}]$. In the instance where there does not exists a $t \in [0, t_{\text{des}} + t_{\text{b}}]$ so that $H(t;x) \geq 0$, the backup control input is applied to the system, since in this instance, it cannot be verified that it will be possible to return to the safe region $\mathcal{C}_{\text{b}}$ after the human operator's input is applied. In the other case, where there exists a time t_{k^*} with $H(t_{k^*};x) \geq 0$, we store t_{k^*} for further computations within the RTA.

Indeed, while the existence of a t_{k^*} with $H(t_{k^*};x) \geq 0$ guarantees that is it always possible to reach the safe region $\mathcal{C}_{\text{b}}$ after the human operator's input is applied, this condition does not ensure that the system will not violate the safety constraint before entering $\mathcal{C}_{\text{b}}$. To that end, we apply the mixed monotonicity result in a second way, where we now ensure that $\varphi(x) \geq 0$ holds for future states on $[0, t_{k^*}]$. For this step, we use an inclusion function for φ, so that when

$$\Xi(t_{k^*}; x_0) := \min_{\tau \in [0, t_{k^*}]} \left\{ \varphi(x) \,\middle|\, x \in [\![\Phi^E(t; x_0)]\!] \right\} \geq 0 \tag{6.47}$$

holds, we also have that x will not leave $\mathcal{C}_{\text{A}}$ on the time-horizon $[0, t_{k^*}]$ when the human operator's suggested input is applied. This procedure ensures that the system violates the safety constraint, *i.e.*, $\phi(x) \geq 0$ holds for future states on $[0, t_{k^*}]$. Furthermore, in the instance where (6.47) holds, the desired input $\mathbf{u}_{\text{des}}$ is applied to the system; otherwise, the backup control input $\mathbf{u}_{\text{b}}$ is applied. We provide an pseudocode implementation of the RTA mechanism developed in this section as Algorithm 2.

6.2.5 Hardware Demonstration on the Georgia Tech ASTROS Testbed

We demonstrate the proposed framework for assured safety with a real-world experiment on the Autonomous Spacecraft Testing of Robotic Operations in Space (ASTROS) platform at the Georgia Institute of Technology. The spacecraft is controlled with 12 pressurized air thrusters, arranged in a 3-3-3-3 configuration, and a linear program is used to allocate the desired control torque to the thrusters. The experiments are conducted with an admissible control set $\mathcal{U}$ =

Algorithm 2 Mixed-Monotonicity-Based Simplex Architecture for Spacecraft Systems

input : Desired control policy $\mathbf{u}^{\mathrm{d}} : \mathcal{X} \to \mathbb{R}^m$.
: Current State $x \in \mathcal{X}$.
: Class-$\mathcal{K}$ function $\alpha : \mathbb{R} \to \mathbb{R}$.
output: Assured control input $\mathbf{u}^{\mathrm{RTA}}(x) \in \mathbb{R}^m$.

function $\mathbf{u}^{\mathrm{RTA}}(x)$ =RTA($\mathbf{u}^{\mathrm{d}}$, $x,\ \alpha$)
  Compute: $\Phi^E(t; x_0)$ on $t \in [0, t_{\mathrm{des}} + t_{\mathrm{b}}]$, where
  $\mathbf{u}^{\mathrm{d}}$ is applied for the first t_{des} seconds, and where
  $\mathbf{u}^{\mathrm{b}}$ is applied for the remaining t_{b} seconds.

  Compute: $H(t; x_0)$ for all $t \in [0, t_{\mathrm{des}} + t_{\mathrm{b}}]$
  if $\nexists\, t \in [0, t_{\mathrm{des}} + t_{\mathrm{b}}]$ s.t. $H(t; x_0) \geq 0$ **then return** $\mathbf{u}^{\mathrm{b}}(x)$
  else $t_{k^*} \leftarrow t$ s.t. $H(t; x_0) \geq 0$

  Compute: $\Xi(t_{k^*}; x_0)$
  if $\Xi(t_{k^*}; x_0) \geq 0$ **then return** $\mathbf{u}^{\mathrm{d}}(x)$
  else return $\mathbf{u}^{\mathrm{b}}(x)$

$[-2.0, 2.0] \times [-0.8, 0.8]^2$ Nm and considers disturbance torques in $\mathcal{W} = [-0.02, 0.02]^3$ Nm.

In the experiment, a 5 degree avoid cone is considered ($\theta_{\max} = 175$ degrees). As shown in Figure 6.4, the avoid cone is constructed in such a way that prevents an onboard laser from entering a ring placed approximately 18 feet away from the vehicle's center of rotation. The desired control input to the vehicle is provided by a human-controlled pilot joystick. The user attempts to orient the vehicle in such a way that the laser enters the ring, however, the RTA mechanism is effective at preventing the safety constraint from being violated. That is, the user has full control of the vehicle when the RTA is inactive, and the RTA activates only as necessary to prevent violations of the line-of-sight constraint (6.35).

Numerical data from the experiment is provided in Figure 6.5. Observe that while the human operator suggests unsafe control actions via the joystick, the RTA mechanism applies the backup controller, when necessary, in order to ensure the satisfaction of the safety constraint for all time. A video of the experiment also available at `https://youtu.be/g1-zMepDm1I`.

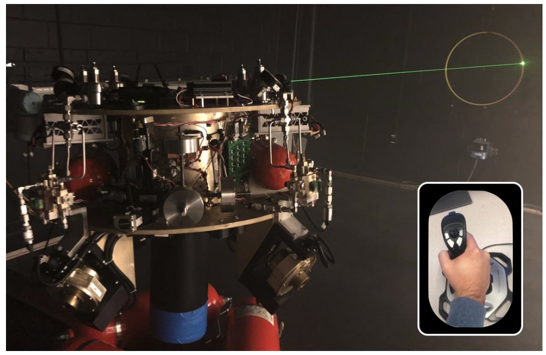
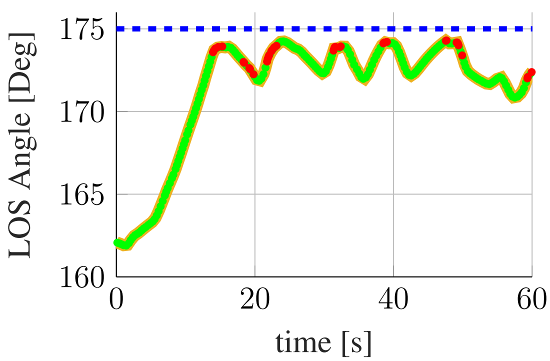
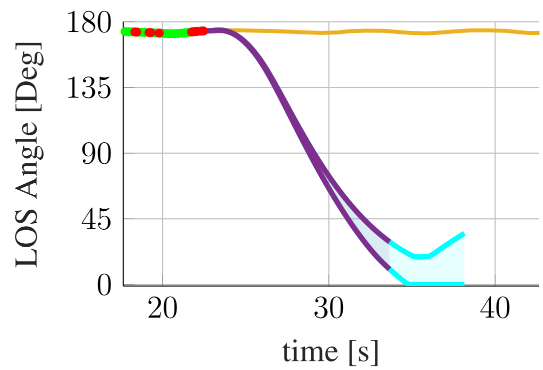


Figure 6.4: Case Study of Section 6.2: ASTROS testbed and experimental setup. The inertially-fixed $\widehat{K}$ vector is chosen to point toward a ring, with the border of the ring describing the extent of the unsafe set. A lazer-pointer is fixed to the body-fixed $\widehat{k}$ direction, so that the laser touches the ring when $\theta(x) = 175°$. Control actions are suggested by a human operator via a joystick.



