UNIVERSITY OF CALIFORNIA, SAN DIEGO

Control, Planning, and Learning with Control Barrier Functions in Safety-Critical Systems

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mechanical and Aerospace Engineering

by

Pol Mestres

Committee in charge:

Professor Jorge Cortés, Chair
Professor Miroslav Krstić
Professor Sylvia Herbert
Professor Nikolay Atanasov

2025

The dissertation of Pol Mestres is approved, and it is acceptable in quality and form for publication on microfilm:

_____

_____

_____

_____

_____

Chair

University of California, San Diego

2025

DEDICATION

To my parents.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Professor Jorge Cortés for all of his support during the last five years. I first met Jorge in the Fall of 2019, when he kindly accepted to host me in his group to do my Bachelor's Thesis. His guidance and mentorship were formidable since the beginning, and that is one of the reasons why I decided to do my Ph.D in his research group. During these last five years, Jorge has spent a countless amount of hours providing me with valuable research insights, and more importantly helping me grow as a researcher. Throughout the years, Jorge has made sure I make the most out of my Ph.D experience, and provided me with opportunities (such as the participation on multiple conferences, research internships, and collaborations) that I will cherish for the rest of my career. In short, this dissertation would not have been possible without him. I will be forever grateful for his trust and support and I hope to have a chance to work with him again in the future.

I would also like to thank my dissertation committee members, Prof. Miroslav Krstić, Prof. Sylvia Herbert, and Prof. Nikolay Atanasov, for taking time out of their schedules and providing me with suggestions and criticisms. Besides serving in my committee, they have all been role models throughout my PhD.

UCSD is a unique place to do a Ph.D in control theory. On the one hand, the Center for Control Systems and Dynamics gathers an exceptional group of faculty members with expertise on all areas of control theory, from whom I have learned a lot through courses, informal interactions, and seminar series. On the other hand, the affiliation with the Contextual Robotics Institute has greatly exposed me a with the world of robotics, and it has shaped a lot of the research projects I have pursued throughout my Ph.D.

Doing a Ph.D at UCSD would not have been possible without the support of the *Centre de Formació Interdisciplinària Superior* (CFIS) at the Universitat Politècnica de Catalunya, my alma matter. CFIS funded my undergraduate studies and provided me with the financial support to first come to the UCSD for my Bachelor's Thesis. Besides that, CFIS provided me with an exceptional education in Mathematics and Engineering that have been the backbone of my Ph.D. It also

allowed me to connect with many exceptional people, with whom I am still lucky to be friends to this day.

I would also like to extend my gratitude to the Robotics Branch of the Army Research Laboratory (ARL) for hosting me during the summers of 2023 and 2024 for two research internships, which have helped me apply my research to more practical robotics problems. In particular, I would like to thank Dr. Carlos Nieto-Granda for being my mentor at ARL. I am very grateful for his patience and dedication in teaching me the ins and outs of ROS and helping me out in hardware experiments.

Throughout my Ph.D I have been fortunate to collaborate with a lot of outstanding researchers, from whom I have learned a lot. I would like to thank Prof. Nikolay Atanasov, Prof. Emiliano Dall'anese, Prof. Maurice Heemels, Prof. Eduardo Sontag, Prof. Melvin Leok, Kehan Long, Dr. Ahmed Allibhoy, Dr. Carlos Nieto-Granda (again), Yiting Chen, Dr. Giannis Delimpaltadakis, and Arnau Marzabal. I have enjoyed every single collaboration with all of you.

I would also like to thank the members of the joint research group of Prof. Jorge Cortés and Prof. Sonia Martínez for the countless lunches, coffee breaks, and casual chats about research and life in general. I especially thank Jaap Eising, Dhruv Shah, Mohammed Alyaseen, Ahmed Allibhoy, Scott Brown, Scott Addams, Azra Begzadic, Michael McCreesh, Paul Lathrop, Nirabhra Mandal, Neilabh Banzal, Steven Nguyen, Arnau Marzabal, Aleix Salvador, Guillem Pascual, Ana Pons, Javier Gallardo, Steven Nguyen, Mattia Bianchi, and Tomasso Menara. A special thanks goes to Pio, who has also been helpful in landing my next job as a postdoctoral scholar at Caltech.

My friends Sander Tonkens, Nick Hansen, Pau Batlle, Tomàs Ortega, and Guillem Ramírez have been incredibly valuable throughout all these years. Of course, a huge thanks goes to Talia for all the time we have spent together and for always being a source of joy.

Finally, I am extremely grateful to my parents for shaping me to be who I am today and supporting me in all of my decisions, even if they were $10,000$ km away from home.

The research reported in this dissertation was supported in part by the National Science Foundation awards IIS-2007141, and CECS-1947050, as well as the Army Research Laboratory award ARL-W911NF-22-20231.

Chapter 3 is a reprint of the material [4], as it appears in 'Optimization-based safe stabilizing feedback with guaranteed region of attraction', by P. Mestres and J. Cortés, in IEEE Control Systems Letters, 2022. The dissertation author was the primary investigator and author of this paper.

Chapter 4, in full, has been submitted for publication of the material [5] as it may appear as 'Control Barrier Function-Based Safety Filters: Characterization of Undesired Equilibria, Unbounded Trajectories, and Limit Cycles' by P. Mestres, Y. Chen, E. Dall'anese and J. Cortés in the Journal of Nonlinear Science, 2025. The dissertation author was the primary investigator and author of this paper. Chapter 4 is also in part a reprint of [6] as it appears in 'Characterization of the dynamical properties of safety filters for linear planar systems' in IEEE Conference on Decision and Control, 2024. The dissertation authors was one of the primary investigators and authors of this paper.

Chapter 5, in full, has been submitted for publication of the material [7] as it will appear as 'Converse Theorems for Certificates of Safety and Stability', in IEEE Transactions on Automatic Control, 2025. The dissertation author was the primary investigator and author of this paper.

Chapter 6 is a reprint of the material [8] as it appears in 'Regularity Properties of Optimization-Based Controllers', by P. Mestres, A. Allibhoy, and J. Cortés, in the European Journal of Control, 2025. The disseration author was the primary investigator and author of this paper.

Chapter 7 is a reprint of the material [9], as it appears in 'Distributed Safe Navigation of Multi-Agent Systems Using Control Barrier Function-Based Controllers', by P. Mestres, C. Nieto-Granda, and J. Cortés, in IEEE Robotics and Automation Letters, 2024. The dissertation author was the primary investigator and author of this paper. The work in Chapter 7 is also based on the material [10] as it appears in 'Distributed and anytime algorithm for network optimization problems with separable structure' by P. Mestres and J. Cortés, in IEEE Conference on Decision

and Control, 2023. The dissertation author was also the primary investigator and author of this paper.

Chapter 8, in full, has been submitted for publication of the material [11], as it may appear as "Safe and Dynamically-Feasible Motion Planning using Control Lyapunov and Barrier Functions", by P. Mestres, C. Nieto-Granda, and J. Cortés, in IEEE Transactions on Robotics, 2025. The dissertation author was the primary investigator and author of this paper.

Chapter 9 is a reprint of the material [12] as it appears in 'Feasibility and regularity analysis of safe stabilizing controllers under uncertainty' by P. Mestres and J. Cortés, in Automatica, 2024. The dissertation author was the primary investigator and author of this paper.

Chapter 10 is a reprint of the material [13] as it appeared in 'Feasibility analysis and regularity characterization of distributionally robust safe stabilizing controllers' by P. Mestres, K. Long, N. Atanasov, and J. Cortés, in IEEE Control Systems Letters, 2023. The dissertation author was the primary investigator and author of this paper.

Chapter 11, in part, is based on the material [3], which will appear as 'Anytime Safe Reinforcement Learning' by P. Mestres, A. Marzabal, and J. Cortés, in the 7th Annual Learning for Dynamics and Control Conference, 2025. The dissertation author was the primary investigator and author of this paper.

VITA

2020	B. Sc. in Mathematics, Universitat Politècnica de Catalunya
2020	B. Sc in Engineering Physics, Universitat Politècnica de Catalunya
2021	M. Sc in Mechanical Engineering, University of California, San Diego
2025	Ph. D. in Mechanical Engineering, University of California, San Diego

Journal Publications:

(1) P. Mestres, Y. Chen, E. Dall'anese, and J. Cortés, "Control Barrier Function-Based Safety Filters: Characterization of Undesired Equilibria, Unbounded Trajectories, and Limit Cycles", *Journal of Nonlinear Science*, submitted.

(2) P. Mestres, C. Nieto-Granda, and J. Cortés, "Safe and Dynamically-Feasible Motion Planning using Control Lyapunov and Barrier Functions", *IEEE Transactions on Robotics*, submitted.

(3) Y. Chen, P. Mestres, J. Cortés, and E. Dall'anese, "Equilibria and Their Stability Do Not Depend on the Control Barrier Function in Safe Optimization-Based Control", *Automatica*, submitted.

(4) P. Mestres and J. Cortés, "Converse Theorems for Certificates of Safety and Stability", *IEEE Transactions on Automatic Control*, to appear.

(5) P. Mestres, C. Nieto-Granda, and J. Cortés, "Distributed Safe Navigation of Multi-Agent Systems using Control Barrier Function-Based Optimal Controllers", *IEEE Robotics and Automation Letters*, vol. 9, no. 7, pp. 6760-6767, 2024.

(6) P. Mestres, A. Allibhoy, and J. Cortés, "Regularity Properties of Optimization-Based Controllers", *European Journal of Control*, vol. 81, pp. 1011098, 2025.

(7) P. Mestres, K. Long, N. Atanasov, and J. Cortés, "Feasibility Analysis and Regularity Characterization of Distributionally Robust Safe Stabilizing Controllers", *IEEE Control Systems Letters*, vol. 8, pp. 91-96, 2024.

(8) P. Mestres and J. Cortés, "Feasibility and Regularity Analysis of Safe Stabilizing Controllers", *Automatica*, vol. 167, pp. 111800, 2024.

(9) P. Mestres and J. Cortés, "Optimization-Based Safe Stabilizing Feedback with Guaranteed Region of Attraction", *IEEE Control Systems Letters* vol. 7, pp. 367-372, 2023.

Conference Publications:

(1) P. Mestres, J. Cortés, and E. D. Sontag, "Neural Network-Based Universal Formulas for Control", *The Thirty-Ninth Annual Conference on Neural Information Processing Systems*, submitted.

(2) G. Delimpaltadakis*, P. Mestres*[1], J. Cortés, and W. P. M. H. Heemels, "Feedback Optimization with State Constraints through Control Barrier Functions", *64th IEEE Conference on Decision and Control*, submitted.

(3) P. Mestres, A. Marzabal, and J. Cortés, "Anytime Safe Reinforcement Learning", *7th Annual Learning for Dynamics and Control Conference*, *Proceedings of Machine Learning Research*, vol. 283, pp. 1-12, 2025.

(4) Y. Chen*, P. Mestres*, E. Dall'anese, and J. Cortés, "Characterization of the Dynamical Properties of Safety Filters for Linear Planar Systems", *63rd IEEE Conference on Decision and Control*, Milan, Italy, 2024, pp. 2397-2402.

(5) P. Mestres, K. Long, M. Leok, N. Atanasov, and J. Cortés, "Stabilization of Nonlinear Systems through Control Barrier Functions", *63rd IEEE Conference on Decision and Control*, Milan, Italy, 2024, pp. 8858-8863.

(6) P. Mestres and J. Cortés, "Distributed and Anytime Algorithm for Network Optimization Problems with Separable Structure", *62nd IEEE Conference on Decision and Control*, Singapore, 2023, pp. 5457-5462.

[1] * denotes equal contribution.

(7) P. Mestres and J. Cortés, "Safe Design for Controlling Epidemic Spreading under Heterogeneous Testing Capabilities", *2022 American Control Conference*, Atlanta, Georgia, USA, 2022, pp. 697-702.

ABSTRACT OF THE DISSERTATION

Control, Planning, and Learning with Control Barrier Functions in Safety-Critical Systems

by

Pol Mestres
Doctor of Philosophy in Mechanical and Aerospace Engineering
University of California San Diego, 2025
Professor Jorge Cortés, Chair

Recent technological advances have led to the use of autonomous systems in a variety of different domains of human life, including manufacturing, transportation, power systems, and healthcare. These technologies are increasingly being deployed into safety-critical scenarios where minimal mistakes in their operation can lead to catastrophic societal consequences, such as loss of life, significant property damage, or environmental harm. The requirement of building these technologies with formal safety guarantees poses novel technical challenges, which has recently sparked the interest of many researchers from a wide range of disciplines such as control theory, formal methods, robotics, and design optimization.

This dissertation advances our understanding of the design of autonomous systems in safety-critical conditions. A central piece of our approach are control barrier functions, which are a control-theoretic tool to design safe controllers for autonomous systems.

This dissertation is divided in three parts. The first part considers the fundamental problem of designing controllers that combine safety and stability. The interplay between these two objectives raises a number of interesting challenges for control design. We study a variety of control designs based on control Lyapunov functions, safety filters, and outline their advantages and limitations.

In the second part of the dissertation we consider the problem of robotic naviga-

tion, where a robot needs to safely traverse an environment with multiple obstacles and eventually reach a goal location. In this setting, safe and stable controllers have limited applicability. In order to mitigate that, we explore the use of hierarchical controllers that couple low-level safe and stable controllers with high-level motion planners. We also explore how to extend the control barrier function framework to multi-robot settings in a distributed manner (i.e., with each robot designing its local controller using only information from neighboring agents).

In the third part of the dissertation we seek to understand how the presence of model uncertainty in real-world systems degrades the performance of safety-critical controllers. In order to achieve this, we leverage a variety of uncertainty quantification techniques, such as Gaussian processes or Wasserstein ambiguity sets. We also explore the design of reinforcement learning algorithms that are able to obtain an optimal control policy for uncertain systems modeled as Markov Decision Processes, while maintaining the safety constraints of the system during the training process.

Chapter 1

Introduction

Over the past several decades, rapid technological progress has led to the widespread adoption of autonomous systems across numerous domains of human activity, such as manufacturing, transportation, energy, and healthcare. In each of these settings, the close interaction between humans and autonomous systems underscores the critical importance of embedding safety into their design and operation. For instance, in autonomous driving, several high-profile accidents involving self-driving vehicles have tragically resulted in human fatalities. Likewise, the deployment of industrial robots in manufacturing environments has been linked to incidents causing serious injuries to human workers. The recent widespread use of Large Language Models (LLMs) has also stressed the importance of incorporating safety guardrails in their deployment, so that such models do not output harmful or offensive text, or do not lead the user to committing illegal activities. Beyond robotics and artificial intelligence, recent large-scale power blackouts have also exposed the economic and societal consequences of the unsafe operation of power grids.

This dissertation seeks to advance the design of decision-making strategies for autonomous systems in safety-critical conditions.

There are several challenges associated with the design of such strategies, some of which include the following. First, safety must be achieved together with other objectives, such as stabilization, trajectory tracking, minimizing energy consumption, etc. Second, the presence of uncertainty in sensor measurements and the

lack of full knowledge about the environment and system dynamics. Third, in many applications decisions must be made online under extremely tight time constraints. This emphasizes the need to devise decision-making strategies that are computationally efficient and can be executed in real time. Fourth, the need to integrate such decision-making strategies with other system modules, such as perception, state estimation, or humans-in-the-loop. Fifth, computing a set of safe states is significantly challenging in many cases, particularly under uncertainty in the dynamics or the environment.

Although there has recently been significant progress in devising techniques that can address the aforementioned challenges, state-of-the-art approaches still face significant limitations.

The goal of this dissertation is to advance the state-of-the-art and contribute in the mitigation of such limitations. Although there exist many different tools in the literature to design decision-making strategies in safety-critical systems, in this dissertation we focus on control barrier functions (CBFs). CBFs are a well-established control-theoretic technique to design safe controllers for autonomous systems. Although CBFs provide a simple and computationally lightweight way to design safe controllers, there exists a significant gap between the theory of CBFs and its applicability in real-world autonomous systems.

In the first part of this dissertation, we explore different control designs that seek to address the challenges associated with the satisfaction of safety together with other control objectives, such as the stabilization of the state of the system to a desired goal (e.g., ensuring that a robot eventually reaches a region of interest, or ensuring that the frequency of a power system converges to some desired setpoint). This comprises the first part of the dissertation (Chapters 3, 4, 5, and 6).

In the context of robotic navigation, a robot (or potentially a team of robots) needs to safely traverse a cluttered environment with multiple complex obstacles, and eventually reach a goal location. In general, safe and stable controllers often fall short of providing a good performance for this set of tasks. This is because of the lack of optimality guarantees of CBF-based controllers over long time horizons, as well as the presence of obstructions, topological in nature, preventing the design

of continuous safe and stabilizing controllers in various spaces of interest. Additionally, in such robotic applications, CBF-based controllers must be integrated in a system-level stack, including perception, mapping, and high-level motion planning modules.

In the second part of this dissertation, we explore the use of hierarchical controllers that couple low-level CBF-based safe and stable controllers with high-level motion planners. Furthermore, in scenarios involving multiple robots, and motivated by the need to design the controllers in a distributed fashion when communication is only possible with a subset of the agents, we also explore how to extend the CBF framework to multi-agent settings in a distributed manner (i.e., with each agent designing its local controller using only information from neighboring agents). This comprises the second part of the dissertation (Chapters 7 and 8).

In the third part of this dissertation, we study the problem of designing CBF-based controllers in systems with uncertainty. In particular, we seek to understand the level of model uncertainty that is required in order to still be able to guarantee safety along with other system requirements such as stability. In order to achieve this, we leverage a variety of uncertainty quantification techniques from the literature, such as Gaussian processes or Wasserstein ambiguity sets. In such systems with uncertainty, and also motivated by the lack of long-horizon optimality guarantees of CBF-based controllers, we explore the design of reinforcement learning algorithms that are able to obtain an optimal control policy while maintaining the safety constraints of the system during the training process. This comprises the third part of the dissertation (Chapters 9, 10, and 11).