(a)



(b)

Figure 6.5: Case Study of Section 6.2: Hardware demonstration. A mixed monotonicity based run time assurance mechanism is demonstrated on the ASTROS testbed. Subfigures: (a) Experimental Data: Line-of-sight (LOS) angle versus time. Green indicates time iterations that are unfiltered and red indicates times when the RTA filter is active. The extent of the admissible set, $\theta_{\max} = 175°$, is shown dashed in blue. (b) In-the loop reachability analysis using Mixed Monotonicity: At time $t = 22.5$ seconds, the backup controller is applied due to a violation of the safety constraint. The $t_{\mathrm{p}} + t_{\mathrm{b}} = 15.6$ second reachable set prediction is shown in light blue. If the backup controller is applied, the system is guaranteed to reenter the backup region $\mathcal{C}_{\mathrm{b}}$ in 11 seconds, as shown in purple.

Appendices

APPENDIX A

DECOMPOSITION FUNCTIONS FOR TRIGONOMETRIC SYSTEMS

In this section, we tabulate many tight decomposition functions in closed-form for continuous time dynamical systems defined by trigonometric vector fields. Sample implementations of each of the decomposition functions constructed here are available in code through the GitHub repository accompanying this document: `https://github.com/gtfactslab/Abate_Thesis`. Further, the theory provided in this section can be easily adapted, through the results of Chapter 3, in order to construct, *e.g.*, decomposition functions for discrete-time systems with trigonometric update maps or inclusion functions for trigonometric maps.

The system

$$\dot{x} = \sin(w) \tag{A.1}$$

with is mixed monotone with a tight decomposition function given in closed form by

$$d^{\sin}(w, \widehat{w}) := \begin{cases} \sin(w) & \text{if } (\cos(w),\, \cos(\widehat{w})) \succeq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \sin(\widehat{w}) & \text{if } (\cos(w),\, \cos(\widehat{w})) \preceq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \text{sign}(w - \widehat{w}) & \text{if } |w - \widehat{w}| \geq 2\pi, \\ \text{sign}(w - \widehat{w}) & \text{if } \cos(w) \leq 0 \leq \cos(\widehat{w}) \text{ and } |w - \widehat{w}| \leq 2\pi, \\ \text{sign}(w - \widehat{w}) & \text{if } \cos(w)\cos(\widehat{w}) \geq 0 \text{ and } \pi \leq |w - \widehat{w}| \leq 2\pi, \\ \min\{\sin(w), \sin(\widehat{w})\} & \text{if } w \leq \widehat{w} \text{ and } \cos(w) \geq 0 \geq \cos(\widehat{w}), \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi, \\ \max\{\sin(w), \sin(\widehat{w})\} & \text{if } w \geq \widehat{w} \text{ and } \cos(w) \geq 0 \geq \cos(\widehat{w}) \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi. \end{cases} \tag{A.2}$$

Moreover, since $\cos(w) = \sin(w + \frac{\pi}{2})$, the tight decomposition function for

$$\dot{x} = \cos(w) \tag{A.3}$$

is given by

$$d^{\cos}(w, \widehat{w}) := d^{\sin}\left(w + \frac{\pi}{2}, \widehat{w} + \frac{\pi}{2}\right), \tag{A.4}$$

or, equivalently,

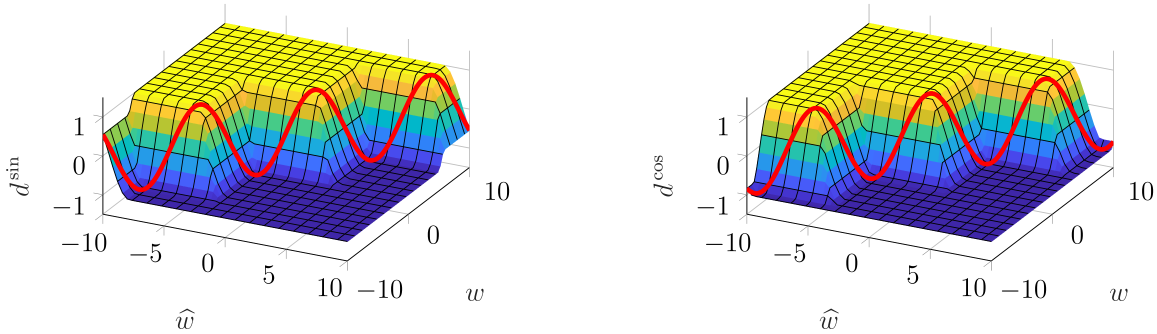
$$d^{\cos}(w, \widehat{w}) := \begin{cases} \cos(w) & \text{if } (\sin(w),\, \sin(\widehat{w})) \preceq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \cos(\widehat{w}) & \text{if } (\sin(w),\, \sin(\widehat{w})) \succeq 0 \text{ and } |w - \widehat{w}| \leq \pi, \\ \text{sign}(w - \widehat{w}) & \text{if } |w - \widehat{w}| \geq 2\pi \\ \text{sign}(w - \widehat{w}) & \text{if } \sin(w) \geq 0 \geq \sin(\widehat{w}) \text{ and } |w - \widehat{w}| \leq 2\pi, \\ \text{sign}(w - \widehat{w}) & \text{if } \sin(w)\sin(\widehat{w}) \geq 0 \text{ and } \pi \leq |w - \widehat{w}| \leq 2\pi, \\ \min\{\cos(w), \cos(\widehat{w})\} & \text{if } w \leq \widehat{w} \text{ and } \sin(w) \leq 0 \leq \sin(\widehat{w}) \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi, \\ \max\{\cos(w), \cos(\widehat{w})\} & \text{if } w \geq \widehat{w} \text{ and } \sin(w) \leq 0 \leq \sin(\widehat{w}) \\ & \quad \text{and } |w - \widehat{w}| \leq 2\pi. \end{cases} \tag{A.5}$$

We show $d^{\sin}$ and $d^{\cos}$ graphically in Figure A.1, and additional tight decomposition functions for trigonometric systems are provided Table A.1.

Note that the results of Chapter 3 can now easily be applied to compute decomposition functions for systems defined by scaled and shifted trigonometric functions. For example

$$\dot{x} = -\sin(w) \tag{A.6}$$

with $x \in \mathbb{R}$ and $w \in \mathbb{R}$ is mixed monotone with respect to $d^{-\sin}(w, \widehat{w}) = -d^{\sin}(\widehat{w}, w)$, and



(a) $d^{\sin}(w, \widehat{w})$ (b) $d^{\cos}(w, \widehat{w})$

Figure A.1: The tight decomposition functions $d^{\sin}(w, \widehat{w})$ and $d^{\cos}(w, \widehat{w})$ are plotted above the w–$\widehat{w}$ plane. The evaluations of $\sin(w)$ and $\cos(w)$ are plotted on the diagonal (w, w) in red.

decomposition functions for similar systems are provided in Table A.2. In Table A.2, we allow a_1, a_2 and a_3 to represent be functions of x so that, *e.g.*, $a_1 = g_1(x), a_2 = g_2(x)$ and $a_3 = g_3(x)$, and in this case the system

$$\dot{x} = g_1(x) \sin(g_2(x) w + g_3(x)) \tag{A.7}$$

is mixed monotone with a tight decomposition function given in closed form by

$$d^{g_1(x) \sin(g_2(x) w + g_3(x))}(x, w, \widehat{x}, \widehat{w}) := d^{a_1 \sin(a_2 w + a_3)}(w, \widehat{w}). \tag{A.8}$$

The results above for scaled and shifted trigonometric systems can also be applied to compute decomposition functions for systems defined by the product of trigonometric functions. For example, applying $\sin(w)\cos(w) = \frac{1}{2}\sin(2w)$ we find that the system

$$\dot{x} = \sin(w) \cos(w) \tag{A.9}$$

with $x \in \mathbb{R}$ and $w \in \mathbb{R}$ is mixed monotone with a tight decomposition function given in closed form by

$$d^{\sin\cos}(w, \widehat{w}) = d^{\frac{1}{2}\sin(2w)}(w, \widehat{w}) \tag{A.10}$$

and additional systems are considered in Table A.3.

Table A.1: Tight decomposition functions for common trigonometric systems.

System	Domain	Tight Decomp.
$\dot{x} = \sin(w)$	$w \in \mathbb{R}$	$d^{\sin}(w, \widehat{w})$ given by (A.2)
$\dot{x} = \cos(w)$	$w \in \mathbb{R}$	$d^{\cos}(w, \widehat{w})$ given by (A.5), also (3.60)
$\dot{x} = \tan(w)$	$w \in (\frac{\pi}{2}, \frac{\pi}{2})$	$d^{\tan}(w, \widehat{w}) = \tan(w)$
$\dot{x} = \arcsin(w)$	$w \in [-1, 1]$	$d^{\arcsin}(w, \widehat{w}) = \arcsin(w)$
$\dot{x} = \arccos(w)$	$w \in [-1, 1]$	$d^{\arccos}(w, \widehat{w}) = \arccos(\widehat{w})$
$\dot{x} = \arctan(w)$	$w \in \mathbb{R}$	$d^{\arctan}(w, \widehat{w}) = \arctan(w)$
$\dot{x} = \sinh(w)$	$w \in \mathbb{R}$	$d^{\sinh}(w, \widehat{w}) = \sinh(w)$
$\dot{x} = \cosh(w)$	$w \in \mathbb{R}$	$d^{\cosh}(w, \widehat{w}) = \begin{cases} \cosh(w) & \text{if } w \geq \max\{0, -\widehat{w}\}, \\ \cosh(\widehat{w}) & \text{if } \widehat{w} \leq \min\{0, -w\}, \\ 1 & \text{if } w \leq 0 \leq \widehat{w}. \end{cases}$
$\dot{x} = \tanh(w)$	$w \in \mathbb{R}$	$d^{\tanh}(w, \widehat{w}) = \tanh(w)$
$\dot{x} = \sin(w) + w$	$w \in \mathbb{R}$	$d^{\sin(w)+w}(w, \widehat{w}) = \sin(w) + w$
$\dot{x} = \cos(w) + w$	$w \in \mathbb{R}$	$d^{\cos(w)+w}(w, \widehat{w}) = \cos(w) + w$
$\dot{x} = \tan(w) - w$	$w \in (\frac{\pi}{2}, \frac{\pi}{2})$	$d^{\tan(w)-w}(w, \widehat{w}) = \tan(w) - w$

We next study systems $\dot{x} = F(x, w)$ with $x \in \mathbb{R}$ and input vector $w \in \mathcal{W} \subseteq \mathbb{R}^m$. Consider first

$$\dot{x} = \sin(w_1 + w_2) \tag{A.11}$$

with $w \in \mathbb{R}^2$. To form a tight decomposition function $d^{\sin(w_1+w_2)}$, observe that

$$d^{\sin(w_1+w_2)}(w, \widehat{w}) = d^{\sin}(w_1 + w_2, \widehat{w}_1 + \widehat{w}_2). \tag{A.12}$$

It follows by consequence that for vector $a \in \mathbb{R}^{1\times m}$, the system

$$\dot{x} = \sin(aw) \tag{A.13}$$

with $x \in \mathbb{R}$ and $w \in \mathbb{R}^m$ is mixed monotone with a tight decomposition function given in closed

Table A.2: Tight decomposition functions scaled and shifted trigonometric systems.

System	Domain	Tight Decomp.
$\dot{x} = -\sin(w)$	$w \in \mathbb{R}$	$d^{-\sin}(w, \widehat{w}) = -d^{\sin}(\widehat{w}, w)$
$\dot{x} = -\cos(w)$	$w \in \mathbb{R}$	$d^{-\cos}(w, \widehat{w}) = -d^{\cos}(\widehat{w}, w)$
$\dot{x} = -\tan(w)$	$w \in (-\frac{\pi}{2}, \frac{\pi}{2})$	$d^{-\tan}(w, \widehat{w}) = -\tan(\widehat{w})$
$\dot{x} = a_1 \sin(a_2 w + a_3)$	$w \in \mathbb{R}$	$d^{a_1 \sin(a_2 w + a_3)}(w, \widehat{w}) = \begin{cases} a_1 d^{\sin}(a_2 w + a_3, a_2 \widehat{w} + a_3) & \text{if } a_1 a_2 \geq 0 \\ a_1 d^{\sin}(a_2 \widehat{w} + a_3, a_2 w + a_3) & \text{if } a_1 a_2 < 0 \end{cases}$
$\dot{x} = a_1 \cos(a_2 w + a_3)$	$w \in \mathbb{R}$	$d^{a_1 \cos(a_2 w + a_3)}(w, \widehat{w}) = \begin{cases} a_1 d^{\cos}(a_2 w + a_3, a_2 \widehat{w} + a_3) & \text{if } a_1 a_2 \geq 0 \\ a_1 d^{\cos}(a_2 \widehat{w} + a_3, a_2 w + a_3) & \text{if } a_1 a_2 < 0 \end{cases}$
$\dot{x} = a_1 \tan(a_2 w + a_3)$	$w \in [\frac{-\pi - 2a_3}{2a_2}, \frac{\pi - 2a_3}{2a_2}]$ if $a_2 > 0$ $w \in [\frac{\pi - 2a_3}{2a_2}, \frac{-\pi - 2a_3}{2a_2}]$ if $a_2 < 0$ $w \in \mathbb{R}$ if $a_2 = 0$	$d^{a_1 \tan(a_2 w + a_3)}(w, \widehat{w}) = \begin{cases} a_1 \tan(a_2 w + a_3) & \text{if } a_1 a_2 \geq 0 \\ a_1 \tan(a_2 \widehat{w} + a_3) & \text{if } a_1 a_2 < 0 \end{cases}$

Table A.3: Tight decomposition functions for systems defined by products of trigonometric functions.