1.1 Literature Review

Here we review the state of the art on safety-critical control. We focus on the existing progress on the topics that are most related to the approach presented in this dissertation.

1.1.1 Control Design with Safety and Stability Guarantees

There are a variety of control-theoretic tools that can be used to verify the safe operation of an autonomous system.

Hamilton-Jacobi (HJ) Reachability [14] seeks to find the reach-avoid set, defined as the set of states from which the system can be driven to a target set while satisfying state constraints at all times under all possible disturbances. This reach-avoid set can be found as the solution of a partial differential equation (PDE), which however suffers from the curse of dimensionality, because its solution becomes computationally more expensive as the state dimension grows. However, there have been significant advances in providing computationally tractable solutions for this PDE [15, 16]. Although the problem of computing control invariant sets is crucial, this topic is not investigated throughout this thesis. Instead, we usually assume the knowledge of a control invariant set.

Artificial Potential Fields (APF) [17, 18] are a well-established tool introduced in the 80s for collision-avoidance tasks in robotics. The technical approach underpinning APF constricts a vector field that is created by the combination of an attractive force towards a goal location and a repulsive force resonating from the obstacles, resulting in a force that steers the robot away from obstacles and towards a goal. However, the applicability of APFs is limited to specific types of control systems.

Model Predictive Control (MPC) [19] is a powerful framework to design controllers for systems with hard state and input constraints. MPC relies on the online solution of a state-dependent optimization problem. Despite the great success of MPC in practical applications and the strong theoretical backing for linear dynamics, general nonlinear dynamics and state constraints lead to non-convex optimization problems which can be computationally difficult to solve in real time.

Lyapunov functions, which are often used to certify stability properties of nonlinear systems, can also be used to guarantee safety. For example, computational tools to synthesize such functions for polynomial systems with sum-of-squares programming [20] can be utilized to verify that the nonlinear system remains inside a predefined safe region [21].

In this dissertation we focus on control barrier functions (CBFs), a control-theoretic tool [22, 23] to design controllers that render a certain predefined safe set forward invariant. CBFs provide a computationally lightweight way to design safe controllers for a wide range of nonlinear systems of interest, including control-affine systems. Additionally, CBFs can be combine with some of the previously mentioned approaches. For example, [24] refines CBFs with HJ reachability, and [25, 26] combines CBFs with MPC.

However, in applications where both safety and stability must be certified, CBFs fall short of providing provable stability guarantees. There are a variety of different works in the literature whose goal is to endow CBF-based controllers with stability guarantees.

One possibility is to use control Lyapunov functions (CLFs) [27], which have been successfully used in the control design for stabilization of nonlinear systems. For example, [28] combines a CLF and a CBF into a so-called CLBF, and then uses Sontag's universal formula [29] to derive a smooth safe and stable controller. However, in general it might be difficult to satisfy the conditions required for the existence of such a CLBF [30]. Another approach is the universal formula for smooth safe stabilization from [31]. However, this formula is only applicable in a set where both the CLF and the CBF are compatible (i.e., there exists a control satisfying their associated inequalities at every point of the set). An alternative approach [23] to tackle joint safety and stability specifications is to combine the CLF and the CBF in a quadratic program (QP). To guarantee the feasibility of the program when the functions are not compatible and to avoid the resulting controller to be non-Lipschitz when they are [32], the stability constraint is often relaxed. This results in a lack of guarantee of stability, even for arbitrarily large penalties in the relaxation parameter [33]. Moreover, as shown in [34, 35], this QP formulation can introduce undesired equilibria beyond the original equilibrium, which can even be asymptotically stable. This line of work [33, 35] then identifies conditions under which local stability guarantees of the equilibrium can be given.

Another possibility is to use CBF-based *safety filters* [36]. Safety filters yield a controller that minimally modifies a nominal stabilizing one while ensuring forward

invariance of a safe set. A critical research question is whether the closed-loop system under the safety filter retains the stability and robustness properties of the dynamical system with the nominal controller only. A first set of results about the dynamical properties of the closed-loop system with safety filters was provided in [37], which estimated the region of attraction of the desirable equilibrium (taken to be the origin w.l.o.g.). However, questions remain on the asymptotic behavior of the trajectories with initial condition outside the estimated region of attraction.

All of the control designs described above assume complete knowledge of the dynamics and safe set. Several recent papers have proposed alternative formulations of the CLF-CBF QP for systems with uncertainty or learned dynamics. For a particular class of uncertainties, [33] shows that the robust control design problem can still be posed as a QP. However, imperfect knowledge of the system dynamics or safety constraints often transforms the affine-in-the-input inequalities arising from CBFs and CLFs into second-order cone constraints (SOCCs). The papers [38, 39, 40] leverage Gaussian Processes (GPs) to learn the system dynamics from data and show that the mean and variance of the estimated GP can be used to formulate two SOCCs whose pointwise satisfaction implies safe stabilization of the true system with a prescribed probability. However, during the control design stage, the SOCC associated to stability is often relaxed and hence the resulting controller does not have stability guarantees. In the case where worst-case error bounds for the dynamics and the CBF are known, [41, 42] show how the satisfaction of two SOCCs can yield a safe stabilizing controller valid for all models consistent with these error bounds. On the other hand, [43] uses the framework of distributionally robust optimization to formulate a second-order convex program that achieves safe stabilization for systems with parametric uncertainty with a finite number of samples. Critically, these works lack guarantees on the simultaneous feasibility of these SOCCs and the regularity of controllers satisfying them. As a result, the proposed controllers might be undefined in practice, resulting in deadlock or unsafe, unstable, or discontinuous system behaviors. Finally, the papers [44, 45] utilize online data to improve the estimates of the dynamics and synthesize (also via SOCCs) less conservative controllers.

In the context of multi-agent systems, many applications require a distributed implementation of the individual agents' controllers. For optimization-based controllers resulting from CBFs, this requires a distributed solution of the resulting optimization problem. The works [46, 36] tackle this problem for quadratic programs (QPs) by splitting a centralized QP into local QPs that can be solved efficiently while preserving safety guarantees. However, the solution of these local QPs might lack optimality guarantees with respect to the original QP. The recent works [47, 48, 49, 50] introduce different algorithms to solve constrained optimization problems in a distributed fashion while satisfying the constraints throughout the execution of the algorithm. However, [47, 49, 48, 50] are restricted to a class of parametric QPs with conditions on the coefficients of the affine constraints. This approach has recently been successfully implemented for the problem of global connectivity maintenance [51].

1.1.2 Motion Planning

Trajectory optimization methods in motion planning [52, 53, 54] seek to directly design trajectories from the initial state to the goal state that take into account the robot dynamics. These methods usually formulate the planning problem as a high-dimensional nonconvex problem, which can be difficult to solve efficiently by off-the-shelf solvers. To address this, it is common to restrict the problem to a parametric class: [55, 56] uses the so-called MINVO basis, [57] uses B-splines, and [58, 59] use polynomial basis. Even with the restriction to such parametric classes, the trajectory optimization problems remain nonconvex, and their complexity scales with the dimension of the parameter space. One exception is the recent work [60], which formulates the trajectory optimization problem as a shortest path problem in Graphs of Convex Sets [61], an optimization framework that allows the trajectory optimization problem to be formulated as a mixed-integer convex program for trajectories parameterized by Bernstein polynomials. Despite the low runtimes that this algorithm exhibits in a variety of different robotic systems, it requires a partition of the environment in convex sets, which needs to be precomputed offline.

Regardless of the computational complexity, the restriction of trajectory optimization methods to parametric classes means that they are only guaranteed to produce dynamically feasible solutions for special classes of systems (for example [55, 56, 57, 58] work for quadrotors, and [59] for feedback linearizable systems). Furthermore, since the controllers needed to track these trajectories are generally open loop, they do not possess the inherent robustness properties associated with feedback control (an exception is [54], which uses model predictive control to generate optimal trajectories).

The approach taken in this dissertation is more closely aligned with *sampling-based motion planning* methods [62], which seeks to find a collision-free path from an initial state to a goal state through randomly sampling the state space. Despite its simplicity, it has been shown to be a practical solution for efficiently finding feasible paths even for high-dimensional problems. Rapidly-exploring random trees (RRTs) [63] and its variants [64, 65] are a family of sampling-based motion planning algorithms that are simple to implement and are probabilistically complete, meaning that a feasible path (if it exists) is found with probability one as the number of samples goes to infinity. RRTs build a tree rooted at a starting configuration and efficiently explore the configuration space by adding more samples. Despite the widespread use of RRT and the variants outlined above, their performance in systems with general differential constraints and dynamics remains limited, since they rely on the ability to connect any neighboring nodes of the tree with a dynamically feasible trajectory. This requires solving a *two-point boundary value problem* (BVP) [66, Chapter 14], which in general is challenging. Different works [67, 68] address this problem by developing algorithms that achieve optimality guarantees for different classes of systems without requiring the use of a BVP solver. On the one hand, [67] considers controllable linear systems, for which the explicit solution of the BVP can be computed, and [68] focuses on non-holonomic systems where *Chow's condition* holds, whose accessibility properties can also be used to sidestep the use of a BVP solver. Alternatively, other works introduce heuristics that approximate the solution of the BVP: [69, 70] do it using the linear quadratic regulator, and [71] leverages bang-bang controllers. Other works circumvent solv-

ing the BVP by using learning-based approaches. For instance, [72, 73] introduces an offline machine learning phase that learns the solution of the BVP, [74] refines the generation of the dataset used in this offline phase, and [75] learns the solution of the BVP using reinforcement learning techniques. There are also approaches [76] that combine the benefits of trajectory optimization methods with RRT, by constructing a tree of optimized trajectories along with tubes defining their regions of attraction, derived with sum-of-squares programming [20].

We are particularly interested in works that bypass the need to solve the BVP or to optimize over sets of trajectories by using CLFs and CBFs. There exist a few works in the literature [77, 78, 79, 80] that combine the effectiveness of RRT-based algorithms with the safety guarantees and computational efficiency provided by CBFs and CLFs, hence also bypassing the need to compute the solution of a BVP. However, these approaches require the simulation of trajectories derived from a CLF-CBF-based controller in order to determine whether new candidate nodes should be added to the tree. The repeated simulation of such trajectories can significantly slow down the search for a feasible path and compromise the computational efficiency of the resulting algorithm. Moreover, these existing works can be prone to safety violations as a consequence of the numerical errors introduced when simulating these trajectories, and do not formally ensure that the low-level CLF and CBF-based controller possesses both safety and stability guarantees. Finally, [81] introduces `LQR-CBF-RRT*`, which is asymptotically optimal and also leverages CBFs to ensure collision-free trajectories. Moreover, this method does not require simulating trajectories obtained with a CLF-CBF-based controller. However, the CBF condition is only verified at a finite sequence of points along a trajectory, which might compromise safety in-between such sampled points. Furthermore, the reference trajectory is generated through an LQR-based controller of a linearized model, which might also not be stabilizing for the original nonlinear system.

1.1.3 Safe Reinforcement Learning

The safe RL literature is vast and, in what follows, we focus on works which are most aligned with the approach presented in this dissertation. For more exhaustive surveys on safe RL, we refer the reader to [82, 83, 84, 85]. Safety constraints in RL are often expressed in the form of *cumulative constraints*, i.e., expected cumulative rewards that need to be kept below a certain threshold over certain time horizon [86, 2, 87, 88]. MDPs with such type of constraints are referred to as Constrained Markov Decision Processes (CMDPs).

A popular approach to solve CMDPs are primal-dual methods [89, 90], which simultaneously perform a maximization step in the primal variable and a minimization step in the dual variable, and can be shown to converge to the optimal policy for finite state and action CMDPs for a special class of probability transition functions [91].

In continuous state-action space, [88] also provides a primal-dual scheme, and shows that if a non-convex unconstrained RL problem is solved at every iteration, the algorithm provably converges to the optimal policy. However, solving such unconstrained RL problem at every iteration is computationally intractable.

Primal-dual algorithms do not guarantee the satisfaction of the safety constraints during the training process. Other works have employed primal-dual methods to guarantee safety during training, but are either limited to particular policy parameterizations [92] or solve a relaxed version of the problem and hence introduce an optimality gap [93, 94]. On the other hand, [2] proposes CPO, an algorithm purely based on primal variable updates that enjoys safety guarantees at every iteration. However, since the exact policy update law is computationally intensive, the work provides a practical algorithm based on a first-order approximations of the objective and constraints that might not satisfy the safety constraints during training. Alternatively, [95] presents IPO, another primal method that adds the constraints as penalty terms in the objective function, and also guarantees the satisfaction of safety constraints during training. However, it requires a feasible initial policy and does not possess formal convergence guarantees. Other primal methods such as [96] leverage Lyapunov functions to guarantee the satisfaction of

constraints during training. However, the method proposed to search for such Lyapunov functions might be computationally intensive, and convergence guarantees are only given for a limited class of problems. Finally, [97] optimizes over a class of truncated policies so that unsafe actions have probability zero, but the restriction to such class of policies also introduces an optimality gap, which is not formally quantified.

1.2 Statement of Contributions

The goal of this dissertation is to advance the design of decision-making strategies for autonomous systems in safety-critical conditions. We do so by studying methods whose aim is to control, learn, and perform motion planning for such systems.

Our technical contributions are structured in three parts. In the first part we study the design of controllers with safety and stability guarantees. In the second part, we investigate how such controllers can be utilized together with a high-level motion planner to achieve robotic navigation for single and multi-robot systems. In the third part, we examine the use of learning-based methods to endow safe and stable controllers with robustness to uncertainties, as well as the use of reinforcement learning algorithms that possess safety guarantees during the training process. Next we state our contributions in each of the three blocks on a more technical level.

1.2.1 Low-Level Optimization-Based Controllers with Safety and Stability Guarantees

In this first part we consider the problem of designing controllers that achieve safe stabilization of known control affine systems.

Given a CLF and a CBF whose 0-superlevel set defines an arbitrary, possibly non-convex safe set, the goal of Chapter 3 is to synthesize a safe, stabilizing feedback and identify the region of attraction of the origin for the resulting closed-loop system. To do so, we design an optimization with penalty-based controller that

has one of the objectives as a hard constraint and the other as a soft constraint. The controller depends on a penalty parameter that can be tuned to enhance the soft objective at the cost of reduced optimality, while guaranteeing the satisfaction of the hard constraint. An advantage of the proposed design is that the controller is automatically Lipschitz and has a closed-form expression. Next we show that the controller can introduce undesired equilibrium points different from the origin. By choosing the penalty parameter appropriately, and under some technical conditions, these undesired equilibria can be eliminated. Finally, our third contribution shows that the proposed controller can be tuned to provide an inner approximation of the region of attraction of the origin for the closed-loop system. As a consequence of this analysis, we provide conditions under which all of the safe set belongs to the region of attraction of the origin for the closed-loop system. Simulations on a planar system compare our design with other approaches in the literature.

In Chapter 4 we turn our attention to studying the dynamical properties of CBF-based safety filters, paying special attention to the emergence of undesired behaviors. We characterize the undesired equilibria that emerge in closed-loop systems with general control-affine dynamical systems, a stabilizing, locally-Lipschitz nominal controller, and a CBF-based safety filter. We show that finding the undesired equilibria is equivalent to solving an algebraic equation. We provide an example showing that, in general, the set of undesired equilibria can be a continuum. This motivates our next contribution, which consists in providing conditions under which the equilibria are isolated points. We also show that, in general, the trajectories of the closed-loop system can be unbounded. We then show how, by appropriately selecting some of the parameters of the safety filter, and under mild assumptions, one can ensure that the trajectories of the closed-loop system remain bounded. In the case of planar systems, we show that by suitably tuning the parameters of the safety filter, the closed-loop system does not contain any limit cycles. This implies that all trajectories of the closed-loop system either converge to the origin or to an undesired equilibrium. Therefore, the solutions of the algebraic equation for the undesired equilibria define all the possible limits of trajectories of

the closed-loop system. Since solving this algebraic equation for general systems is complicated, we also provide qualitative results regarding the structure of the set of undesired equilibria. We show that if the safe set is bounded, the number of undesired equilibria is even, and half of them are saddle points, whereas if the unsafe set is bounded, the number of undesired equilibria is odd, equal to $2l-1$ with $l \in \mathbb{Z}_{>0}$, and l of them are saddle points. We illustrate the existence of undesired equilibria and their stability properties for linear planar systems in a variety of different cases. For underactuated systems and safe sets that are parametrizable in polar coordinates, we show that no undesired equilibria exist. We provide different examples in which asymptotically stable undesired equilibria exist, including a fully actuated system with a convex safe set, an underactuated system with a safe set not parameterizable in polar coordinates, and an underactuated and fully actuated systems with a bounded unsafe set. We also provide an example with nonconvex unsafe set where asymptotically stable undesired equilibria exist for any choice of stabilizing nominal controller. Finally, for the special case where the unsafe set is an ellipse, we provide analytical expressions for the undesired equilibria and their stability properties. We show that if the system is underactuated, there exists exactly one undesired equilibria, which is a saddle point, whereas if the system is fully actuated, the behavior is much richer and includes a variety of different cases. Our contributions highlight the intrincate relationship between the system dynamics, the geometry of the safe set, and the existence of undesired equilibria and their stability properties. They also serve as a cautionary note to practitioners, for whom we provide a variety of methods to tune (when possible) their controllers to avoid this plethora of undesirable behaviors.

In Chapter 5, we introduce a variety of converse results regarding the existence of CBFs for the study of safety and safe stabilization of control systems. Specifically, we provide an example that shows that for unbounded safe sets, there might be candidate CBFs (i.e., functions whose zero super-level set is the safe set) which are not CBFs, and candidate CBFs which are. This is in contrast to the case of bounded safe sets, where all candidate CBFs are CBFs. We also provide an example that shows that the existence of a CBF does not guarantee the existence of

a locally Lipschitz safe feedback controller, even if the CBF condition is satisfied strictly at every point. Given a safe set, we provide a set of general conditions on the dynamics and the safe set under which a CBF is guaranteed to exist. These conditions include safe sets for which there exists a safe controller such that trajectories of the closed-loop system do not get arbitrarily close to the boundary of the safe set, or polynomial systems with polynomial safe set and safe feedback. We also define an extended notion of CBF, termed *extended control barrier function* (eCBF), which relies on a generalization of the notion of extended class $\mathcal{K}_\infty$ function and show that they are always guaranteed to exist for any given dynamics and safe set. Drawing on existing results in the literature, we provide a result that shows that if the unsafe set has a bounded connected component, there does not exist a CLBF or a strictly compatible CLF-CBF pair, and if the safe set is unbounded, there does not exist a CLBF. However, for a compact safe set, we show that if there exists a controller satisfying the CBF condition strictly and another controller that is stabilizing, the safe set admits a CLBF and a strictly compatible CLF-CBF pair. We also show that if the origin is safely stabilizing, under the same conditions that we can guarantee the existence of a CBF, we can also guarantee the existence of a compatible CLF-CBF pair. Finally, we show via a counterexample that the existence of a CLF and a CBF does not imply the existence of a strictly compatible CLF-CBF pair. On the positive side, we find sufficient conditions under which the existence of a CLF and a CBF implies the existence of a strictly compatible CLF-CBF pair and a compatible CLF-eCBF pair.

In Chapter 6, motivated by the fact that safe and stable controllers are generally defined at every state as the solution of an optimization problem, we provide an integrative presentation of insights and results about the regularity properties of optimization-based controllers. Under appropriate constraint qualifications and conditions on the data defining the optimization problem, we show that the optimization-based controllers are locally Lipschitz, continuously differentiable, and even analytic. We characterize the properties enjoyed by parametric optimizers arising from optimization problems defined by second-order continuously differentiable objective function and constraints, strictly convex objective, and

feasible set with nonempty interior. We show that even though such parametric optimizers might not be locally Lipschitz, they enjoy other important regularity properties, like point-Lipschitz continuity. Even if the optimization-based controller is discontinuous, under appropriate conditions on the optimization problem data, we show that it is measurable and locally bounded. Building on the results on regularity properties of optimization-based controllers, we study the existence and uniqueness of classical and Filippov solutions of closed-loop systems obtained from an optimization-based controller, and identify conditions ensuring that all (not necessarily unique) solutions remain in a safe set of interest.

1.2.2 Motion Planning using Safe and Stable Controllers

In this second part we seek to leverage the safe and stable controllers studied in the first part to achieve safe navigation in robotic systems.

In Chapter 7 we design a distributed controller for safe navigation of multi-agent robotic systems. We propose a synthesis framework which leverages CBFs to formulate obstacle avoidance and inter-agent collision avoidance constraints as affine inequalities in the control input. These constraints are included in a state-dependent network optimization problem that finds the control inputs allowing the agents to reach different waypoints of interest while maintaining a given formation and satisfying the safety constraints.

Motivated by this problem, our first contribution introduces a continuous-time dynamical system to solve convex optimization problems with separable objective function and constraints in a distributed and anytime fashion. The constraints couple the decision variables of all agents and this poses a difficulty in the design of distributed algorithms that solve such problems. We first show that the separable structure permits the intoduction of auxiliary variables to reformulate the original problem into one with local constraints while still preserving the same solution set. However, this reformulation still does not allow to fully decouple the optimization problem into one per agent because the auxiliary variables require coordination. In order to sort this hurdle, our technical approach constructs a dynamical system by combining the use of projected saddle-point dynamics, which

are distributed but not anytime, and the safe gradient flow, which is anytime but not distributed. First, we establish the well-posedness of the proposed dynamical system. Second, we show that it is distributed, exhibits the anytime property and is scalable. Finally, we prove that all trajectories with feasible initial condition converge to a neighborhood of the optimizer, which can be made arbitrarily small by tuning a design parameter accordingly. Moreover, in the case where the feasible set is bounded, we show that all trajectories with feasible initial condition exactly converge to the optimizer.

Our second contribution leverages this distributed continuous-time algorithm for constrained optimization to design a distributed controller. We establish that the proposed controller design is distributed, safe, and asymptotically converges to the solution of the state-dependent network optimization problem. Our last contribution is the implementation of the proposed controller in a variety of different environments, robots and formations, both in simulation and in real hardware.

In Chapter 8 we consider the problem of designing motion planning algorithms that generate collision-free paths from an initial to a final destination for systems with control-affine dynamics. To ensure that the sequence of waypoints generated by the sampling-based algorithm can be tracked by a controller while ensuring safety and stability, we leverage the theory of CBFs and CLFs. First, we introduce a result of independent interest which shows that the problem of verifying whether a CLF and a CBF are compatible in a set of interest can be solved by solving an optimization problem. Although in general such optimization problem is non-convex, we show that for linear systems and CBFs of polytopic or ellipsoidal obstacles, it reduces to a quadratically constrained quadratic program (QCQP), and for CBFs of circular obstacles it can be solved in closed form. Next, we leverage the results on compatibility checking of a CLF-CBF pair to develop Compatible CLF-CBF-RRT (or `C-CLF-CBF-RRT` for short), a sampling-based motion planning algorithm that is a variant of RRT. We show that, by construction, `C-CLF-CBF-RRT` generates collision-free paths that can be executed with a CLF-CBF-based controller, and formally establish it is probabilistically complete. We also show how our proposed approach can be generalized to systems where safety constraints have a high rel-

ative degree. We illustrate our results in simulation and hardware experiments for differential drive robots and compare them with the literature, showing that `C-CLF-CBF-RRT` can generate safe and stable paths with a better average execution time. Noteworthy properties of `C-CLF-CBF-RRT` as compared to the literature are: it does not require generating closed-loop trajectories at every sampling step because of the compatibility verification of CLF-CBF pairs; it avoids the potential safety violations that occur as a consequence of the numerical errors introduced when simulating trajectories; its computational complexity is tractable provided that the optimization problem verifying the compatibility of the CLF and CBF is tractable; and it ensures by construction that the sequence of generated waypoints can be robustly asymptotically tracked by a safe controller, without introducing unwanted dynamical behaviors such as undesired equilibria, and while ensuring that the optimization problem defining such controller is recursively feasible.

1.2.3 Learning in Safety-Critical Systems under Uncertainty

In this third part we study the use of learning-based techniques to ensure safety, stability, and optimality in systems with uncertainty.

In Chapter 9 we study the problem of safe stabilization of control-affine systems under uncertainty. We consider two scenarios for the estimates of the dynamics and safe set: either worst-case error bounds or probabilistic descriptions in the form of Gaussian Processes (GPs) are available. In both cases, the problem of designing a safe stabilizing controller can be reduced to satisfying two SOCCs at every point in the safe set. Our first contribution consists of giving conditions for the feasibility of each pair of SOCCs. The first result is a sufficient condition that requires a bound on the norm of a safe and stabilizing controller and quantifies what model errors are tolerable while still being able to find a controller that guarantees safe stabilization. Our second result is a sufficient condition that does not require knowledge of such bound and consists of finding a root of a scalar nonlinear equation. Our third contribution consists in giving different regularity properties for controllers satisfying a set of SOCCs. First we show that if each pair of SOCCs is feasible, then there exists a smooth safe stabilizing controller.

Second, we show that the minimum-norm controller satisfying each pair of SOCCs is point-Lipschitz. Third, we provide a universal formula for satisfying a single SOCC and hence achieving either safety or stability. We illustrate our results in the safe stabilization of a planar system.

In Chapter 10 we also study the problem of safe stabilization of control-affine systems under uncertainty. However, in this case we assume that the distribution of the uncertainty is unknown and formulate the control design problem through a second-order cone program (SOCP) using distributionally robust versions of the CLF and CBF constraints constructed on the basis of uncertainty samples. Our first contribution is the derivation of a necessary condition and two sufficient conditions for the feasibility of the optimization problem. We characterize the computational complexity of these conditions and show that, for a large number of samples, it is significantly smaller than solving the SOCP directly, which makes them useful to efficiently check whether the problem is feasible without having to solve it. Our first sufficient condition is dependent on the quality of the uncertainty samples but is limited to a single control objective. Our second sufficient condition is only dependent on the number of samples but can be used for any number of constraints. Our final contribution shows that the solution of this distributionally robust optimization problem is point-Lipschitz, and hence continuous, which means that solutions of the closed loop system are guaranteed to exist and the controller obtained from it can be implemented without inducing chattering.

In Chapter 11 we consider the problem of designing an algorithm that finds the optimal policy of a constrained RL problem and is anytime (i.e., it satisfies the constraints of the problem at every iteration). To achieve this goal, first we introduce the Robust Safe Gradient Flow (RSGF), a continuous-time algorithm for constrained optimization that is a variation of the recently introduced Safe Gradient Flow (SGF) [98]. The RSGF (as well as the SGF) leverages the theory of CBFs to design an algorithm for constrained optimization that guarantees forward invariance of the feasible set. We formally establish a set of assumptions under which the RSGF is locally and globally Lipschitz, it is anytime, and converges to the set of KKT points of the original constrained optimization problem. Second,

we define estimates for the value functions defining the constrained RL problem as well as their gradients. These estimates are off-policy, in the sense that the estimates of any given policy can be constructed using trajectories generated by other policies. We establish different statistical properties of these estimates such as their mean, a bound on their variance, and the probability that the difference between the estimates and their true values is within a tolerance. Third, we introduce Reinforcement Learning-based Robust Safe Gradient Flow (RL-RSGF), an off-policy RL algorithm that is based on a discretization of RSGF and utilizes the introduced estimates of the value function and their estimates. We show that for any prescribed confidence, if the estimates are generated with a sufficiently large number of episodes (which we quantify), RL-RSGF updates safe policies to safe policies. We also show that the iterates of RL-RSGF asymptotically converge to a KKT point with probability one, and characterize its rate of convergence. Finally, we illustrate the performance of RL-SGF in different simulation examples.

Chapter 2

Preliminaries

2.1 Notation

We denote by $\mathbb{Z}_{>0}$, $\mathbb{R}$, and $\mathbb{R}_{\geq 0}$ the set of positive integers, real, and nonnegative real numbers, respectively. Boldface symbols denote vectors and non-boldface symbols denote scalars, functions, or matrices. Let $n \in \mathbb{Z}_{>0}; \mathbf{0}_n$ represents the n-dimensional zero vector, $\mathbb{0}_n$ the $n \times n$-dimensional zero matrix and $\mathbf{I}_n$ the n-dimensional identity matrix. We also write $[n] = \{1, \cdots, n\}$. Given a set $\mathcal{S}$, $|\mathcal{S}|$ denotes its cardinality, and $\mathcal{P}(\mathcal{S})$ the collection of subsets of $\mathcal{S}$. If $\mathcal{S}$ is a subset of $\mathbb{R}^n$, $\overline{co}$ denotes its convex closure and μ its Lebesgue measure. Given $\mathbf{x} \in \mathbb{R}^n$, $\|\mathbf{x}\|$ denotes its Euclidean norm. Let $G \in \mathbb{R}^{n \times n}$ be a matrix. Then, $\det(G)$ denotes its determinant, and $\|\mathbf{x}\|_G = \sqrt{\mathbf{x}^\top G \mathbf{x}}$. Given a set $S \subset \mathbb{R}^n$, we denote by $\mathrm{Int}(S)$ and ∂S the interior and boundary of S, respectively. For $r > 0$ and $\mathbf{p} \in \mathbb{R}^n$, we let $\mathcal{B}_r(\mathbf{p}) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{y} - \mathbf{p}\| < r\}$. The tangent cone of the set $\mathcal{C}$ at the point $\mathbf{x} \in \mathbb{R}^n$ is defined as

$$T_{\mathcal{C}}(\mathbf{x}) = \Big\{\mathbf{v} \in \mathbb{R}^n \;\Big|\; \liminf_{h \to 0} \frac{\mathrm{dist}(\mathbf{x} + h\mathbf{v}, \mathcal{C})}{h} = 0\Big\}.$$

Given $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^{n \times m}$ and a smooth function $W : \mathbb{R}^n \to \mathbb{R}$, the notation $L_f W : \mathbb{R}^n \to \mathbb{R}$ (resp. $L_g W : \mathbb{R}^n \to \mathbb{R}^m$) denotes the Lie derivative of W with respect to f (resp. g), that is $L_f W = \nabla W^\top f$ (resp. $\nabla W^\top g$). For a function $\bar{f} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$, we write the column vectors of partial derivatives of $\bar{f}$ with respect to the first and second arguments as $\nabla_{\mathbf{x}} \bar{f}$ and $\nabla_{\mathbf{y}} \bar{f}$, respectively. Given $k \in \mathbb{Z}_{>0}$,

$\mathcal{C}^k(\mathbb{R}^n)$ denotes the set of k-times continuously differentiable functions in $\mathbb{R}^n$. We say that a function $f : \mathbb{R}^n \to \mathbb{R}^n$ is Lipschitz at $\mathbf{x}$ if there exists a neighborhood $\mathcal{N}_\mathbf{x}$ of $\mathbf{x}$ such that for any $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{N}_\mathbf{x}$ we have $\|f(\mathbf{x}_1) - f(\mathbf{x}_2)\| \leq L_\mathbf{x} \|x_1 - x_2\|$ for some constant $L_\mathbf{x} > 0$. If f is Lipschitz at every $\mathbf{x} \in \mathbb{R}^n$, we say that f is Lipschitz. If there exists a uniform constant $L > 0$ such that $\|f(\mathbf{x}_1) - f(\mathbf{x}_1)\| \leq L \|\mathbf{x}_1 - \mathbf{x}_2\|$ for all $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{R}^n$, then we say that f is globally Lipschitz.

Given $\mathbf{a} \in \mathbb{R}^n$, $b \in \mathbb{R}$, let $H = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{a}^\top \mathbf{x} = b\}$. We write the projection of $\mathbf{v} \in \mathbb{R}^n$ onto H as $P_H(\mathbf{v}) = \mathbf{c} - \frac{\mathbf{a}^\top \mathbf{x} - b}{\|\mathbf{a}\|^2}\mathbf{a}$.

For $a \in \mathbb{R}$ and $b \in \mathbb{R}_{\geq 0}$, we let

$$[a]_b^+ = \begin{cases} a & \text{if } b > 0, \\ \max\{0, a\} & \text{if } b = 0. \end{cases}$$

Given $\mathbf{a} \in \mathbb{R}^n$ and $\mathbf{b} \in \mathbb{R}^n_{\geq 0}$, $[\mathbf{a}]_\mathbf{b}^+$ denotes the vector whose i-th component is $[a_i]_{b_i}^+$, for $i \in [n]$. Given a set $P \subset \mathbb{R}^n$ and variables $\xi = \{x_{i_j}\}_{j=1}^k$, we denote by $\Pi_\xi P = \{(x_{i_1}, x_{i_2}, \cdots, x_{i_k}) \in \mathbb{R}^k : \mathbf{x} \in P\}$ the projection of P onto the ξ variables.

A function $\beta : \mathbb{R} \to \mathbb{R}$ is of class $\mathcal{K}$ if $\beta(0) = 0$ and β is strictly increasing. It is of class $\mathcal{K}_\infty$ if moreover, $\lim_{s \to \infty} \beta(s) = \infty$, and of extended class $\mathcal{K}_\infty$ if moreover, $\lim_{s \to \pm\infty} \beta(s) = \pm\infty$.

A function $V : \mathbb{R}^n \to \mathbb{R}$ is positive definite if $V(\mathbf{0}) = \mathbf{0}$ and $V(\mathbf{x}) > 0$ for all $\mathbf{x} \neq 0$. V is proper in a set Γ if the set $\{\mathbf{x} \in \Gamma : V(\mathbf{x}) \leq c\}$ is compact for any $c \geq 0$.

Given a matrix $A \in \mathbb{R}^{n \times m}$, the kernel of A is $\ker(A) = \{\mathbf{x} \in \mathbb{R}^m : M\mathbf{x} = \mathbf{0}_n\}$ and the image of A is $\mathrm{Im}(A) = \{y \in \mathbb{R}^m : \exists x \in \mathbb{R}^n \text{ s.t. } y = Ax\}$. Given two integers i, j such that $1 \leq i < j \leq n$, $A_{i:j}$ denotes the $m \times (j - i + 1)$ matrix obtained by selecting the columns from i to j of A. On the other hand, $\sigma_{\max}(A)$ denotes the maximum singular value of A.

If A is a square matrix (i.e., $A \in \mathbb{R}^{n \times n}$) with eigenvectors $\{v_j\}_{j=1}^n$ and corresponding eigenvalues $\{\lambda_j\}_{j=1}^n$, the stable subspace of A is defined as $\mathcal{V}_s(A) = \mathrm{span}(\{v_j : \Re(\lambda_j) < 0, j \in [n]\})$, where $\Re(\lambda_j)$ denotes the real part of λ_j. Furthermore, $\bar{\lambda}_{\min}(A)$ and $\lambda_{\max}(A)$ refer to the smallest non-zero and largest real parts of the eigenvalues of A, respectively.

An undirected graph is a pair $\mathcal{G} = (V, \mathcal{E})$, where $V = V(\mathcal{G}) = [N]$ is the vertex set and $\mathcal{E} = \mathcal{E}(\mathcal{G}) \subset V \times V$ is the edge set, with $(i, j) \in \mathcal{E}$ if and only if $(j, i) \in \mathcal{E}$.