System	Domain	Tight Decomp.
$\dot{x} = \sin(w)\cos(w)$	$w \in \mathbb{R}$	$d^{\sin\cos}(w, \widehat{w}) = d^{\frac{1}{2}\sin(2w)}(w, \widehat{w})$
$\dot{x} = \sin(w)^2$	$w \in \mathbb{R}$	$d^{\sin^2}(w, \widehat{w}) = \frac{1}{2} + d^{-\frac{1}{2}\cos(2w)}(w, \widehat{w})$
$\dot{x} = \cos(w)^2$	$w \in \mathbb{R}$	$d^{\cos^2}(w, \widehat{w}) = \frac{1}{2} + d^{\frac{1}{2}\cos(2w)}(w, \widehat{w})$
$\dot{x} = \sin(w)^{a_1}$	$w \in \mathbb{R}$ $a_1 \in \mathbb{N}$	$d^{\sin^{a_1}}(w, \widehat{w}) = \begin{cases} d^{\sin}(w, \widehat{w})^n & \text{if } a_1 \text{ odd} \\ d^{\sin^2}(w, \widehat{w})^{\frac{n}{2}} & \text{if } a_1 \text{ even.} \end{cases}$
$\dot{x} = \sin(w)^{a_1}$	$w \in (0, \pi)$ $a_1 \in \mathbb{R}$	$d^{\sin^{a_1}}(w, \widehat{w}) = \begin{cases} d^{\sin}(w, \widehat{w})^{a_1} & \text{if } a_1 \geq 0 \\ d^{\sin}(\widehat{w}, w)^{a_1} & \text{if } a_1 < 0. \end{cases}$
$\dot{x} = \cos(w)^{a_1}$	$w \in \mathbb{R}$ $a_1 \in \mathbb{N}$	$d^{\cos^{a_1}}(w, \widehat{w}) = \begin{cases} d^{\cos}(w, \widehat{w})^n & \text{if } a_1 \text{ odd} \\ d^{\cos^2}(w, \widehat{w})^{\frac{n}{2}} & \text{if } a_1 \text{ even.} \end{cases}$
$\dot{x} = \cos(w)^{a_1}$	$w \in (0, \pi)$ $a_1 \in \mathbb{R}$	$d^{\cos^{a_1}}(w, \widehat{w}) = \begin{cases} d^{\cos}(w, \widehat{w})^{a_1} & \text{if } a_1 \geq 0 \\ d^{\cos}(\widehat{w}, w)^{a_1} & \text{if } a_1 < 0. \end{cases}$

form by

$$d^{\sin(aw)}(w, \widehat{w}) = d^{\sin}(a^+ w + a^- \widehat{w}, a^- w + a^+ \widehat{w}) \tag{A.14}$$

where $a^+, a^- \in \mathbb{R}^{1\times m}$ denote the positive and negative parts of a, respectively.

Consider now

$$\dot{x} = w_1 \sin(w_2) \tag{A.15}$$

with $w \in \mathbb{R}^2$, and recall

$$d^{w_1 w_2}(w, \widehat{w}) = \begin{cases} \min\{w_1 w_2,\ \widehat{w}_1 w_2,\ w_1 \widehat{w}_2,\ \widehat{w}_1 \widehat{w}_2\} & \text{if } w \preceq \widehat{w} \\ \max\{w_1 w_2,\ \widehat{w}_1 w_2,\ w_1 \widehat{w}_2,\ \widehat{w}_1 \widehat{w}_2\} & \text{if } \widehat{w} \preceq w. \end{cases} \tag{A.16}$$

Now a tight decomposition function for $\dot{x} = w_1 \sin(w_2)$ is given by

$$d^{w_1 \sin(w_2)}(w, \widehat{w}) = d^{w_1 w_2}\left(\begin{bmatrix} w_1 \\ d^{\sin}(w_2, \widehat{w}_2) \end{bmatrix}, \begin{bmatrix} \widehat{w}_1 \\ d^{\sin}(\widehat{w}_2, w_2) \end{bmatrix} \right), \tag{A.17}$$

and, using a symmetric argument, a tight decomposition function for

$$\dot{x} = w_1 \cos(w_2) \tag{A.18}$$

is given by

$$d^{w_1 \cos(w_2)}(w, \widehat{w}) = d^{w_1 w_2}\left(\begin{bmatrix} w_1 \\ d^{\cos}(w_2, \widehat{w}_2) \end{bmatrix}, \begin{bmatrix} \widehat{w}_1 \\ d^{\cos}(\widehat{w}_2, w_2) \end{bmatrix} \right). \tag{A.19}$$

In a similar way, observe that the system

$$\dot{x} = w_1(\sin(w_2) + w_2) \tag{A.20}$$

Table A.4: Tight decomposition functions for trigonometric systems with vector inputs.

System	Domain	Decomp.
$\dot{x} = \sin(w_1 + w_2)$	$w \in \mathbb{R}^2$	$d^{\sin(w_1+w_2)}(w, \widehat{w}) = d^{\sin}(w_1 + w_2, \widehat{w}_1 + \widehat{w}_2)$
$\dot{x} = \cos(w_1 + w_2)$	$w \in \mathbb{R}^2$	$d^{\cos(w_1+w_2)}(w, \widehat{w}) = d^{\cos}(w_1 + w_2, \widehat{w}_1 + \widehat{w}_2)$
$\dot{x} = \sin(aw)$	$w \in \mathbb{R}^m$ $a \in \mathbb{R}^{1\times m}$	$d^{\sin(aw)}(w, \widehat{w}) = d^{\sin}(a^+w + a^-\widehat{w}, a^-w + a^+\widehat{w})$
$\dot{x} = \cos(aw)$	$w \in \mathbb{R}^m$ $a \in \mathbb{R}^{1\times m}$	$d^{\cos(aw)}(w, \widehat{w}) = d^{\cos}(a^+w + a^-\widehat{w}, a^-w + a^+\widehat{w})$
$\dot{x} = w_1(\sin(w_2) + w_2)$	$w \in \mathbb{R}^2$	$d^{w_1(\sin(w_2)+w_2)}(w, \widehat{w})$ given by (A.21)
$\dot{x} = w_1(\cos(w_2) + w_2)$	$w \in \mathbb{R}^2$	$d^{w_1(\cos(w_2)+w_2)}(w, \widehat{w})$ given by (A.23)
$\dot{x} = w_1 \sin(w_2)$	$w \in \mathbb{R}^2$	$d^{w_1 \sin(w_2)}(w, \widehat{w})$ given by (A.17)
$\dot{x} = w_1 \cos(w_2)$	$w \in \mathbb{R}^2$	$d^{w_1 \cos(w_2)}(w, \widehat{w})$ given by (A.19)

is mixed monotone with a tight decomposition function given by

$$d^{w_1(\sin(w_2)+w_2)}(w, \widehat{w}) = \begin{cases} \min\{\, z_1(\sin(z_2) + z_2) \mid z \in \langle w, \widehat{w}\rangle\} & \text{if } w \preceq \widehat{w}, \\ \max\{z_1(\sin(z_2) + z_2) \mid z \in \langle \widehat{w}, w\rangle\} & \text{if } \widehat{w} \preceq w, \end{cases} \tag{A.21}$$

and the system

$$\dot{x} = w_1(\cos(w_2) + w_2) \tag{A.22}$$

is mixed monotone with a tight decomposition function given by

$$d^{w_1(\cos(w_2)+w_2)}(w, \widehat{w}) = \begin{cases} \min\{\, z_1(\cos(z_2) + z_2) \mid z \in \langle w, \widehat{w}\rangle\} & \text{if } w \preceq \widehat{w} \\ \max\{z_1(\cos(z_2) + z_2) \mid z \in \langle \widehat{w}, w\rangle & \text{if } \widehat{w} \preceq w. \end{cases} \tag{A.23}$$

The previous results and tight decomposition functions are collected in Table A.4.

APPENDIX B

SOLUTIONS TO EXERCISES

Problem 2.1: The time-1 reachable set of (2.66) is exactly equal to

$$R(1;A) = [\phi(1;10), \phi(1;15)] = [3.68, 5.52], \tag{B.1}$$

and this is because the true reachable set is a hyperrectangle. See Lemmas 7 and 8.

To show that (2.66) is mixed monotone with respect to d^1, d^2, and d^3, it is enough to show that $d^i(x,x) = -x$ and $\frac{\partial d^i}{\partial \widehat{x}}(x,\widehat{x}) \leq 0$ for all $x, \widehat{x}$ and for all $i \in \{1,2,3\}$.

The embedding system with respect to $d^1(x,\widehat{x}) = -x$ admits a stable equilibrium at $(x,\widehat{x}) = (0,0)$ and is given by

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ \widehat{x} \end{bmatrix}. \tag{B.2}$$

The embedding system with respect to $d^2(x,\widehat{x}) = -\widehat{x}$ admits an unstable equilibrium at $(x,\widehat{x}) = (0,0)$ and is given by

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ \widehat{x} \end{bmatrix}. \tag{B.3}$$

Thus, the reachable set approximations derived from the application of Proposition 2 with d^1 tend to *shrink* with time, whereas the reachable set approximations derived from the application of Proposition 2 with d^2 tend to *grow* with time.

The embedding system with respect to $d^3(x,\widehat{x}) = -\frac{1}{2}x - \frac{1}{2}\widehat{x}$ is given by

$$\begin{bmatrix} \dot{x} \\ \dot{\widehat{x}} \end{bmatrix} = \begin{bmatrix} -1/2 & -1/2 \\ -1/2 & -1/2 \end{bmatrix} \begin{bmatrix} x \\ \widehat{x} \end{bmatrix}, \tag{B.4}$$

where we observe that $\dot{x} = \dot{\widehat{x}}$, always in (B.4), and additionally the dynamics matrix $\overline{A} = \left[\begin{smallmatrix} -1/2 & -1/2 \\ -1/2 & -1/2 \end{smallmatrix}\right]$ is singular. Thus, reachable set approximations derived (B.4) will *stay the same size*, in the sense that the side-lengths of the approximation will be equal to the side-lengths of in the initial set of interest, and this is true for any horizon time.

Problem 2.2: The function d from (2.67) *is* a decomposition function for the 2-dimensional linear time-invariant system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} -2 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 4 \\ 0 \end{bmatrix} w, \tag{B.5}$$

as studied previously in Example 4. Observe that d from (2.67) leads to overly-conservative reachable set approximations, however, and excess conservatism can be attributed to the fact that the resulting embedding system dynamics matrix $\overline{A}$ admits larger eigenvalues—larger than in Example 4.

Problem 2.3: The system (2.68) is mixed monotone with respect to

$$\begin{aligned} d_1(x, \widehat{x}) &= x_1^3 + x_2 \\ d_2(x, \widehat{x}) &= \begin{cases} -\widehat{x}_1^2 & \text{if } \widehat{x}_1 \geq 0 \text{ and } \widehat{x}_1 \geq -x_1, \\ -x_1^2 & \text{if } x_1 \leq 0 \text{ and } \widehat{x}_1 < -x_1, \\ -x_1\widehat{x}_1 & \text{if } \widehat{x}_1 < 0 \text{ and } x_1 > 0. \end{cases} \end{aligned} \tag{B.6}$$

Consider the extended hyperrectangular subset

$$\begin{aligned} \mathcal{X}' &:= \{x \in \mathbb{R}^2 \,|\, x_1 \geq 0\} \\ &= [0, \infty] \times [-\infty, \infty] \\ &= \overline{\mathbb{R}}_{\geq 0} \times \overline{\mathbb{R}}. \end{aligned} \tag{B.7}$$

Since it is true that $\frac{\partial F}{\partial x}(x)$ is Metzler always for (2.68) on $\mathcal{X}'$, we also have that (2.68) is a monotone system on this subregion of the statespace.

Problem 3.1: To show that $\dot{x} = F(x, w)$ is mixed monotone with respect to

$$d(x, w, \widehat{x}, \widehat{w}) := \alpha d^1(x, w, \widehat{x}, \widehat{w}) + (1 - \alpha)d^2(x, w, \widehat{x}, \widehat{w}), \tag{B.8}$$

for decomposition functions d^1, d^2 and $\alpha \in [0, 1]$, it is enough to show that $d(x, w, x, w) = F(x, w)$ and that d satisfies the remaining derivative conditions in Definition 6.

Problem 3.2: For any $A \in \mathbb{R}^{m\times p}$, the tightest hyperrectangle containing the image

$$\{y \in \mathbb{R}^m \,|\, y = Ax, x \in [\underline{x}, \overline{x}]\} \tag{B.9}$$

is given by $[\underline{y}, \overline{y}] \subset \mathbb{R}^m$, where $\underline{y}, \overline{y}$ are given by

$$\begin{bmatrix} \underline{y} \\ \overline{y} \end{bmatrix} := \begin{bmatrix} A^+ & A^- \\ A^- & A^+ \end{bmatrix} \begin{bmatrix} \underline{x} \\ \overline{x} \end{bmatrix}. \tag{B.10}$$

Problem 3.3: See [45] and [46].

Problem 4.1: Assume that, for all i, F_i does not depend on x_i. If $d^F(x, w, \widehat{x}, \widehat{w})$ is the tight decomposition function for $\dot{x} = F(x, w)$, then

$$d^{-F}(x, w, \widehat{x}, \widehat{w}) := -d^F(\widehat{x}, \widehat{w}, x, w) \tag{B.11}$$

is the tight decomposition function for the backward-time dynamics, $\dot{x} = -F(x, w)$. In this instance, also, observe that an equilibrium point $(x_{\text{eq}}, \widehat{x}_{\text{eq}})$ for *any* of the four embedding system formulations in Section 4.1.3 will be an equilibrium for *all* of these systems, and this is true since,

$$d^F(x_{\mathrm{eq}}, \underline{w}, \widehat{x}_{\mathrm{eq}}, \overline{w}) = d^F(\widehat{x}_{\mathrm{eq}}, \overline{w}, x_{\mathrm{eq}}, \underline{w}) = 0. \tag{B.12}$$

Thus, in the instance where $(x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}) \in \mathcal{T}$, we have that the hyperrectangular set $[x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ is robustly forward invariant for $\dot{x} = F(x, w)$ and, further, the complement $\mathbb{R}^n \backslash [x_{\mathrm{eq}}, \widehat{x}_{\mathrm{eq}}]$ is a robustly forward invariant set, as well.