The set $\mathcal{N}_i = \{j \in V : (i,j) \in \mathcal{E}\}$ refers to the neighbors of node i.

Given a random variable X taking scalar values, $\mathbb{E}[X]$ denotes the expectation of X, and $\mathrm{Var}[X] = \mathbb{E}[(X - \mathbb{E}[X])^2]$ denotes its variance. We write as $\mathcal{GP}(\mu(\mathbf{x}), K(\mathbf{x}, \mathbf{x}'))$ a Gaussian Process distribution with mean function μ and covariance function K.

2.2 Notions of Regularity of Functions

In this section we review various notions of regularity of functions.

Definition 2.2.1. (Notions of Lipschitz continuity): *A function $f : \mathbb{R}^n \to \mathbb{R}^q$ is*

- point-Lipschitz at $\mathbf{x}_0 \in \mathbb{R}^n$ *if there exists a neighborhood $\mathcal{U}$ of $\mathbf{x}_0$ and a constant $L \geq 0$ such that*

$$\|f(\mathbf{x}) - f(\mathbf{x}_0)\| \leq L \|\mathbf{x} - \mathbf{x}_0\|, \quad \forall \mathbf{x} \in \mathcal{U}. \tag{2.1}$$

- locally Lipschitz at $\mathbf{x}_0 \in \mathbb{R}^n$ *if there exists a neighborhood $\tilde{\mathcal{U}}$ of $\mathbf{x}_0$ and a constant $\tilde{L} \geq 0$ such that*

$$\|f(\mathbf{x}) - f(\mathbf{y})\| \leq \tilde{L} \|\mathbf{x} - \mathbf{y}\|, \quad \forall \mathbf{x}, \mathbf{y} \in \tilde{\mathcal{U}}. \tag{2.2}$$

The notion of point-Lipschitz continuity is used, for instance, in [99, Section 6.3] and called *Lipschitz stability*, without clearly acknowledging the difference with the notion of local Lipschitz continuity. In the optimization literature, this property is sometimes referred to as *calmness* (cf. [100, Chapter 8.F]). Locally Lipschitz functions are point-Lipschitz, but the converse is not true. For instance, the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x \sin(\frac{1}{x})$ if $x \neq 0$ and $f(0) = 0$ is point-Lipschitz but not locally Lipschitz at the origin.

Definition 2.2.2. (Hölder property): *A function $f : \mathbb{R}^n \to \mathbb{R}^q$ has the* Hölder property *at $\mathbf{x}_0 \in \mathbb{R}^n$ if there exists a neighborhood $\hat{\mathcal{U}}$ of $\mathbf{x}_0$ and constants $C > 0$, $\alpha \in (0, 1]$ such that*

$$\|f(\mathbf{x}) - f(\mathbf{y})\| \leq C \|\mathbf{x} - \mathbf{y}\|^{\alpha}, \quad \forall \mathbf{x}, \mathbf{y} \in \hat{\mathcal{U}}. \tag{2.3}$$

Note that if f is locally Lipschitz at $\mathbf{x}_0$ then it also has the Hölder property at $\mathbf{x}_0$ but the converse is not true.

Definition 2.2.3. (Directionally differentiable function): *A function $f : \mathbb{R}^n \to \mathbb{R}$ is directionally differentiable if for any vector $\mathbf{v} \in \mathbb{R}^n$, the limit*

$$\lim_{h \to 0} \frac{f(\mathbf{x} + h\mathbf{v}) - f(\mathbf{x})}{h}$$

exists. A vector-valued function is directionally differentiable if each of its components is directionally differentiable.

Let $\Omega \subset \mathbb{R}^n$. Throughout the paper, a function $\varphi : \Omega \to \mathbb{R}^d$ belongs to the set $\mathcal{C}^k(\Omega)$ if φ is k-times continuously differentiable in Ω. A function $\varphi : \Omega \to \mathbb{R}^d$ belongs to the set $\mathcal{C}^0(\Omega)$ if φ is continuous in Ω. In case we view the elements in Ω as vectors of the Cartesian product $\mathbb{R}^{m_1} \times \mathbb{R}^{m_2}$ and φ takes the form $(\mathbf{x}, \mathbf{u}) \mapsto \varphi(\mathbf{x}, \mathbf{u})$, the function $\varphi \in \mathcal{C}^{0,k}(\Omega)$ if for every $\mathbf{x} \in \Omega$, the derivatives of order up to k of $\varphi(\mathbf{x}, \cdot)$ with respect to u exist and are continuous with respect to x and u.

Definition 2.2.4. (Analytic function): *A function $f : \mathbb{R}^n \to \mathbb{R}$ is analytic in an open set D if for any $\mathbf{x} \in D$ there exists a sequence $\{A_\alpha\}_{\alpha \in \mathbb{Z}^n_{\geq 0}, n \in \mathbb{Z}_{\geq 0}}$ such that $f(\mathbf{x}) = \sum_{n=0}^{\infty} \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} A_\alpha (\mathbf{x} - \mathbf{x}_0)^n$ for all $\mathbf{x}$ in a neighborhood of $\mathbf{x}_0$, where $(\mathbf{x} - \mathbf{x}_0)^\alpha = (x_1 - x_{0,1})^{\alpha_1} \cdots (x_n - x_{0,n})^{\alpha_n}$. A vector-valued function is analytic in an open set D if each of its components is analytic.*

Note that an analytic function in an open set D belongs to $\mathcal{C}^k(D)$ for any $k \in \mathbb{Z}_{\geq 0}$. Finally, we introduce the last notion of regularity, which is weaker than all the ones presented above and only requires the function to be bounded in a neighborhood of a point.

Definition 2.2.5. (Locally bounded function): *A function $f : \mathbb{R}^n \to \mathbb{R}^q$ is locally bounded at $\mathbf{x}_0 \in \mathbb{R}^n$ if there exists a neighborhood $\breve{\mathcal{U}}$ of $\mathbf{x}_0$ and a constant $B > 0$ such that $\|f(\mathbf{x})\| \leq B$ for all $\mathbf{x} \in \breve{\mathcal{U}}$.*

2.3 Dynamical Systems

In this section we review various notions related to the analysis of dynamical systems. Consider the dynamical system $\dot{\mathbf{x}} = f(\mathbf{x})$, with $f : \mathbb{R}^n \to \mathbb{R}^n$ locally

Lipschitz. Then, for any initial condition $\mathbf{x}_0 \in \mathbb{R}^n$ at time t_0, there exists a maximal interval of existence $[t_0, t_1)$ such that $x(t; \mathbf{x}_0)$ is the unique solution to $\dot{\mathbf{x}} = f(\mathbf{x})$ on $[t_0, t_1)$ (cf. [27]). If f is continuously differentiable and $\mathbf{x}_*$ is an equilibrium point of f (i.e., $f(\mathbf{x}_*) = \mathbf{0}_n$), then $\mathbf{x}_*$ is *degenerate* if the Jacobian of f evaluated at $\mathbf{x}_*$ has at least one eigenvalue with real part equal to zero. Otherwise, we say that $\mathbf{x}_*$ is *hyperbolic*.

Given a hyperbolic equilibrium point with $k \in \mathbb{Z}_{>0}$ eigenvalues with negative real part, the Stable Manifold Theorem [101, Section 2.7] ensures that there exists an invariant k-dimensional manifold M such that all trajectories with initial conditions on M converge to $\mathbf{x}_*$. The global stable manifold at $\mathbf{x}_*$ is defined as $W_s(\mathbf{x}_*) = \bigcup_{t \leq 0, \mathbf{x}_0 \in M} x(t; \mathbf{x}_0)$. An equilibrium point $\mathbf{x}_*$ is isolated if there exists an open neighborhood $\mathcal{U}$ of $\mathbf{x}_*$ such that $\mathbf{x}_*$ is the only equilibrium point in $\mathcal{U}$.

A set $\mathcal{C} \subset \mathbb{R}^n$ is forward invariant under the dynamical system $\dot{\mathbf{x}} = f(\mathbf{x})$ if any trajectory with initial condition in $\mathcal{C}$ at time $t = 0$ remains in $\mathcal{C}$ for all positive times.

Let $f : \mathbb{R}^n \times \mathbb{R}^m$ be locally Lipschitz. We say that the set $\mathcal{C}$ is safe for the control system $\dot{\mathbf{x}} = f(\mathbf{x}, \mathbf{u})$ if there exists a locally Lipschitz control $k : \mathbb{R}^n \to \mathbb{R}^m$ such that $\mathcal{C}$ is forward invariant for $\dot{\mathbf{x}} = f(\mathbf{x}, k(\mathbf{x}))$.

2.4 Markov Decision Processes

In this section we review various notions related to Markov Decision Processes. Let $\mathcal{S}$ be a set of states, $\mathcal{A}$ be a set of actions, and $P : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \to [0, 1]$ be a probability transition function, where $P(s, a, s')$ represents the probability of transitioning to state s' when at state s and taking action a. We further let $R_0 : \mathcal{S} \times \mathcal{A} \times \mathcal{S} \to \mathbb{R}$ be a function defining the reward associated with completing a task then transitioning to state s' from state s and taking action a. We refer to the tuple $(\mathcal{S}, \mathcal{A}, P, R_0)$ as a Markov Decision Process.

Furthermore, let $q \in \mathbb{Z}_{>0}$ and for $i \in [q]$, let $R_i : \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ be a function defining the cost associated with a safety constraint when transitioning to state s' from state s and taking action a. We refer to the tuple $(\mathcal{S}, \mathcal{A}, P, R_0, \{R_i\}_{i=1}^q)$ as a Constrained

Markov Decision Process (CMDP).

A policy π for the CMDP is a function that maps every state $s \in \mathcal{S}$ to a distribution over the set of actions $\mathcal{A}$. Such distribution is denoted as $\pi(\cdot|s)$, and $\pi(a|s)$ is the probability of taking action $a \in \mathcal{A}$ at state $s \in \mathcal{S}$.

2.5 Control Lyapunov and Barrier Functions

In this section we introduce the notions of control Lyapunov and barrier functions. We consider a nonlinear control system

$$\dot{\mathbf{x}} = f(\mathbf{x}, \mathbf{u}), \tag{2.4}$$

where $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is locally Lipschitz, with $\mathbf{x} \in \mathbb{R}^n$ the state and $\mathbf{u} \in \mathbb{R}^m$ the input.

First we introduce the notion of control Lyapunov function.

Definition 2.5.1. (Control Lyapunov Function [27, 102]): *Given a set $\Gamma \subseteq \mathbb{R}^n$, with $\mathbf{0}_n \in \Gamma$, a continuously differentiable function $V : \Gamma \to \mathbb{R}$ is a **CLF** on Γ for the system (2.4) if it is proper in Γ, positive definite, and there exists a positive definite function $W : \Gamma \to \mathbb{R}$ such that, for each $\mathbf{x} \in \Gamma \backslash \{\mathbf{0}_n\}$, there exists a control $\mathbf{u} \in \mathbb{R}^m$ satisfying*

$$\nabla V(\mathbf{x})^\top f(\mathbf{x}, \mathbf{u}) \leq -W(\mathbf{x}). \tag{2.5}$$

A locally Lipschitz controller $k : \mathbb{R}^n \to \mathbb{R}^m$ such that $\mathbf{u} = k(\mathbf{x})$ satisfies (2.5) for all $\mathbf{x} \in \Gamma \backslash \{\mathbf{0}_n\}$ makes the origin of the corresponding closed-loop system asymptotically stable. Therefore, CLFs provide a way to guarantee asymptotic stabilizability through an appropriately designed controller.

Next, we introduce the notion of control barrier function (CBF). Consider the set $\mathcal{C}$ defined as the zero-superlevel set of a continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$ as follows:

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}, \tag{2.6a}$$

$$\partial\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) = 0\}, \tag{2.6b}$$

$$\mathrm{Int}(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) > 0\}. \tag{2.6c}$$

For a fixed safe set $\mathcal{C}$, we refer to a function satisfying (2.6) as a candidate CBF. We further assume that $\text{Int}(\mathcal{C}) \neq \varnothing$.

Definition 2.5.2. (Control Barrier Function [23]): *Let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function satisfying* (2.6)*. The function h is a **CBF** of $\mathcal{C}$ for the system* (2.4) *if there exists an extended class $\mathcal{K}_\infty$ function α such that, for all $\mathbf{x} \in \mathcal{C}$, there exists a control $\mathbf{u} \in \mathbb{R}^m$ satisfying*

$$\nabla h(\mathbf{x})^\top f(\mathbf{x}, \mathbf{u}) + \alpha(h(\mathbf{x})) \geq 0. \tag{2.7}$$

If the inequality holds strictly, we refer to h as a strict CBF.

Analogously to CLFs for stability, CBFs can be used to certify safety of $\mathcal{C}$.

Theorem 2.5.3. (CBFs certify safety [23, Theorem 2]): *Let $\mathcal{C} \subset \mathbb{R}^n$, h be a CBF of $\mathcal{C}$ for the system* (2.4)*, and* 0 *be a regular value of h. Any Lipschitz controller $u_{sf} : \mathbb{R}^n \to \mathbb{R}^m$ that satisfies*

$$u_{sf}(\mathbf{x}) \in K_{\text{cbf}}(\mathbf{x}) = \{\mathbf{u} \in \mathbb{R}^m : \nabla h(\mathbf{x})^\top f(\mathbf{x}, \mathbf{u}) \geq -\alpha(h(\mathbf{x}))\} \tag{2.8}$$

for all $\mathbf{x} \in \mathcal{C}$ renders the set $\mathcal{C}$ forward invariant.

The following result states that for compact safe sets the converse of Theorem 2.5.3 also holds.

Theorem 2.5.4. (Converse CBF result for compact safe sets [23, Theorem 3]): *Let $\mathcal{C}$ be a compact set defined as in* (2.6) *and assume that* 0 *is a regular value of h. If $\mathcal{C}$ is safe for system* (2.4)*, then $h|_{\mathcal{C}} : \mathcal{C} \to \mathbb{R}$ is a CBF of $\mathcal{C}$.*

Note that the result not only states the existence of a CBF but also that the function defining the set $\mathcal{C}$ is itself a CBF.

Remark 2.5.5. (Existence of Lipschitz safe controllers): As pointed out in Theorem 2.5.3, any locally Lipschitz safe controller satisfying that CBF condition renders the set safe. However, in general, such locally Lipschitz controller might not exist even if a CBF is available. In fact, [103, Example III.5] shows that the so-called *minimum-norm* controller (obtained at every $x \in \mathbb{R}^n$ as the controller with

smallest norm that satisfies (2.7)) can be unbounded. Since the minimum-norm controller is unbounded, this example shows that even if a CBF exists, there might not exist a locally Lipschitz controller satisfying (2.7). However, [103, Lemma III.2] shows that if (2.4) is control-affine, $\mathcal{C}$ is compact and the CBF condition (2.7) holds strictly at the boundary, then the minimum-norm controller is locally Lipschitz. Alternatively, if $\mathcal{C}$ is compact and there exists an open set $\mathcal{D}$ containing $\mathcal{C}$ for which the CBF condition is feasible, then a Lipschitz safe controller also exists [104, Theorem 5]. We next complement this discussion by presenting an example inspired by [105] that shows that if the system is not control-affine, even if $\mathcal{C}$ is compact and the CBF condition (2.7) holds strictly at the boundary, there might not exist a continuous safe controller. Let $h : \mathbb{R}^2 \to \mathbb{R}$ be defined as $h(x, y) = -(x^2 + y^2) + 10$ and take $\mathcal{C}$ as in (2.6). Consider the system

$$\dot{x} = x\big((u-1)^2 - (x-1)\big)\big((u+1)^2 + (x-2)\big), \tag{2.9a}$$

$$\dot{y} = y\big((u-1)^2 - (x-1)\big)\big((u+1)^2 + (x-2)\big). \tag{2.9b}$$

Let us show that h is a CBF of $\mathcal{C}$ for system (2.9). Take $(x, y) \in \mathcal{C}$, and note that (2.7) is equivalent to

$$-2(x^2 + y^2)\big((u-1)^2 - (x-1)\big)\big((u+1)^2 + (x-2)\big) \geq -\alpha(h(x, y)). \tag{2.10}$$

Note that the set of points $(x, u) \in \mathbb{R}^2$ that satisfy

$$\big((u-1)^2 - (x-1)\big)\big((u+1)^2 + (x-2)\big) \leq 0, \tag{2.11}$$

consists of two disjoint connected sets, one formed by the points to the right of the parabola $x = 1 + (u-1)^2$, and the other formed by the set of points to the left of the parabola $x = 2 - (u+1)^2$. This set is illustrated in Figure 2.1. Note that the projection of these two sets onto the x axis covers the whole axis. Hence, h is a CBF. Now let $\tilde{u}_0 : \mathcal{C} \to \mathbb{R}$ be a controller such that $u = \tilde{u}_0(x, y)$ satisfies (2.10) at all points in $\mathcal{C}$, and let $\tilde{u} : [-\sqrt{10}, \sqrt{10}] \to \mathbb{R}$ be defined as $\tilde{u}(x) = \tilde{u}_0(x, \sqrt{10 - x^2})$. Note that since the two connected sets are disjoint, $\tilde{u}$ can not be continuous. This implies that $\tilde{u}_0$ can also not be continuous. We note also that in this example, $\mathcal{C}$ is compact and for all $x \in \mathbb{R}$, there exists $u \in \mathbb{R}$ satisfying

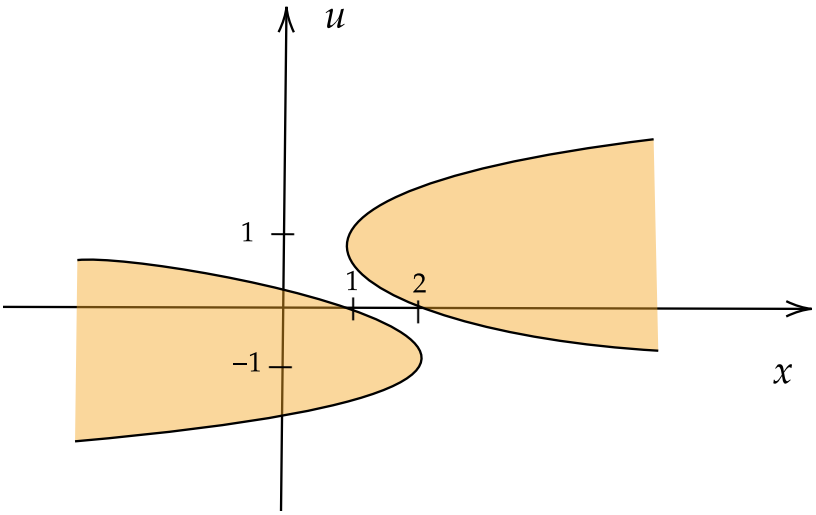


Figure 2.1: Illustration of the set of points (x, u) satisfying (2.11). For every value of x, there are controls (colored in orange) that satisfy (2.11).

the inequality $\big((u-1)^2-(x-1)\big)\big((u+1)^2+(x-2)\big) \leq 0$ strictly, which means that for all $(x, y) \in \partial\mathcal{C}$, there exists $u \in \mathbb{R}$ satisfying (2.10) strictly, and there also exists a neighborhood of $\mathcal{C}$ for which (2.10) is feasible. Hence, the only hypothesis of [103, Lemma III.2] and [104, Theorem 5] that fails is that the system is not control-affine. •

Remark 2.5.6. (Minimal Control Barrier Functions): The work [104] shows that the regularity assumption can be dropped in both Theorems 2.5.3 and 2.5.4. This work identifies the minimal set of conditions that guarantee safety and defines the set of functions satisfying these conditions as *minimal (control) barrier functions* (M(C)BFs). Even though here we focus on CBFs, we also point out various connections of our results to M(C)BFs. •

When dealing with both stability and safety requirements under the dynamics (2.4), one should note that a control input $\mathbf{u}$ might satisfy the CLF constraint (2.5), but not the CBF constraint (2.7), or vice versa. The following definition captures when the CLF and the CBF are compatible.