REFERENCES

[1] Peter Goldreich and Stanton J Peale. "The dynamics of planetary rotations". In: *Annual Review of Astronomy and Astrophysics* 6.1 (1968), pp. 287–320.

[2] Wang Sang Koon et al. "Dynamical systems, the three-body problem and space mission design". In: *Equadiff 99: (In 2 Volumes)*. World Scientific, 2000, pp. 1167–1181.

[3] Bin Ran and David Boyce. *Modeling dynamic transportation networks: an intelligent transportation system oriented approach*. Springer Science & Business Media, 2012.

[4] Edward N Lorenz. *Empirical orthogonal functions and statistical weather prediction*. Vol. 1. Massachusetts Institute of Technology, Department of Meteorology Cambridge, 1956.

[5] Edward N Lorenz. "Nondeterministic theories of climatic change". In: *Quaternary Research* 6.4 (1976), pp. 495–506.

[6] Oliver Porges et al. "Reachability and capability analysis for manipulation tasks". In: *ROBOT2013: First Iberian robotics conference*. Springer. 2014, pp. 703–718.

[7] Andrew Singletary et al. "Online Active Safety for Robotic Manipulators". In: *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 2019, pp. 173–178.

[8] Thomas Gurriet. "Applied safety critical control". PhD thesis. California Institute of Technology, 2020.

[9] Athanasios C Antoulas. *Approximation of large-scale dynamical systems*. SIAM, 2005.

[10] Josef Honerkamp. *Stochastic dynamical systems: concepts, numerical methods, data analysis*. John Wiley & Sons, 1996.

[11] Arjan J Van Der Schaft and Johannes Maria Schumacher. *An introduction to hybrid dynamical systems*. Vol. 251. Springer London, 2000.

[12] Arjan Schaft and Hans Schumacher. *An introduction to hybrid dynamical systems*. 2000.

[13] Somil Bansal et al. "Hamilton-jacobi reachability: A brief overview and recent advances". In: *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE. 2017, pp. 2242–2253.

[14] William S Levine. *The Control Systems Handbook: Control System Advanced Methods*. CRC press, 2010.

[15] Maxence Dutreix and Samuel Coogan. “Specification-Guided Verification and Abstraction Refinement of Mixed Monotone Stochastic Systems”. In: *IEEE Transactions on Automatic Control* 66.7 (2021), pp. 2975–2990.

[16] Calin Belta, Boyan Yordanov, and Ebru Aydin Gol. *Formal methods for discrete-time dynamical systems*. Vol. 15. Springer, 2017.

[17] M. Abate and S. Coogan. “Enforcing Safety at Runtime for Systems with Disturbances”. In: *2020 59th IEEE Conference on Decision and Control (CDC)*. 2020, pp. 2038–2043.

[18] Alexander B Kurzhanski and Pravin Varaiya. “Ellipsoidal techniques for reachability analysis”. In: *International workshop on hybrid systems: Computation and control*. Springer. 2000, pp. 202–214.

[19] John Maidens and Murat Arcak. “Reachability analysis of nonlinear systems using matrix measures”. In: *IEEE Transactions on Automatic Control* 60.1 (2014), pp. 265–270.

[20] Pierre-Jean Meyer, Alex Devonport, and Murat Arcak. *Interval Reachability Analysis: Bounding Trajectories of Uncertain Systems with Boxes for Control and Verification*. Springer, 2021.

[21] H.L. Smith. *Monotone Dynamical Systems: An Introduction to the Theory of Competitive and Cooperative Systems*. Mathematical surveys and monographs. American Mathematical Society, 2008. ISBN: 9780821844878.

[22] D. Angeli and E. D. Sontag. “Monotone control systems”. In: *IEEE Transactions on Automatic Control* 48.10 (Oct. 2003), pp. 1684–1698.

[23] J Schröder. “Fehlerabschätzungen bei linearen Gleichungssystemen mit dem Brouwerschen Fixpunktssatz”. In: *Arch Rat Mech Anal* 3 (1959), pp. 28–44.

[24] Jean-Luc Gouzé. “A criterion of global convergence to equilibrium for differential systems. application to Lotka-Volterra systems”. PhD thesis. INRIA, 1988.

[25] JL Gouzé and KP Hadeler. “Monotone flows and order intervals”. In: *Nonlinear World* 1 (1994), pp. 23–34.

[26] H. L. Smith. “The Discrete Dynamics of Monotonically Decomposable Maps”. In: *Journal of Mathematical Biology* 53.4 (May 2006), p. 747.

[27] G.A. Enciso, H.L. Smith, and E.D. Sontag. “Nonmonotone systems decomposable into monotone systems with negative feedback”. In: *Journal of Differential Equations* 224.1 (2006), pp. 205 –227.

[28] David Angeli, Germán A. Enciso, and Eduardo D. Sontag. "A small-gain result for orthant-monotone systems under mixed feedback". In: *Systems & Control Letters* 68 (2014), pp. 9 –19.

[29] Samuel Coogan and Murat Arcak. "Efficient finite abstraction of mixed monotone systems". In: *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*. 2015, pp. 58–67.

[30] S. Coogan. "Mixed Monotonicity for Reachability and Safety in Dynamical Systems". In: *2020 59th IEEE Conference on Decision and Control (CDC)*. 2020, pp. 5074–5085.

[31] L. Yang, O. Mickelin, and N. Ozay. "On Sufficient Conditions for Mixed Monotonicity". In: *IEEE Transactions on Automatic Control* 64.12 (Dec. 2019), pp. 5080–5085.

[32] Samuel Coogan and Murat Arcak. "Stability of Traffic Flow Networks with a Polytree Topology". In: *Automatica* 66.C (Apr. 2016), pp. 246–253.

[33] P. Meyer and D. V. Dimarogonas. "Hierarchical Decomposition of LTL Synthesis Problem for Nonlinear Control Systems". In: *IEEE Transactions on Automatic Control* 64.11 (Nov. 2019), pp. 4676–4683.

[34] Pierre-Jean Meyer, Alex Devonport, and Murat Arcak. "TIRA: Toolbox for Interval Reachability Analysis". In: *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*. HSCC '19. An extended version of this work appears on ArXive https://arxiv.org/abs/1902.05204. Montreal, Quebec, Canada: Association for Computing Machinery, 2019, 224–229. ISBN: 9781450362825.

[35] Matthew Abate and Samuel Coogan. "Computing Robustly Forward Invariant Sets for Mixed-Monotone Systems". In: *2020 59th IEEE Conference on Decision and Control (CDC)*. 2020, pp. 4553–4559.