Definition 2.5.7. (Compatibility of CLF-CBF pair [4, Definition 3]): *Let* $\Gamma \subseteq \mathbb{R}^n$ *be open,* $\mathcal{C} \subset \Gamma$ *closed,* V *a CLF on* Γ *and* h *a CBF of* $\mathcal{C}$*. Then,* V *and* h *are*

(strictly) ***compatible*** *at* $\mathbf{x} \in \mathcal{C}$ *if there exists* $\mathbf{u} \in \mathbb{R}^m$ *satisfying* (2.5) *and* (2.7) *(strictly) simultaneously.*

Given a set $\mathcal{D} \subset \mathbb{R}^n$, we refer to V, h as a compatible pair in $\mathcal{D}$ if they are compatible at every point in $\mathcal{D}$. Similarly, V and h are a strictly compatible pair in $\mathcal{D}$ if they are strictly compatible at every point in $\mathcal{C}\backslash\{\mathbf{0}_n\}$.

For control-affine systems, [31] shows that if V and h are strictly compatible in $\mathcal{C}$, then there exists a smooth safe stabilizing controller. If V and h are only compatible in $\mathcal{C}$, the existence of a smooth safe stabilizing controller is not guaranteed in general. However by including the CBF and CLF inequalities as hard constraints of an optimization problem, one can use the theory of parametric optimization to obtain conditions under which the resulting optimization-based controller satisfies desirable regularity properties without requiring strict compatibility, cf. [8].

Finally we recall the notion of Control Lyapunov-Barrier Function (CLBF) introduced in [28] to design safe stabilizing controllers. Although the original definition is for control-affine systems, here we present it for general control systems of the form (2.4).

Definition 2.5.8. (Control Lyapunov-Barrier Function [28, Definition 2]): *A proper and lower-bounded function* $\bar{V} \in \mathcal{C}^1(\mathbb{R}^n)$ *is a Control Lyapunov-Barrier Function (****CLBF****) of* $\mathbb{R}^n\backslash\mathcal{C}$ *if it satisfies*

$$\bar{V}(\mathbf{x}) > 0 \quad \forall \mathbf{x} \in \mathbb{R}^n\backslash\mathcal{C}, \tag{2.12a}$$

$$\mathcal{U} := \{\mathbf{x} \in \mathbb{R}^n : \bar{V}(\mathbf{x}) \leq 0\} \neq \varnothing, \tag{2.12b}$$

$$(\overline{\mathcal{C}\backslash\mathcal{U}}) \cap (\overline{\mathbb{R}^n\backslash\mathcal{C}}) = \varnothing, \tag{2.12c}$$

$$\inf_{\mathbf{u}\in\mathbb{R}^m} \nabla\bar{V}(\mathbf{x})^T f(\mathbf{x}, \mathbf{u}) < 0 \quad \forall \mathbf{x} \in \mathcal{C}\backslash\{0\}. \tag{2.12d}$$

In the case where $\mathcal{U} = \mathcal{C}$, the conditions (2.12a), (2.12b) are reminiscent of (2.6) (with the sign changed), and (2.12d) is a more restrictive version of the inequality in Definition 2.5.2. On the other hand, the requirement that $\bar{V}$ is proper and (2.12d) resemble the definition of CLF (cf. Definition 2.5.1), although in this case we do not require $\bar{V}$ to be positive definite. Finally, condition (2.12c) is technical and

guarantees that trajectories never enter the unsafe set even if their initial value of $\bar{V}$ is positive (cf. [28, Theorem 2]). This condition is trivially satisfied in the case $\mathcal{U} = \mathcal{C}$. Given a CLBF, [28, Proposition 3] provides an explicit construction of a safe stabilizing controller in $\mathcal{C}$. In particular, this means that if there exists a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$, then $\mathcal{C}$ is safe.

2.6 Boolean Nonsmooth Control Barrier Functions

Here we introduce the notion of Boolean Nonsmooth Control Barrier Function, adapted from [106, Definition II.8].

Definition 2.6.1. (BNCBF): *Given $N \in \mathbb{Z}_{>0}$, let $h_i : \mathbb{R}^n \to \mathbb{R}$, for $i \in [N]$, be continuously differentiable functions. Let $h(\mathbf{x}) = \max_{i \in [N]} h_i(\mathbf{x})$ and let $\mathcal{C}$ satisfy* (2.6)*. Suppose that the set $\mathcal{C}$ is nonempty. Then, h is a BNCBF of $\mathcal{C}$ for* (2.4) *if there exists a locally Lipschitz extended class $\mathcal{K}_\infty$ function $\alpha : \mathbb{R} \to \mathbb{R}$ such that for every $\mathbf{x} \in \mathcal{C}$ there exists $\mathbf{u} \in \mathbb{R}^m$ such that,*

$$\min_{\mathbf{v} \in \partial h(\mathbf{x})} \mathbf{v}^\top (f(\mathbf{x}, \mathbf{u})) \geq -\alpha(h(\mathbf{x})).$$

In case $N = 1$, Definition 2.6.1 reduces to the standard notion of Control Barrier Function [23, Definition 2]. Given $\mathbf{x} \in \mathbb{R}^n$, let $\mathcal{I}(\mathbf{x}) := \{i \in [N] : h(\mathbf{x}) = h_i(\mathbf{x})\}$ denote the set of *active* functions. The following result is adapted from [106, Theorem III.6] and provides a sufficient condition for h to be a BNCBF.

Proposition 2.6.2. (Sufficient Condition for BNCBF): *Suppose there is an extended class $\mathcal{K}_\infty$ function $\alpha : \mathbb{R} \to \mathbb{R}$ such that, for all $\mathbf{x} \in \mathbb{R}^n$, there exists $\mathbf{u} \in \mathbb{R}^m$ with*

$$\nabla h_i(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}) \geq -\alpha(h(\mathbf{x})), \tag{2.13}$$

for all $i \in \mathcal{I}(\mathbf{x})$. Then, h is a BNCBF of $\mathcal{C}$.

If a measurable and locally bounded controller $u_s : \mathbb{R}^n \to \mathbb{R}^m$ is such that, for every $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{u} = u_s(\mathbf{x})$ satisfies (2.13), then u_s renders $\mathcal{C}$ forward invariant (cf. [106, Theorem II.7, Definition II.8]).

When dealing with both safety and stability specifications, it is important to note that an input $\mathbf{u}$ might satisfy (2.5) but not (2.13), or vice versa. The following notion, adapted from [31, Definition 2.3], captures when a CLF V and a BNCBF h are compatible.

Definition 2.6.3. (Compatibility of CLF-BNCBF pair): *Let $\mathcal{D} \subseteq \mathbb{R}^n$ be open, $\mathcal{C} \subset \mathcal{D}$ be closed, V a CLF on $\mathcal{D}$ and h a BNCBF of $\mathcal{C}$. Then, V and h are compatible in a set $\tilde{\mathcal{D}} \subset \mathcal{D}$ if there exist a positive definite function $W : \mathbb{R}^n \to \mathbb{R}$ and an extended class $\mathcal{K}_\infty$ function $\alpha : \mathbb{R} \to \mathbb{R}$ such that, for all $\mathbf{x} \in \tilde{\mathcal{D}}$, there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (2.5) and (2.13) for all $i \in \mathcal{I}(x)$ simultaneously.*

If V and h are compatible in a set $\tilde{\mathcal{D}}$, we can define the minimum norm controller that satisfies the CLF and BNCBF conditions $u^* : \tilde{\mathcal{D}} \to \mathbb{R}^m$ as follows:

$$\begin{aligned} u^*(\mathbf{x}) \coloneqq \arg\min_{u \in \mathbb{R}^m} \ & \frac{1}{2}\|\mathbf{u}\|^2 \\ \text{s.t. } & \nabla V(\mathbf{x})^\top f(\mathbf{x},\mathbf{u}) \leq -W(\mathbf{x}), \\ & \nabla h_i(\mathbf{x})^\top f(\mathbf{x},\mathbf{u}) \geq -\alpha(h(\mathbf{x})),\ \forall\ i \in \mathcal{I}(\mathbf{x}). \end{aligned} \tag{2.14}$$

If u^* is locally Lipschitz, then it ensures that $\mathcal{C}$ is forward invariant and that the origin is asymptotically stable for the closed-loop system.

Remark 2.6.4. (Alternative CLF and CBF conditions): Without loss of generality, if V is a CLF on an open set Γ, we can assume that there exists a positive definite function S such that, for all $\mathbf{x} \in \Gamma$, there is $\mathbf{u} \in \mathbb{R}^m$ with

$$\nabla V(\mathbf{x})^\top f(\mathbf{x},\mathbf{u}) + W(\mathbf{x}) \leq -S(\mathbf{x}). \tag{2.15}$$

This is because if (2.5) holds, we can always define $\tilde{W}(\mathbf{x}) \coloneqq \frac{1}{2}W(\mathbf{x})$ and let $\tilde{W}$ play the role of W in (2.15) and take $S(\mathbf{x}) \coloneqq \frac{1}{2}W(\mathbf{x})$. Similarly, if h is an η-robust CBF, then there exists a class $\mathcal{K}_\infty$ function ζ such that for all $\mathbf{x} \in \mathcal{C}$, there is $\mathbf{u} \in \mathbb{R}^m$ with

$$\nabla h(\mathbf{x})^\top f(\mathbf{x},\mathbf{u}) \geq \eta + \zeta(h(\mathbf{x})). \quad \bullet \tag{2.16}$$

2.7 Constraint Mismatch Variables

Given $N \in \mathbb{Z}_{>0}$, consider a network composed by agents $\{1, \cdots, N\}$ whose communication topology is described by a connected undirected graph $\mathcal{G}$. An edge (i, j) represents the fact that agent i can receive information from agent j and vice versa. For each $i \in [N]$ and $k \in [p]$, where $p \in \mathbb{Z}_{>0}$, let $f_i : \mathbb{R}^n \to \mathbb{R}$ be a strongly convex function and $g_i^k : \mathbb{R}^n \to \mathbb{R}$ a convex function. We consider the following optimization problem with separable objective function and constraints

$$\begin{aligned} &\min_{\mathbf{u} \in \mathbb{R}^{nN}} \sum_{i=1}^{N} f_i(\mathbf{u}_i) \\ &\text{s.t.} \sum_{i \in V(\mathcal{G}_k)} g_i^k(\mathbf{u}_i) \leq 0, \quad k \in [p], \end{aligned} \tag{2.17}$$

where $\mathcal{G}_k$ is a connected subgraph of $\mathcal{G}$ for each $k \in [p]$. For each $k \in [p]$, the constraint in (2.17) couples the local variable $\mathbf{u}_i$ of agent i with the variables of all the other agents in $\mathcal{G}_k$. The constraints in (2.17) can be decoupled by introducing *constraint-mismatch variables* [107, 10], which help agents keep track of local constraints while collectively satisfying the original constraints. Specifically, we add one constraint-mismatch variable per agent and constraint. We let $z_i^k \in \mathbb{R}$ be the constraint-mismatch variable for agent i and constraint k. Let $P_i := \{k \in [p] : i \in V(\mathcal{G}_k)\}$ be the indices of the constraints involving agent i. For convenience, we let $\mathbf{u} = [\mathbf{u}_1, \cdots, \mathbf{u}_N]$, $z_i = \{z_i^k\}_{k \in P_i}$, $\mathbf{z} = [\mathbf{z}_1, \cdots, \mathbf{z}_N]$ and $q := \sum_{i=1}^{N} |P_i|$. Next, consider the problem

$$\begin{aligned} &\min_{\mathbf{u} \in \mathbb{R}^{nN},\ z \in \mathbb{R}^q} \sum_{i=1}^{N} f_i(\mathbf{u}_i) \\ &\text{s.t.} \quad g_i^k(\mathbf{u}_i) + \sum_{j \in \mathcal{N}_i \cap V(\mathcal{G}_k)} (z_i^k - z_j^k) \leq 0,\ i \in V(\mathcal{G}_k),\ k \in [p]. \end{aligned} \tag{2.18}$$

In (7.9), the constraints are now locally expressible, meaning that agent $i \in [N]$ can evaluate the ones in which its variable u_i is present by using variables obtained from its neighbors. The next result establishes the equivalence of (2.17) and (7.9).

Proposition 2.7.1. (Equivalence between the two formulations): *Let $\mathcal{F}^*$ be the solution set of* (7.9). *Then, $\mathbf{u}^* = \Pi_{\mathbf{u}}(\mathcal{F}^*)$ is the optimizer of* (2.17).

The proof is similar to [10, Proposition 4.1], with the necessary modifications to account for the fact that the constraints of (2.17) might only involve a subset of the agents.

2.8 Rapidly-Exploring Random Trees (RRTs)

Here, we review `GEOM-RRT` [64], cf. Algorithm 1, a version of RRT [63] upon which we rely later. The goal of `GEOM-RRT` is to obtain a collision-free path from an initial state to a final state. The input for `GEOM-RRT` consists of a state space

Algorithm 1 `GEOM-RRT`

Parameters: $x_{\text{init}}, \mathcal{X}_{\text{goal}}, k, \eta$
$\mathcal{T}$.init(x_{init})
for $i \in [1, \cdots, k]$ **do**
    $x_{\text{rand}} \leftarrow$ `RANDOM_STATE`
    $x_{\text{near}} \leftarrow$ `NEAREST_NEIGHBOR`($x_{\text{rand}}, \mathcal{T}$)
    $x_{\text{new}} \leftarrow$ `NEW_STATE`($x_{\text{rand}}, x_{\text{near}}, \eta$)
    if `COLLISION_FREE`($x_{\text{near}}, x_{\text{new}}$) **then**
        $\mathcal{T}$.`add_vertex`(x_{new})
        $\mathcal{T}$.`add_edge`($x_{\text{near}}, x_{\text{new}}$)
        if $x_{\text{new}} \in \mathcal{X}_{\text{goal}}$ **then**
            return $\mathcal{T}$
        end if
    end if
end for
return $\mathcal{T}$

$\mathcal{X}$, an initial configuration x_{init}, goal region $\mathcal{X}_{\text{goal}}$, number of iterations k, and a steering parameter η whose use is defined in the sequel. The algorithm builds a tree $\mathcal{T}$ by executing k iterations of the following form:

> At each iteration, a new random sample x_{rand} is obtained by uniformly sampling $\mathcal{X}$ using `RANDOM_STATE`(). The function `NEAREST_NEIGHBOR`($x_{\text{rand}}, \mathcal{T}$)

returns the vertex x_{near} from $\mathcal{T}$ that is closest in the Euclidean distance to x_{rand}. Next, a new configuration $x_{\text{new}} \in \mathcal{X}$ is returned by the `NEW_STATE` function such that x_{new} is on the line segment between x_{near} and x_{rand} and the distance $\|x_{\text{near}} - x_{\text{new}}\|$ is at most η. Finally, the function `COLLISION_FREE`$(x_{\text{near}}, x_{\text{new}})$ checks whether the straight line from x_{near} and x_{new} is collision free. If this is the case, x_{new} is added as a vertex to $\mathcal{T}$ and is connected by an edge from x_{near}. If $x_{\text{new}} \in \mathcal{X}_{\text{goal}}$, there exists a single path in $\mathcal{T}$ from x_{init} to x_{new}.

A notable property of `GEOM-RRT` is that it is *probabilistically complete*, meaning that the probability that the algorithm will return a collision-free path from the initial state to the goal state (if one exists) approaches one as the number of iterations tends to infinity [108].