[36] Matthew Abate and Samuel Coogan. "Robustly Forward Invariant Sets for Mixed-Monotone Systems". In: *IEEE Transactions on Automatic Control* (2022). to appear.

[37] HL Smith. "Global stability for mixed monotone systems". In: *Journal of Difference Equations and Applications* 14.10-11 (2008), pp. 1159–1164.

[38] Tianguang Chu and Lin Huang. "Mixed monotone decomposition of dynamical systems with application". In: *Chinese Science Bulletin* 43.14 (July 1998), pp. 1171–1175.

[39] M. Dutreix and S. Coogan. "Efficient Verification for Stochastic Mixed Monotone Systems". In: *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. Apr. 2018, pp. 150–161.

[40] Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. "Verification and Control for Finite-Time Safety of Stochastic Systems via Barrier Functions". In: *2019 IEEE Conference on Control Technology and Applications (CCTA)*. Aug. 2019, pp. 712–717.

[41] Matthew Abate, Maxence Dutreix, and Samuel Coogan. "Tight Decomposition Functions for Continuous-Time Mixed-Monotone Systems With Disturbances". In: *IEEE Control Systems Letters* 5.1 (2021), pp. 139–144.

[42] Matthew Abate and Samuel Coogan. "Decomposition Functions for Interconnected Mixed Monotone Systems". In: *IEEE Control Systems Letters* 6 (2022), pp. 2120–2125.

[43] Matthew Abate and Samuel Coogan. "Improving the Fidelity of Mixed-Monotone Reachable Set Approximations via State Transformations". In: *2021 American Control Conference (ACC)*. 2021, pp. 4674–4679.

[44] Matthew Abate et al. *Run Time Assurance for Spacecraft Attitude Control Under Nondeterministic Assumptions*. In submission. 2022.

[45] Saber Jafarpour et al. "Robustness Certificates for Implicit Neural Networks: A Mixed Monotone Contractive Approach". In: *4th Annual Learning for Dynamics & Control Conference (L4DC)*. To appear. 2022.

[46] Alexander Davydov et al. "Comparative Analysis of Interval Reachability for Robust Implicit and Feedforward Neural Networks". In: *2022 IEEE 61st Conference on Decision and Control (CDC)*. To appear. 2022.

[47] Christian Llanes, Matthew Abate, and Samuel Coogan. "Safety from in-the-loop reachability for cyber-physical systems". In: *2021 Workshop on Computation-Aware Algorithmic Design for Cyber-Physical Systems (CAADCPS)*. CPS-IoT week. 2021.

[48] Christian Llanes, Matthew Abate, and Samuel Coogan. "Safety from Fast, In-the-Loop Reachability with Application to UAVs". In: in submission. 2021.

[49] Matthew Abate et al. "Verification and runtime assurance for dynamical systems with uncertainty". In: *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*. 2021, pp. 1–10.

[50] Michael E Cao, Matthieu Bloch, and Samuel Coogan. "Estimating High Probability Reachable Sets using Gaussian Processes". In: *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE. 2021, pp. 3881–3886.

[51] Michael E Cao, Matthieu Bloch, and Samuel Coogan. *Efficient Learning of Hyperrectangular Invariant Sets using Gaussian Processes*. In submission. 2022.

[52] Pierre-Jean Meyer. *Reachability analysis of neural networks using mixed monotonicity*. 2021. arXiv: `2111.07683 [eess.SY]`.

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

[54] Mohammad Khajenejad and Sze Zheng Yong. *Tight Remainder-Form Decomposition Functions with Applications to Constrained Reachability and Interval Observer Design*. 2021. arXiv: `2103.08638 [math.OC]`.

[55] Liren Yang and Necmiye Ozay. "Tight decomposition functions for mixed monotonicity". In: *2019 IEEE 58th Conference on Decision and Control (CDC)*. 2019, pp. 5318–5322.

[56] Kerianne Hobbs et al. "Run Time Assurance for Safety-Critical Systems: An Introduction to Safety Filtering Approaches for Complex Control Systems". In: *arXiv preprint arXiv:2110.03506* (2021).

[57] A. D. Ames et al. "Control Barrier Functions: Theory and Applications". In: *2019 18th European Control Conference*. 2019, pp. 3420–3431.

[58] Panagiotis Tsiotras. "ASTROS: a 5DOF experimental platform for research in spacecraft proximity operations". In: Georgia Institute of Technology. 2014.

[59] Lorenzo Farina and Sergio Rinaldi. *Positive linear systems: theory and applications*. Vol. 50. John Wiley & Sons, 2000.

[60] Germán A Enciso and Eduardo D Sontag. "Global attractivity, I/O monotone small-gain theorems, and biological delay systems". In: *Discrete & Continuous Dynamical Systems* 14.3 (2006), p. 549.

[61] Hassan K Khalil and Jessy W Grizzle. *Nonlinear systems*. Vol. 3. Prentice hall Upper Saddle River, NJ, 2002.

[62] Mohit Srinivasan, Cesar Santoyo, and Samuel Coogan. "Continuous Reachability Task Transition Using Control Barrier Functions". In: *IFAC-PapersOnLine* 53.2 (2020). 21th IFAC World Congress, pp. 9696–9701.

[63] Parasara Sridhar Duggirala and Mahesh Viswanathan. "Parsimonious, simulation based verification of linear systems". In: *Computer Aided Verification - 28th International Conference, CAV 2016, Proceedings*. Springer-Verlag Berlin Heidelberg, Jan. 2016, pp. 477–494.

[64] Francesco Bullo. *Lectures on network systems*. Kindle Direct Publishing, 2020.

[65] Kai Shen, Dillard L. Robertson, and Joseph K. Scott. "Tight reachability bounds for constrained nonlinear systems using mean value differential inequalities". In: *Automatica* 134 (2021), p. 109911.

[66] Luc Jaulin et al. "Applied interval analysis". In: Springer, 2001.

[67] N.S. Nedialkov, K.R. Jackson, and G.F. Corliss. "Validated solutions of initial value problems for ordinary differential equations". In: *Applied Mathematics and Computation* 105.1 (1999), pp. 21–68.

[68] Kai Shen and Joseph K Scott. "Rapid and accurate reachability analysis for nonlinear dynamic systems by exploiting model redundancy". In: *Computers & Chemical Engineering* 106 (2017), pp. 596–608.

[69] Alexander Davydov, Saber Jafarpour, and Francesco Bullo. *Non-Euclidean Contraction Theory for Robust Nonlinear Stability*. 2021.

[70] M. Althoff. "An Introduction to CORA 2015". In: *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*. 2015, 120–151.

[71] M. Althoff and D. Grebenyuk. "Implementation of Interval Arithmetic in CORA 2016". In: *Proc. of the 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems*. 2016, pp. 91–105.

[72] M. Althoff, D. Grebenyuk, and N. Kochdumper. "Implementation of Taylor Models in CORA 2018". In: *Proc. of the 5th International Workshop on Applied Verification for Continuous and Hybrid Systems*. 2018.

[73] Eduardo D Sontag. "Contractive systems with inputs". In: *Perspectives in mathematical system theory, control, and signal processing*. Springer, 2010, pp. 217–228.

[74] Mathukumalli Vidyasagar. *Nonlinear systems analysis*. SIAM, 2002.

[75] Charles A Desoer and Mathukumalli Vidyasagar. *Feedback systems: input-output properties*. SIAM, 2009.

[76] Samuel Coogan. "Separability of Lyapunov functions for contractive monotone systems". In: *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE. 2016, pp. 2184–2189.

[77] Jason Kong et al. "Kinematic and dynamic vehicle models for autonomous driving control design". In: *2015 IEEE Intelligent Vehicles Symposium (IV)*. 2015, pp. 1094–1099.

[78] Morris W Hirsch. "Differential equations and convergence almost everywhere in strongly monotone semiflows". In: *Contemp. Math* 17 (1983), pp. 267–285.

[79] A. D. Ames et al. “Control Barrier Function Based Quadratic Programs for Safety Critical Systems”. In: *IEEE Transactions on Automatic Control* 62.8 (2017), pp. 3861–3876.

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

[81] Franco Blanchini. “Set invariance in control”. In: *Automatica* 35.11 (1999), pp. 1747–1767.

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

[83] Alberto Isidori. *Nonlinear control systems: an introduction*. Springer, 1985.

[84] Julian Lowell Coolidge. “The origin of polar coordinates”. In: *The American Mathematical Monthly* 59.2 (1952), pp. 78–85.

[85] Ian R Manchester. “Transverse dynamics and regions of stability for nonlinear hybrid limit cycles”. In: *IFAC Proceedings Volumes* 44.1 (2011), pp. 6285–6290.

[86] John Guckenheimer and Philip Holmes. *Nonlinear oscillations, dynamical systems, and bifurcations of vector fields*. Vol. 42. Springer Science & Business Media, 2013.

[87] Arthur J Krener and Alberto Isidori. “Linearization by output injection and nonlinear observers”. In: *Systems & Control Letters* 3.1 (1983), pp. 47–52.

[88] László Lovász and Alexander Schrijver. “Cones of matrices and set-functions and 0–1 optimization”. In: *SIAM journal on optimization* 1.2 (1991), pp. 166–190.

[89] Hanif D Sherali and Warren P Adams. “A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems”. In: *SIAM Journal on Discrete Mathematics* 3.3 (1990), pp. 411–430.

[90] Mark Leo Mote. “Optimization-based Approaches to Safety-Critical Control with Applications to Space Systems”. PhD thesis. Georgia Institute of Technology, 2021.

[91] Kerianne L Hobbs. “Elicitation and Formal Specification of Run Time Assurance Requirements for Aerospace Collision Avoidance Systems”. PhD thesis. Georgia Institute of Technology, 2020.

[92] Urs Borrmann et al. “Natural Motion-based Trajectories for Automatic Spacecraft Proximity Operation Collision Avoidance”. In: *IFAC-PapersOnLine* 48.27 (2015), pp. 68–73.

[93] Jose G Rivera et al. *An Architectural Description of the Simplex Architecture.* Tech. rep. Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA, 1996.

[94] Danbing Seto et al. "The Simplex architecture for safe online control system upgrades". In: *Proceedings of the 1998 American Control Conference. ACC (IEEE Cat. No. 98CH36207).* Vol. 6. IEEE. 1998, pp. 3504–3508.

[95] Usama Mehmood et al. "Safe CPS from Unsafe Controllers". In: *arXiv preprint arXiv:2102.12981* (2021).

[96] Olatunde Sanni et al. *Ariadne: A common-sense thread for enabling provable safety in air mobility systems with unreliable components*. 2021.

[97] Stephen Prajna. "Barrier certificates for nonlinear model validation". In: *Automatica* 42.1 (2006), pp. 117–126.

[98] A. D. Ames et al. "Control Barrier Function Based Quadratic Programs for Safety Critical Systems". In: *IEEE Transactions on Automatic Control* 62.8 (2017), pp. 3861–3876.

[99] M. Abate, E. Feron, and S. Coogan. "Monitor-Based Runtime Assurance for Temporal Logic Specifications". In: *2019 IEEE 58th Conference on Decision and Control (CDC)*. 2019, pp. 1997–2002.

[100] T. Gurriet et al. "An Online Approach to Active Set Invariance". In: *2018 IEEE Conference on Decision and Control (CDC)*. 2018, pp. 3592–3599.

[101] T. Gurriet et al. "A Scalable Controlled Set Invariance Framework with Practical Safety Guarantees". In: *2019 IEEE 58th Conference on Decision and Control (CDC)*. 2019, pp. 2046–2053.

[102] Tom Schouwenaars. "Safe trajectory planning of autonomous vehicles". PhD thesis. Massachusetts Institute of Technology, 2006.

[103] Stanley Bak et al. "The system-level simplex architecture for improved real-time embedded system safety". In: *2009 15th IEEE Real-Time and Embedded Technology and Applications Symposium*. IEEE. 2009, pp. 99–107.

[104] Andrew Singletary et al. "Onboard safety guarantees for racing drones: High-speed geofencing with control barrier functions". In: *IEEE Robotics and Automation Letters* (2022).

[105] Andrew Singletary et al. *Safety-Critical Manipulation for Collision-Free Food Preparation*. 2022.

[106] William Hogan. "Directional derivatives for extremal-value functions with applications to the completely convex case". In: *Operations Research* 21.1 (1973), pp. 188–209.

[107] Malcolm D Shuster et al. "A survey of attitude representations". In: *Navigation* 8.9 (1993), pp. 439–517.

[108] Panagiotis Tsiotras and James M Longuski. "A new parameterization of the attitude kinematics". In: *Journal of the Astronautical Sciences* 43.3 (1995), pp. 243–262.

[109] Panagiotis Tsiotras, Martin Corless, and JM Longuski. "A novel approach to the attitude control of axisymmetric spacecraft". In: *Automatica* 31.8 (1995), pp. 1099–1112.

[110] John Matthew Brewer and Panagiotis Tsiotras. "Partial attitude synchronization for networks of underactuated spacecraft". In: *Automatica* 97 (2018), pp. 27–37.

VITA

Matthew C. L. Abate received a B.A. degree in engineering sciences and music from Dartmouth College, Hanover, NH, USA, in 2017. He received a B.E. degree in mechanical engineering from the same institution, also in 2017. He received a M.S. degree in mechanical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2018, as well as a M.S. degree in electrical and computer engineering in 2020. Also from Georgia Tech, he received a Ph.D. degree in robotics in 2022, where his graduate research was advised by Professors Samuel Coogan and Eric Feron. His research interest is in the area of safety and verification for dynamical systems with disturbances.

Easy are Theses

by Matt Abate, 2022

Easy are theses I thought. I thought wrong. I thought
o · · o · · o · · o · ·

theses were easy to write. Now I long for the
o · · o · · o · · o · ·

night where I'm not in a fight with myself as to
o · · o · · o · · o · ·

whether each letter I wrote I wrote right.
o · · o · · o · · o