2.9 Distributionally Robust Chance Constrained Programs

Given a random vector $\boldsymbol{\xi}$ following distribution $\mathbb{P}^*$ supported on set $\Xi \subseteq \mathbb{R}^k$ and a closed convex set $\mathcal{Z} \subset \mathbb{R}^n$, let $G : \mathcal{Z} \times \Xi \to \mathbb{R}$ define a probabilistic constraint $G(z, \boldsymbol{\xi}) \leq 0$. We are interested in satisfying this constraint with a prescribed confidence $1 - \epsilon$, with $\epsilon \in (0, 1)$, while minimizing a convex objective function $c : \mathcal{Z} \to \mathbb{R}$. To achieve this, define the chance-constrained program:

$$\begin{aligned} &\min_{z \in \mathcal{Z}} c(\mathbf{z}) \\ &\text{s.t. } \mathbb{P}^*(G(\mathbf{z}, \boldsymbol{\xi}) \leq 0) \geq 1 - \epsilon. \end{aligned} \tag{2.19}$$

The feasible set of (2.19) is not convex in general. Nemirosvski and Shapiro [109, Section 2] propose a convex approximation of the feasible set of (2.19) by replacing the chance constraint with a conditional value-at-risk (CVaR) constraint. CVaR of $G(z, \boldsymbol{\xi})$ can be formulated as the following convex program:

$$\text{CVaR}^{\mathbb{P}^*}_{1-\epsilon}(G(z, \boldsymbol{\xi}) := \inf_{t \in \mathbb{R}} [\epsilon^{-1} \mathbb{E}_{\mathbb{P}^*}[(G(\mathbf{z}, \boldsymbol{\xi}) + t)_+] - t]. \tag{2.20}$$

The resulting problem

$$\begin{aligned} &\min_{z\in\mathcal{Z}} c(\mathbf{z}) \\ &\text{s.t. } \mathrm{CVaR}^{\mathbb{P}^*}_{1-\epsilon}(G(\mathbf{z},\boldsymbol{\xi})) \le 0, \end{aligned} \tag{2.21}$$

is convex and its feasible set is contained in that of (2.19).

Both (2.19) and (2.21) assume that $\mathbb{P}^*$ is known. Instead, suppose that it is unknown and we only have access to samples $\{\boldsymbol{\xi}_i\}_{i\in[N]}$ from $\mathbb{P}^*$. We describe a way of constructing a set of distributions that could have generated the samples. Let $\mathcal{P}_p(\Xi)$ be the set of probability measures with finite p-th moment supported on Ξ. Let $\hat{\mathbb{P}}_N := \frac{1}{N}\sum_{i=1}^N \delta_{\boldsymbol{\xi}_i}$ be the empirical distribution constructed from the samples $\{\boldsymbol{\xi}_i\}_{i=1}^N$. Let W_p be the p-Wasserstein distance [110, Definition 3.1] between two probability measures in $\mathcal{P}_p(\Xi)$ and let $\mathcal{M}_N^r := \{\mu \in \mathcal{P}_p(\Xi) : W_p(\mu, \hat{\mathbb{P}}_N) \le r\}$ be the ball of radius r centered at $\hat{\mathbb{P}}_N$. We define the following distributionally robust chance-constrained program:

$$\begin{aligned} &\min_{z\in\mathcal{Z}} c(\mathbf{z}) \\ &\text{s.t. } \inf_{\mathbb{P}\in\mathcal{M}_N^r} \mathbb{P}(G(\mathbf{z},\boldsymbol{\xi}) \le 0) \ge 1-\epsilon. \end{aligned} \tag{2.22}$$

We can use CVaR to obtain a convex conservative approximation of (2.22):

$$\begin{aligned} &\min_{z\in\mathcal{Z}} c(\mathbf{z}) \\ &\text{s.t. } \sup_{\mathbb{P}\in\mathcal{M}_N^r} \mathrm{CVaR}^{\mathbb{P}}_{1-\epsilon}(G(\mathbf{z},\boldsymbol{\xi})) \le 0. \end{aligned} \tag{2.23}$$

If (2.23) is feasible, then (2.22) is also feasible [109, Section 2].

We say that a distribution $\mathbb{P}$ is light-tailed if there exists $a > 0$ such that $\mathbb{E}_{\mathbb{P}}[\exp \|\boldsymbol{\xi}\|^a] = \int_\Xi \exp \|\boldsymbol{\xi}\|^a \mathbb{P}(d\boldsymbol{\xi}) < \infty$. If $\mathbb{P}^*$ is light-tailed, the following observation specifies how the radius of $\mathcal{M}_N^r$ should be selected so that the true distribution lies in the ball with high confidence.

Remark 2.9.1. (Choice of Wasserstein ball radius): *If the true distribution $\mathbb{P}^*$ is light-tailed, the choice of $r = r_N(\bar{\epsilon})$ given in [110, Theorem 3.5],*

$$r_N(\bar{\epsilon}) = \begin{cases} \left(\frac{\log(c_1\bar{\epsilon}^{-1})}{c_2 N}\right)^{\frac{1}{\max\{m,2\}}} & \text{if } N \ge \frac{\log(c_1\bar{\epsilon}^{-1})}{c_2}, \\ \left(\frac{\log(c_1\bar{\epsilon}^{-1})}{c_2 N}\right)^{\frac{1}{a}} & \text{else,} \end{cases} \tag{2.24}$$

where c_1, c_2 and a are distribution-dependent positive constants (cf. [110, Theorem 3.4]), ensures that the ball $\mathcal{M}_N^{r_N(\bar{\epsilon})}$ contains $\mathbb{P}^*$ with probability at least $1-\bar{\epsilon}$. Then, a solution $\mathbf{z}^*$ of (2.23) satisfies the constraint $\mathrm{CVaR}_{1-\epsilon}^{\mathbb{P}^*}(G(z^*, \boldsymbol{\xi})) \leq 0$ with probability at least $1-\bar{\epsilon}$. •

Remark 2.9.2. (Choice of ϵ): *The parameter ϵ determines the confidence level $1-\epsilon$ for constraint satisfaction. Throughout the paper, we assume $\epsilon \leq \frac{1}{N}$, albeit results are valid generally, with explicit expressions becoming more involved.* •

2.10 Constraint Qualifications in Nonlinear Programming

Let $V_0, \cdots, V_q : \mathbb{R}^d \to \mathbb{R}$ be differentiable functions, and consider a nonlinear optimization problem of the form

$$\begin{aligned} &\min_{\boldsymbol{\theta} \in \mathbb{R}^d} V_0(\boldsymbol{\theta}) \\ &\text{s.t.} \quad V_i(\boldsymbol{\theta}) \leq 0, \ i \in [q], \end{aligned} \tag{2.25}$$

where $V_0, \cdots, V_q$ are continuously differentiable. We also let the active and inactive constraint sets be

$$\begin{aligned} I_0(\boldsymbol{\theta}) &= \{i \in [q] : V_i(\boldsymbol{\theta}) = 0\}, \\ I_-(\boldsymbol{\theta}) &= \{i \in [q] : V_i(\boldsymbol{\theta}) < 0\}. \end{aligned}$$

We say that:

- Slater's condition (SC) holds for (2.25) if there exists $\boldsymbol{\theta} \in \mathbb{R}^d$ such that $V_i(\boldsymbol{\theta}) < 0$ for all $i \in [q]$;
- the Mangasarian-Fromovitz Constraint Qualification (MFCQ) holds for (2.25) at $\boldsymbol{\theta} \in \mathbb{R}^d$ if there exist $\boldsymbol{\xi} \in \mathbb{R}^d$ such that $\nabla V_i(\boldsymbol{\theta})^\intercal \boldsymbol{\xi} < 0$ for all $i \in I_0(\boldsymbol{\theta})$;
- the constant rank condition (CRC) holds for (2.25) at $\boldsymbol{\theta} \in \mathbb{R}^d$ if there exists an open set U containing $\boldsymbol{\theta}$ such that for all $I \subset I_0(\boldsymbol{\theta})$ the rank of $\{\nabla V_i(\bar{\boldsymbol{\theta}})\}_{i \in I}$ is constant for all $\bar{\boldsymbol{\theta}} \in U$;

If $\boldsymbol{\theta}^*$ is a local minimizer of (2.25), and any of the two constraint qualification conditions above hold at $\boldsymbol{\theta}^*$, then there exist $\mathbf{u}^* \in \mathbb{R}^q$ such that the *Karush-Kuhn-Tucker* conditions hold:

$$\nabla V_0(\boldsymbol{\theta}^*) + \sum_{i=1}^{q} u_i^* \nabla V_i(\boldsymbol{\theta}^*) = 0, \tag{2.26a}$$

$$V_i(\boldsymbol{\theta}^*) \leq 0,\ u_i^* \geq 0,\ u_i^* V_i(\boldsymbol{\theta}^*) = 0. \tag{2.26b}$$

Any $\boldsymbol{\theta}^* \in \mathbb{R}^d$ for which there exists $\mathbf{u}^* \in \mathbb{R}^q$ satisfying (2.26) is referred to as a KKT point of (2.25).

Let $(\boldsymbol{\theta}^*, \mathbf{u}^*) \in \mathbb{R}^d \times \mathbb{R}^q$ be a KKT point of the optimization problem in (2.25). Then, $(\boldsymbol{\theta}^*, \mathbf{u}^*)$ satisfies Strict Complementary Slackness (SCS) if there does not exist $i \in [p]$ such that $u_i^* = 0$ and $V_i(\boldsymbol{\theta}^*) = 0$.

Consider a version of (2.25) parameterized by a vector $\mathbf{x} \in \mathbb{R}^n$. I.e., let $\tilde{V}_0, \cdots, \tilde{V}_q : \mathbb{R}^n \times \mathbb{R}^d$ be differentiable functions and consider the problem

$$\begin{aligned} &\min_{\boldsymbol{\theta} \in \mathbb{R}^d} V_0(\mathbf{x}, \boldsymbol{\theta}) \\ &\text{s.t.} \quad V_i(\mathbf{x}, \boldsymbol{\theta}) \leq 0,\ i \in [q]. \end{aligned} \tag{2.27}$$

Local compact feasibility (LCF) holds at $\mathbf{x} \in \mathbb{R}^n$ if there exists a compact set $K \subset \mathbb{R}^d$ and $\delta > 0$ such that for all $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}\| < \delta$, there exists $\boldsymbol{\theta} \in K$ such that $V_i(\mathbf{x}, \boldsymbol{\theta}) \leq 0$ for all $i \in [q]$.

Let the active constraint set be defined by

$$I_0(\mathbf{x}, \boldsymbol{\theta}) = \{i \in [q] : V_i(\mathbf{x}, \boldsymbol{\theta}) \leq 0\}.$$

We say that the constant-rank condition (CRC) holds for (2.27) at $(\mathbf{x}_0, \boldsymbol{\theta}_0) \in \mathbb{R}^n \times \mathbb{R}^d$ if there exists a neighborhood $\mathcal{N}$ of $(\mathbf{x}_0, \boldsymbol{\theta}_0)$ such that for any $\tilde{I} \subset \tilde{I}_0(\mathbf{x}_0, \boldsymbol{\theta}_0)$ and $(\mathbf{x}, \boldsymbol{\theta}) \in \mathcal{N}$, $\{\nabla_{\boldsymbol{\theta}} V_i(\mathbf{x}, \boldsymbol{\theta})\}_{i \in \tilde{I}}$ has a constant rank.

Part I

Control Design with Safety and Stability Guarantees

Chapter 3

Optimization-Based Safe Stabilizing Feedback with Guaranteed Region of Attraction

This chapter proposes an optimization with penalty-based feedback design framework for safe stabilization of control-affine systems. Our starting point is the availability of a CLF and a CBF, which for control-affine systems define affine inequalities in the input that certify stability and safety, respectively. By leveraging ideas from penalty methods for constrained optimization, our proposed design imposes one of the constraints as a hard constraint and the other one as a soft constraint. This defines a feedback law that is obtained as the solution of an optimization problem. We study the properties of the resulting closed-loop system and identify conditions on the penalty parameter that allow us to eliminate undesired equilibra that might arise. Furthermore, we provide an inner approximation of the region of attraction of the origin, and identify conditions under which the whole safe set belongs to it. We illustrate our results through simulations.

3.1 Problem Statement

We are interested in designing controllers that are both stabilizing and safe. We also require them to be Lipschitz in order to guarantee existence and uniqueness

of solutions of the closed-loop system. Consider a control-affine system of the form

$$\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}, \tag{3.1}$$

where $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^m$ are Lipschitz functions, with $\mathbf{x} \in \mathbb{R}^n$ the state and $\mathbf{u} \in \mathbb{R}^m$ the input.

Let $V : \mathbb{R}^n \to \mathbb{R}$ be a CLF of (3.1) on an open set $\mathcal{D}$, and $h : \mathbb{R}^n \to \mathbb{R}$ be a CBF of the closed set $\mathcal{C} \subset \mathcal{D}$. We assume that the origin belongs to $\mathcal{C}$. Given the availability of these functions, we want do design a controller that uses V to ensure the stabilizing aspect of the controller and h to ensure safety. We also seek to provide a formal characterization of the region of attraction of the origin for the resulting closed-loop system.

However, [32] gives a counterexample that shows that this pointwise minimization can result in a non-Lipschitz controller. To remedy this, and also to extend the design to scenarios where V and h might not be compatible at some points in the safe set, a popular approach [23] is to relax one of the inequalities (2.5), (2.7) (in safety-critical applications, the CLF constraint (2.5)), and formulate a QP that penalizes the relaxation parameter:

$$\begin{aligned} u(\mathbf{x}) = \arg \min_{(\mathbf{u},\delta)\in\mathbb{R}^{m+1}} \ & \frac{1}{2}\|\mathbf{u}\|^2 + p\delta^2, \\ \text{s.t.} \quad & (2.7),\ L_f V(\mathbf{x}) + L_g V(\mathbf{x})u \le -W(\mathbf{x}) + \delta. \end{aligned} \tag{3.2}$$

Nevertheless, even in the case where the CLF and the CBF are compatible at all points in the safe set, the resulting controller might not be stabilizing even for arbitrarily large values of p [33]. Moreover, as pointed out in [34, 35], this design might introduce undesired equilibria in the closed-loop system, which can even be asymptotically stable. To the best of the authors' knowledge, only local stability guarantees exist in this line of work [35, Theorem 3],[33, Theorem 1]. and no estimates of the region of attraction have been given in the literature. However, by modifying (3.2) through the introduction of a nominal controller, [35] show that it is possible to give an estimate of the region of attraction of the origin.

An alternative design, e.g., [36], assumes a nominal (possibly unsafe) stabilizing controller u_{nom} is available, and seeks to modify it as little as possible while

guaranteeing safety. This can be done by solving the following QP:

$$u(\mathbf{x}) = \arg\min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\left\|\mathbf{u} - u_{\text{nom}}(\mathbf{x})\right\|^2, \quad \text{s.t.} \quad (2.7). \tag{3.3}$$

We refer to this design as a *safety filter*. In general, the resulting modified controller might not retain the stability properties of the original nominal controller but, under certain conditions [111], one can provide an estimate of the region of attraction of the equilibrium.

We are interested in building an alternative to the designs (3.2), (3.3) with improved properties. In particular, we tackle the following problem:

Problem 1. *Determine a Lipschitz control law $u : \mathbb{R}^n \to \mathbb{R}^m$ and a region of attraction $\Gamma \subseteq \mathbb{R}^n$, $\Gamma \cap \mathcal{C} \neq 0$ such that for all $x(0) \in \Gamma \cap \mathcal{C}$, $x(t) \in \mathcal{C}$ for all $t \geq 0$ and the system* (3.1) *in closed-loop with u is asymptotically stable with respect to the origin.* △

3.2 Safety and Stability via QP with Penalty

In this section we design a candidate control law to solve Problem 1 by leveraging the CLF V and the CBF h. We first present our exposition in a general context, then particularize to our setting. Consider general Lipschitz functions $a, c : \mathbb{R}^n \to \mathbb{R}$ and $b, d : \mathbb{R}^n \to \mathbb{R}^m$. Consider the following two affine inequalities in $\mathbf{u} \in \mathbb{R}^m$,

$$a(\mathbf{x}) + b(\mathbf{x})\mathbf{u} \leq 0, \quad c(\mathbf{x}) + d(\mathbf{x})\mathbf{u} \leq 0.$$

Given a neighborhood $\bar{\mathcal{C}}$ of $\mathcal{C}$, we assume that for every $\mathbf{x} \in \bar{\mathcal{C}}$, there exist $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{R}^m$ such that $a(\mathbf{x}) + b(\mathbf{x})\mathbf{u}_1 \leq 0$ and $c(\mathbf{x}) + d(\mathbf{x})\mathbf{u}_2 \leq 0$. To select $\mathbf{u}$, we regard at the first inequality as a *soft constraint* and the second as a *hard constraint*. Inspired by the theory of penalty methods for constrained optimization [112, Chapter 13], we formulate a QP where we include the soft constraint in the objective function with a penalty parameter ($\epsilon > 0$) and enforce the hard constraint. The resulting

solution of the QP is parametrized by $\mathbf{x} \in \mathbb{R}^n$ and ϵ:

$$u_\epsilon(\mathbf{x}) := \arg\min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\|\mathbf{u}\|^2 + \frac{1}{\epsilon}(a(\mathbf{x}) + b(\mathbf{x})\mathbf{u}),$$
$$\text{s.t.} \quad c(\mathbf{x}) + d(\mathbf{x})\mathbf{u} \le 0. \tag{3.4}$$

Since this optimization problem is a QP, it is convex. The following result gives a closed-form expression for u_ϵ and establishes that it is Lipschitz.

Proposition 3.2.1. (Closed-form expression for Lipschitz controller): *Let $a, c : \mathbb{R}^n \to \mathbb{R}$ and $b, d : \mathbb{R}^n \to \mathbb{R}^m$ be Lipschitz, $\bar{\mathcal{C}}$ a neighborhood of $\mathcal{C}$ and assume that for every $\mathbf{x} \in \bar{\mathcal{C}}$, there exist $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{R}^m$ such that $a(\mathbf{x}) + b(\mathbf{x})\mathbf{u}_1 \le 0$ and $c(\mathbf{x}) + d(\mathbf{x})\mathbf{u}_2 \le 0$. For each $\mathbf{x} \in \mathcal{C}$, let $H(\mathbf{x}) := \{\mathbf{u} \in \mathbb{R}^m : c(\mathbf{x}) + d(\mathbf{x})u = 0\}$ and $e(\mathbf{x}) := c(\mathbf{x}) - \frac{1}{\epsilon}d(\mathbf{x})b(\mathbf{x})$. Then,*

$$u_\epsilon(\mathbf{x}) = \begin{cases} -\frac{1}{\epsilon}b(\mathbf{x}) & \text{if } e(\mathbf{x}) \le 0, \\ P_{H(\mathbf{x})}(-\frac{1}{\epsilon}b(\mathbf{x})) & \text{if } e(\mathbf{x}) > 0, \end{cases} \tag{3.5}$$

and u_ϵ is Lipschitz on $\bar{\mathcal{C}}\backslash\{\mathbf{0}_n\}$. Moreover, if $d(\mathbf{0}_n) \neq \mathbf{0}_m$, u_ϵ is Lipschitz at $\mathbf{0}_n$.

Proof. The expression (3.5) follows by calculating the KKT points of (3.4). Note that (3.5) is well defined because if $d(\mathbf{x}) = 0$, necessarily $e(\mathbf{x}) = c(\mathbf{x}) \le 0$. Lipschitzness of $u_\epsilon(\mathbf{x})$ follows from [113, Section 3.10, Theorem 2], which as a special case includes the minimization of a quadratic cost function subject to affine inequality constraints. □

We next particularize the general design (3.4) to our setup. We consider two cases:

Safety QP with stability penalty: The selection $a(\mathbf{x}) = L_fV(\mathbf{x}) + W(\mathbf{x})$, $b(\mathbf{x}) = L_gV(\mathbf{x})$, $c(\mathbf{x}) = -L_fh(\mathbf{x}) - \alpha(h(\mathbf{x}))$, and $d(\mathbf{x}) = -L_gh(\mathbf{x})$ makes the CLF inequality (2.5) a soft constraint and the CBF inequality (2.7) a hard one. We denote by u_ϵ^{safe} the controller resulting from (3.4). If $L_gh(\mathbf{0}_n) \neq \mathbf{0}_n$, Proposition 3.2.1 guarantees that u_ϵ^{safe} is Lipschitz on $\mathcal{C}$. Moreover, since it satisfies the CBF inequality (2.7) for all $\mathbf{x} \in \mathcal{C}$, the resulting closed-loop system is safe for all $\epsilon > 0$;

Stability QP with safety penalty: Alternatively, the selection $a(\mathbf{x}) = -L_fh(\mathbf{x}) - \alpha(h(\mathbf{x}))$, $b(\mathbf{x}) = -L_gh(\mathbf{x})$, $c(\mathbf{x}) = L_fV(\mathbf{x}) + W(\mathbf{x})$, and $d(\mathbf{x}) = L_gV(\mathbf{x})$, makes the

CBF inequality (2.7) a soft constraint and the CLF inequality (2.5) a hard one. We denote by $u_\epsilon^{\text{stable}}$ the resulting controller from (3.4). In this case, $d(\mathbf{0}_n) = \mathbf{0}_m$ and hence Proposition 3.2.1 only guarantees that $u_\epsilon^{\text{stable}}$ is Lipschitz in $\bar{\mathcal{C}}\backslash\{\mathbf{0}_n\}$. Moreover, since (2.5) is satisfied for all $x \in \bar{\mathcal{C}}\backslash\{\mathbf{0}_n\}$, the origin is asymptotically stable for the resulting closed-loop system.

From this point onwards, we formulate the results for the controller u_ϵ^{safe}. With minor modifications, similar results can be stated for $u_\epsilon^{\text{stable}}$. Note also that Proposition 3.2.1 provides a closed-form expression for the controllers. This allows the closed-loop system to be implemented without having to continuously solve the optimization (3.4), which is something one faces when dealing with (3.2), e.g. [23].

Remark 3.2.2. (Nominal Controller): *Our framework can be adapted to the scenario described in* (3.3)*, where instead of a CLF, one has access to a nominal stabilizing controller* u_{nom} *and a certificate of stability in the form of a Lyapunov function* V *satisfying* $L_f V(\mathbf{x}) + L_g V(\mathbf{x}) u_{\text{nom}}(\mathbf{x}) + W(\mathbf{x}) \leq 0$ *for* $\mathbf{x} \in \mathcal{D}$*, with* $\mathcal{D}$ *some open set. To design a control* $\mathbf{u}$ *as close as possible to* u_{nom} *that is safe and stabilizing, one can set* $\mathbf{v} = \mathbf{u} - u_{\text{nom}}$*. Then, it is easy to check that* V *is a CLF for* $\dot{\mathbf{x}} = \bar{f}(\mathbf{x}) + g(\mathbf{x})\mathbf{v}$*, where* $\bar{f}(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}) u_{\text{nom}}(\mathbf{x})$*. In this case, one could use the safety QP with stability penalty setting* $a(\mathbf{x}) = L_{\bar{f}} V(\mathbf{x}) + W(\mathbf{x})$*,* $b(\mathbf{x}) = L_g V(\mathbf{x})$*,* $c(\mathbf{x}) = -L_{\bar{f}} h(\mathbf{x}) - \alpha(h(\mathbf{x}))$*, and* $d(\mathbf{x}) = -L_g h(\mathbf{x})$*.* •

3.3 Analysis of Safety QP with Stability Penalty

In this section we analyze the closed-loop properties of (3.1) under u_ϵ^{safe}. We first show how to choose ϵ to avoid undesired equilibria of the closed-loop system and then go on to solve Problem 1. Throughout the section, we let

$$e(\mathbf{x}) = -L_f h(\mathbf{x}) + \frac{1}{\epsilon} L_g h(\mathbf{x})^\top L_g V(\mathbf{x}) - \alpha(h(\mathbf{x})).$$

3.3.1 Ruling out Undesired Equilibrium Points

Here we show that the closed-loop implementation of the safety QP with stability penalty controller might introduce new equilibria other than the origin. The

next result characterizes such equilibria and shows that, under some conditions, they can be confined to an arbitrarily small neighborhood of the origin for small enough ϵ.

Proposition 3.3.1. (Characterization of Equilibria): *For $\epsilon > 0$, the set of equilibrium points of the closed-loop system $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})u_\epsilon^{\text{safe}}(\mathbf{x})$ in $\mathcal{C}$ is $\mathcal{Q} = \mathcal{Q}_1^\epsilon \cup \mathcal{Q}_2^\epsilon$, with*

$$\mathcal{Q}_1^\epsilon := \{\mathbf{x} \in \mathcal{C} : e(\mathbf{x}) \leq 0,\ f(\mathbf{x}) = \frac{1}{\epsilon} g(\mathbf{x}) L_g V(\mathbf{x})\},$$
$$\mathcal{Q}_2^\epsilon := \{\mathbf{x} \in \partial\mathcal{C} : e(\mathbf{x}) > 0,\ f(\mathbf{x}) = \frac{L_f h(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} g(\mathbf{x}) L_g h(\mathbf{x}) +$$
$$\frac{g(\mathbf{x})}{\epsilon}(L_g V(\mathbf{x}) - \frac{L_g h(\mathbf{x})^\top L_g V(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} L_g h(\mathbf{x}))\},$$

and $\mathbf{0}_n \in \mathcal{Q}_1^\epsilon$. Let $\mathcal{V}$ be a neighborhood of the origin, $\bar{\mathcal{V}}$ a neighborhood of $P_g := \{\mathbf{x} \in \mathcal{C}\backslash\{\mathbf{0}_n\} : L_g V(\mathbf{x}) = \mathbf{0}_m\}$ and let N_1, N_2, $N_3^{\mathcal{V},\bar{\mathcal{V}}}$ and N_4 be defined by

$$N_1 := \sup_{\mathbf{x}\in\mathcal{C}} \|f(\mathbf{x})\|,$$
$$N_2 := \sup_{\substack{\mathbf{x}\in\partial\mathcal{C} \\ e(\mathbf{x})>0}} \left\| f(\mathbf{x}) - \frac{L_f h(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} g(\mathbf{x}) L_g h(\mathbf{x}) \right\|,$$
$$N_3^{\mathcal{V},\bar{\mathcal{V}}} := \inf_{\mathbf{x}\in\mathcal{C}\backslash(\mathcal{V}\cup\bar{\mathcal{V}})} \|g(\mathbf{x}) L_g V(\mathbf{x})\|.$$
$$N_4 := \inf_{\substack{\mathbf{x}\in\partial\mathcal{C} \\ e(\mathbf{x})>0}} \left\| g(\mathbf{x})(L_g V(\mathbf{x}) - \frac{L_g h(\mathbf{x})^\top L_g V(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} L_g h(\mathbf{x})) \right\|.$$

then,

- *if N_1 is finite, then $\mathcal{Q}_1^\epsilon \subseteq \mathcal{V}$ for all $0 < \epsilon < \frac{N_3^{\mathcal{V},\bar{\mathcal{V}}}}{N_1}$,*
- *if N_2 is finite and N_4 is positive, then $\mathcal{Q}_2^\epsilon = \varnothing$ for $0 < \epsilon < \frac{N_4}{N_2}$.*

Proof. Since $u_\epsilon^{\text{safe}}(\mathbf{x})$ takes a different form depending on the sign of $e(\mathbf{x})$, we distinguish two cases:

Case 1: $e(\mathbf{x}) \leq 0$: In this case, the equilibrium points of the closed-loop system satisfy $f(\mathbf{x}) = \frac{1}{\epsilon} g(\mathbf{x}) L_g V(\mathbf{x})$. Note that if $g(\mathbf{x}) L_g V(\mathbf{x}) = \mathbf{0}_n$, by multiplying on the left by $\nabla V(\mathbf{x})^\top$ we obtain $L_g V(\mathbf{x}) = \mathbf{0}_m$. Since V is a CLF, $L_f V(\mathbf{x}) < 0$ if $\mathbf{x} \neq \mathbf{0}_n$.

This implies that $f(\mathbf{x}) \neq \mathbf{0}_n$ and hence $\mathbf{x}$ is not an equilibrium point. Hence, no point other than the origin satisfies $L_gV(\mathbf{x}) = \mathbf{0}_m$ and $f(\mathbf{x}) = \frac{1}{\epsilon}g(\mathbf{x})L_gV(\mathbf{x})$, and we can choose a neighborhood $\bar{\mathcal{V}}$ of P_g with $\mathcal{Q}_1^\epsilon \cap \bar{\mathcal{V}} = \varnothing$. Now, by taking any neighborhood $\mathcal{V}$ of the origin, the choice $\epsilon < \frac{N_3^{\mathcal{V},\bar{\mathcal{V}}}}{N_1}$ rules out any equilibrium of this kind in $\mathcal{C}\backslash\mathcal{V}$. Note that, since $f(\mathbf{0}_n) = \mathbf{0}_n$ and $\nabla V(\mathbf{0}_n) = \mathbf{0}_n$, we have $e(\mathbf{0}_n) = -\alpha(h(\mathbf{0}_n)) \leq 0$, and hence $\mathbf{0}_n \in \mathcal{Q}_1^\epsilon$.

Case 2: $e(\mathbf{x}) > 0$: In this case the equilibrium points of the closed-loop system satisfy

$$f(\mathbf{x}) - \frac{L_fh(\mathbf{x}) + \alpha(h(\mathbf{x}))}{\|L_gh(\mathbf{x})\|^2} g(\mathbf{x})L_gh(\mathbf{x}) = \frac{g(\mathbf{x})}{\epsilon}(L_gV(\mathbf{x}) - \frac{L_gh(\mathbf{x})^T L_gV(\mathbf{x})}{\|L_gh(\mathbf{x})\|^2} L_gh(\mathbf{x})). \tag{3.6}$$

Let us show that these equilibria can only occur in $\partial\mathcal{C}$. Multiplying both sides of (3.6) by $\nabla h(\mathbf{x})^\top$, we obtain $-\alpha(h(\mathbf{x})) = 0$. Since α is a class $\mathcal{K}_\infty$ function, this can only occur when $h(\mathbf{x}) = 0$, i.e., $\mathbf{x} \in \partial\mathcal{C}$. Now, by taking $\epsilon < \frac{N_4}{N_2}$, all equilibrium points of these kind are ruled out. □

Note that the assumption that N_1 and N_2 are finite in Proposition 3.3.1 is satisfied if $\mathcal{C}$ is bounded. The neighborhood $\mathcal{V}$ of the origin in the statement can be taken arbitrarily small and, consequently, if N_4 is positive, the controller u_ϵ^{safe} with sufficiently small ϵ confines the equilibria of the closed-loop system arbitrarily close to the origin. However, as $\mathcal{V}$ gets arbitrarily small, $N_3^{\mathcal{V}}$ (and hence ϵ) could also get arbitrarily small. In Corollary 3.3.5 later, we give sufficient conditions to ensure that this does not happen.

Remark 3.3.2. (Existence of boundary equilibria): *The assumption that N_4 is positive is not satisfied if $g(\mathbf{x})L_gV(\mathbf{x})$ and $g(\mathbf{x})L_gh(\mathbf{x})$ are linearly dependent for some $\mathbf{x} \in \partial\mathcal{C}$ such that $e(\mathbf{x}) > 0$. In this scenario, by using condition* (3.6) *we infer that the equilibrium points in $\partial\mathcal{C}$ that can not be removed by tuning ϵ are those where $f(\mathbf{x})$, $g(\mathbf{x})L_gV(\mathbf{x})$ and $g(\mathbf{x})L_gh(\mathbf{x})$ are collinear and $e(\mathbf{x}) > 0$ for all ϵ.* •

3.3.2 Incompatibility and Region of Attraction

Here we show that u_ϵ^{safe} solves Problem 1. The flexibility provided by the design parameter ϵ is instrumental in doing so. We first introduce a characterization of points where the CLF and the CBF are incompatible, the proof of which follows as a special case of [114, Theorem 1].

Lemma 3.3.3. (Characterization of incompatible points): *Let $\mathcal{D} \subseteq \mathbb{R}^n$ be open, $\mathcal{C} \subset \mathcal{D}$ closed, V a CLF on $\mathcal{D}$ and h a CBF of $\mathcal{C}$. V and h are incompatible at $\mathbf{x} \in \mathcal{C}$ if and only if $L_gV(\mathbf{x})$ and $L_gh(\mathbf{x})$ are linearly dependent, $L_gV(\mathbf{x})^\top L_gh(\mathbf{x}) > 0$ and $L_fV(\mathbf{x}) + W(\mathbf{x}) > \frac{L_gV(\mathbf{x})^\top L_gh(\mathbf{x})}{\|L_gh(\mathbf{x})\|^2}(L_fh(\mathbf{x}) + \alpha(h(\mathbf{x})))$.*

The next result shows that, by taking ϵ sufficiently small for the closed-loop system, any level set of V that does not contain incompatible points is a region of attraction of a neighborhood of the origin.

Theorem 3.3.4. (Parameter tuning for guaranteed region of attraction): *Let $\mathcal{D} \subseteq \mathbb{R}^n$ be open, $\mathcal{C} \subset \mathcal{D}$ closed, V a CLF on $\mathcal{D}$ and h a CBF of $\mathcal{C}$. Let $\nu > 0$ be such that the sublevel set $\Gamma_\nu = \{\mathbf{x} \in \mathbb{R}^n : V(\mathbf{x}) \leq \nu\}$ does not contain any incompatible points. For $\mathbf{x}$ such that $e(\mathbf{x}) > 0$ (which implies $L_gh(\mathbf{x}) \neq \mathbf{0}_m$ since h is a CBF), define*

$$B(\mathbf{x}) := L_fV(\mathbf{x}) + W(\mathbf{x}) - \frac{L_fh(\mathbf{x}) + \alpha(h(\mathbf{x}))}{\|L_gh(\mathbf{x})\|^2} L_gV(\mathbf{x})^\top L_gh(\mathbf{x}),$$
$$C(\mathbf{x}) := \frac{(L_gV(\mathbf{x})^\top L_gh(\mathbf{x}))^2}{\|L_gh(\mathbf{x})\|^2} - \|L_gV(\mathbf{x})\|^2.$$

Let $\mathcal{V}$ be a neighborhood of the origin, $\bar{\mathcal{V}}$ a neighborhood of $P_g := \{\mathbf{x} \in \mathcal{C} \backslash \{\mathbf{0}_n\} : L_gV(\mathbf{x}) = \mathbf{0}_m\}$ such that $L_fV(\mathbf{x}) + W(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \bar{\mathcal{V}}$ and $\mathcal{W}$ a neighborhood of $P_\nu = \{\mathbf{x} \in \Gamma_\nu : e(\mathbf{x}) > 0, C(\mathbf{x}) = 0\}$ such that $e(\mathbf{x}) > 0$ and $B(\mathbf{x}) \leq 0$ for all

$\mathbf{x} \in \mathcal{W} \backslash \{\mathbf{0}_n\}$. *Define constants* M_1^ν, M_2^ν, $M_3^{\nu,\mathcal{V},\bar{\mathcal{V}}}$ *and* $M_4^{\nu,\mathcal{V},\mathcal{W}}$ *by*

$$
\begin{aligned}
M_1^\nu &:= \sup_{\mathbf{x} \in \Gamma_\nu} |L_f V(\mathbf{x}) + W(\mathbf{x})|, \\
M_2^\nu &:= \sup_{\substack{\mathbf{x} \in \Gamma_\nu \\ e(\mathbf{x}) > 0}} \left| \frac{L_f h(\mathbf{x}) + \alpha(h(\mathbf{x}))}{\|L_g h(\mathbf{x})\|^2} L_g h(\mathbf{x})^T L_g V(\mathbf{x}) \right|, \\
M_3^{\nu,\mathcal{V},\mathcal{V}} &:= \inf_{\mathbf{x} \in \Gamma_\nu \backslash (\mathcal{V} \cup \bar{\mathcal{V}})} \|L_g V(\mathbf{x})\|^2, \\
M_4^{\nu,\mathcal{V},\mathcal{W}} &:= \inf_{\substack{x \in \Gamma_\nu \backslash (\mathcal{W} \cup \mathcal{V}) \\ e(\mathbf{x}) > 0}} |C(\mathbf{x})|.
\end{aligned}
$$

Then, for $\epsilon < \bar{\epsilon} := \min\{\frac{M_4^{\nu,\mathcal{V},\mathcal{W}}}{M_1^\nu + M_2^\nu}, \frac{M_3^{\nu,\mathcal{V},\bar{\mathcal{V}}}}{M_1^\nu}\}$, $\mathcal{V}$ *is asymptotically stable and* $\Gamma_\nu \cap \mathcal{C}$ *is forward invariant and a subset of the region of attraction of* $\mathcal{V}$.

Proof. Let $z_\epsilon(\mathbf{x}) := L_f V(\mathbf{x}) + L_g V(\mathbf{x}) u_\epsilon^{\text{safe}}(\mathbf{x}) + W(\mathbf{x})$. It follows from (3.5) that

$$
z_\epsilon(\mathbf{x}) = \begin{cases} L_f V(\mathbf{x}) + W(\mathbf{x}) - \frac{1}{\epsilon} \|L_g V(\mathbf{x})\|^2 & \text{if } e(\mathbf{x}) \leq 0, \\ B(\mathbf{x}) + \frac{1}{\epsilon} C(\mathbf{x}) & \text{if } e(\mathbf{x}) > 0. \end{cases}
$$

We show that $z_\epsilon(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \mathcal{C} \backslash \mathcal{V}$ if $\epsilon < \bar{\epsilon}$, from which the result follows. First, note that $\bar{\mathcal{V}}$ as required in the statement exists because V is a CLF and hence, any point $\mathbf{x} \neq \mathbf{0}_n$ that satisfies $L_g V(\mathbf{x}) = \mathbf{0}_n$ is such that $L_f V(\mathbf{x}) + W(\mathbf{x}) < 0$ (without loss of generality, since if $L_f V(\mathbf{x}) + W(\mathbf{x}) = 0$ we can take $\tilde{W}(\mathbf{x}) = \frac{1}{2} W(\mathbf{x})$). Hence, by continuity there exists a neighborhood $\bar{\mathcal{V}}$ of P_g where $L_f V(\mathbf{x}) + W(\mathbf{x}) - \frac{1}{\epsilon} \|L_g V(\mathbf{x})\|^2 \leq L_f V(\mathbf{x}) + W(\mathbf{x}) < 0$ for all $\mathbf{x} \in \bar{\mathcal{V}}$, for any $\epsilon > 0$. Hence by taking $\epsilon < \bar{\epsilon}$, we ensure that $z_\epsilon(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \bar{\mathcal{V}}$ independently of the sign of $e(\mathbf{x})$. Note also that $\mathcal{W}$ as required in the statement exists because Γ_ν does not contain any point where V and h are incompatible and therefore by Lemma 3.3.3, all points in Γ_ν satisfying $C(\mathbf{x}) = 0$ necessarily also satisfy $B(\mathbf{x}) < 0$ (without loss of generality, using a similar argument as above). Therefore, by continuity of $B(\mathbf{x})$ for any $\epsilon > 0$ we can take a neighborhood $\mathcal{W}$ around P_ν so that $B(\mathbf{x}) + \frac{1}{\epsilon} C(\mathbf{x}) \leq B(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \mathcal{W}$ (since by Cauchy-Schwartz's inequality, $C(\mathbf{x}) \leq 0$). Hence, by taking $\epsilon < \bar{\epsilon}$, independently of whether $e(\mathbf{x}) \leq 0$ or $e(\mathbf{x}) > 0$ we ensure that $z_\epsilon(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \mathcal{W} \cup \bar{\mathcal{V}}$. Now we argue that if $\epsilon < \bar{\epsilon}$, $z_\epsilon(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \Gamma_\nu \backslash (\mathcal{W} \cup \mathcal{V} \cup \bar{\mathcal{V}})$. Note that $\Gamma_\nu \backslash (\mathcal{W} \cup \mathcal{V} \cup \bar{\mathcal{V}})$ does not contain any points where $L_g V(\mathbf{x})$ and $L_g W(\mathbf{x})$

are linearly dependent, since that would imply $C(\mathbf{x}) = 0$ and hence $\mathbf{x} \in \mathcal{W}$. Thus, by Cauchy-Schwartz's inequality, $C(\mathbf{x}) < 0$ for all $\mathbf{x} \in \Gamma_\nu \backslash (\mathcal{W} \cup \mathcal{V} \cup \bar{\mathcal{V}})$. Hence, $M_4^{\nu,\mathcal{V},\mathcal{W}} > 0$. Note also that $M_3^{\nu,\mathcal{V},\bar{\mathcal{V}}} > 0$. Therefore, regardless of whether $e(\mathbf{x}) \leq 0$ or $e(\mathbf{x}) > 0$, by taking $\epsilon < \bar{\epsilon}$ we ensure that $z_\epsilon(\mathbf{x}) \leq 0$ for all $\mathbf{x} \in \Gamma_\nu \backslash (\mathcal{W} \cup \mathcal{V} \cup \bar{\mathcal{V}})$, as claimed. Moreover, since by construction u_ϵ^{safe} satisfies (2.7) and is Lipschitz, by [23, Theorem 2], trajectories stay inside $\mathcal{C}$ for all $t \geq 0$. □

Note that in the statement of Theorem 3.3.4, one can pick $\mathcal{V}$ arbitrarily small, which might require an arbitrarily small ϵ. The next result states that under some additional reasonable assumptions, this does not happen and hence there exists a finite ϵ for which trajectories converge to the origin.

Corollary 3.3.5. (Convergence to the origin): *Under the same assumptions and notation of Theorem 3.3.4, assume additionally that* $f, g \in \mathcal{C}^1(\mathbb{R}^n)$, $V \in \mathcal{C}^2(\mathbb{R}^n)$, $\mathbf{0}_n \in \mathit{Int}(\mathcal{C})$ *and* $\ker(g(\mathbf{0}_n)^\top) \subseteq \mathcal{V}_s(\frac{\partial f}{\partial x}(\mathbf{0}_n))$. *Then, for*

$$\epsilon < \hat{\epsilon} := \min\{\frac{\bar{\lambda}_{\min}(g(\mathbf{0}_n)g(\mathbf{0}_n)^\top \nabla^2 V(\mathbf{0}_n))}{|\lambda_{\max}(\frac{\partial f}{\partial x}(\mathbf{0}_n))|}, \bar{\epsilon}\}$$

the origin is asymptotically stable and $\Gamma_\nu \cap C$ *is forward invariant and a subset of the region of attraction of the origin.*

Proof. Since $\mathbf{0}_n \in \text{Int}(\mathcal{C})$, $e(\mathbf{0}_n) < 0$ and the Jacobian of the closed-loop system evaluated at $\mathbf{0}_n$ is $J = \frac{\partial f}{\partial \mathbf{x}}(\mathbf{0}_n) - \frac{1}{\epsilon} g(\mathbf{0}_n)g(\mathbf{0}_n)^\top \nabla^2 V(\mathbf{0}_n)$. We show that, with $\epsilon < \hat{\epsilon}$, one has $\mathbf{v}^\top J \mathbf{v} < 0$ for $\mathbf{v} \in \mathbb{R}^n \backslash \{\mathbf{0}_n\}$. First, consider $\mathbf{v} \in \ker(g(\mathbf{0}_n)^T)$. By assumption, $\mathbf{v} \in \mathcal{V}_s(\frac{\partial f}{\partial \mathbf{x}}(\mathbf{0}_n))$, and hence $\mathbf{v}^\top J \mathbf{v} = \mathbf{v}^\top \frac{\partial f}{\partial \mathbf{x}}(\mathbf{0}_n)\mathbf{v} < 0$. Now, assume $\mathbf{v} \notin \ker(g(\mathbf{0}_n)^T)$. Since $\nabla^2 V(\mathbf{0}_n)$ is positive definite and $g(\mathbf{0}_n)g(\mathbf{0}_n)^\top$ is positive semidefinite,

$$\ker(g(\mathbf{0}_n)g(\mathbf{0}_n)^T \nabla^2 V(\mathbf{0}_n)) = \ker(g(\mathbf{0}_n)g(\mathbf{0}_n)^T),$$

and $g(\mathbf{0}_n)g(\mathbf{0}_n)^T \nabla^2 V(\mathbf{0}_n)$ has non-negative eigenvalues [115, 7.2.P21]. Hence,

$$\mathbf{v}^T J \mathbf{v} \leq (\lambda_{\max}(\frac{\partial f}{\partial \mathbf{x}}(\mathbf{0}_n)) - \frac{1}{\epsilon}\bar{\lambda}_{\min}(g(\mathbf{0}_n)g(\mathbf{0}_n)^T \nabla^2 V(\mathbf{0}_n)))\|\mathbf{v}\|^2.$$

This implies that $J + J^T$ is negative definite, and since the real parts of its eigenvalues are twice those of J, we obtain that J is Hurwitz. Therefore, we can take $\mathcal{V}$ in

Theorem 3.3.4 such that the closed-loop trajectories with $\epsilon < \frac{\bar{\lambda}_{\min}(g(\mathbf{0}_n)g(\mathbf{0}_n)^T\nabla^2 V(\mathbf{0}_n))}{|\lambda_{\max}(\frac{\partial f}{\partial x}(\mathbf{0}_n))|}$ starting at $\mathcal{V}$ converge to $\mathbf{0}_n$. Finally, reasoning as in Theorem 3.3.4, V is decreasing on $\Gamma_\nu \backslash \mathcal{V}$, and the result follows. □

Under the assumptions of Corollary 3.3.5, by ensuring that the origin is asymptotically stable in Γ_ν, we rule out the existence of equilibrium points in Γ_ν other than the origin. If the conditions of Corollary 3.3.5 are not satisfied or $\epsilon \geq \hat{\epsilon}$, other undesired behaviors such as limit cycles or convergence to undesired equilibria like the ones found in Proposition 3.3.1 can not be ruled out. Theorem 3.3.4 and Corollary 3.3.5 solve Problem 1. Under the stated assumptions, by taking u_ϵ^{safe} with $\epsilon < \hat{\epsilon}$ as a safe stabilizing controller, an inner approximation of the region of attraction of the origin is the largest level set of V that does not contain any incompatible points inside it.

In particular, if there exists a sublevel set of V that contains $\mathcal{C}$, u_ϵ^{safe} with $\epsilon < \hat{\epsilon}$ safely stabilizes the origin and the whole safe set $\mathcal{C}$ is in its region of attraction.

3.4 Simulations

In this section, we compare the stability QP with safety penalty controller with the CLF-CBF QP (3.2) and its modification, M-CLF-CBF QP, introduced in [35, Theorem 3] to avoid undesired equilibria. We focus on the following simple planar system

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} u. \tag{3.7}$$

For this system, $V(x_1, x_2) = \frac{1}{2}x_1^2 + \frac{1}{2}x_2^2$ is a CLF. The safe set $\mathcal{C}$ is the complement of the ball $\{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x} - (0, 4)\| \leq 2\}$, and we use the CBF $h(x_1, x_2) = x_1^2 + (x_2 - 4)^2 - 4$, with $\alpha(s) = s$. According to [35], the CLF-CBF QP (3.2) creates undesired equilibria in $\text{Int}(\mathcal{C})$ for all values of p. Instead, both M-CLF-CBF QP and the stability QP with safety penalty controller u_ϵ^{safe}, with $\epsilon \neq 1$, do not introduce undesired equilibria in $\text{Int}(\mathcal{C})$. The latter can be checked from the definition of

$\mathcal{Q}_1^\epsilon$ given in Proposition 3.3.1. In this example, the incompatible points are given by $\{(x_1, x_2) \in \mathbb{R}^2 : x_1 = 0, x_2 > 4\}$. Therefore, the approximation of the region of attraction given by Theorem 3.3.4 is $\Gamma_2 = \{x \in \mathbb{R}^2 : \|\mathbf{x}\|^2 < 4\}$. Figure 3.1 shows that the stability QP with safety penalty controller and M-CLF-CBF QP behave similarly, whereas CLF-CBF QP (3.2) fails to stabilize the origin. The plot also illustrates that trajectories starting at $(0, 9)$ converge to the boundary equilibrium point at $(0, 6)$ for all three approaches (this corresponds to a point where f, gL_gV, and gL_gh are collinear, cf. Remark 3.3.2).

This is not surprising since, for scenarios where the unsafe set is bounded, global convergence with a smooth vector field is impossible due to topological obstructions [116, 117].

An advantage of the approach proposed here is the explicit inner approximation of the region of attraction which, as Figure 3.1 shows, is conservative.

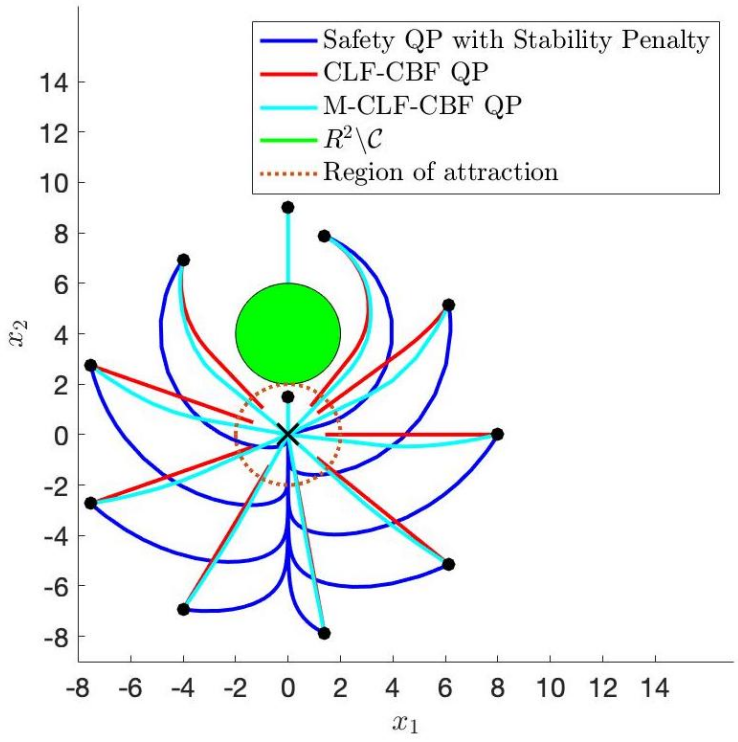


Figure 3.1: Safe stabilization of a planar system. The green ball is the set of unsafe states and the small dots display ten initial conditions for the system trajectories under the CLF-CBF QP, the M-CLF-CBF QP, and the safety QP with stability penalty controllers. The orange dotted curve marks the boundary of the estimate Γ_2 of the region of attraction. The CLF-CBF QP controller (with $p = 1$) preserves safety but does not reach the origin because of undesired equilibrium points. The safety QP with stability penalty (with $\epsilon = 0.01$) and the M-CLF-CBF QP (with $p = 1$) preserve safety and have trajectories converge to the origin, except for the one starting at $(0, 9)$.

Chapter 4

Control Barrier Function-Based Safety Filters: Characterization of Undesired Equilibria, Unbounded Trajectories, and Limit Cycles

This chapter focuses on *safety filters* designed based on CBFs. As briefly introduced in Chapter 3, these are modifications of a nominal stabilizing controller typically used in safety-critical control applications to render a given subset of states forward invariant. In this chapter we investigate the dynamical properties of the closed-loop system obtained from using safety filters.

These undesirable behaviors include unbounded trajectories, limit cycles, and undesired equilibria, which can be locally stable and even form a continuum. Our analysis offers the following contributions: (i) conditions under which trajectories remain bounded and (ii) conditions under which limit cycles do not exist; (iii) we show that undesired equilibria can be characterized by solving an algebraic equation, and (iv) we provide examples that show that asymptotically stable undesired equilibria can exist for a large class of nominal controllers and design parameters of the safety filter (even for convex safe sets).

Further, for the specific class of planar systems, (v) we provide explicit formulas

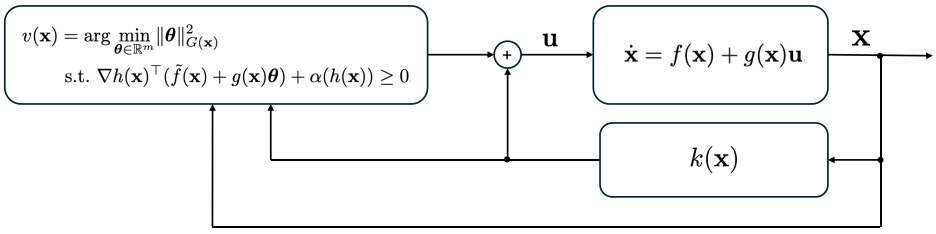


Figure 4.1: Closed-loop system that is the subject of this paper. A nominal controller k is used as input to the safety filter, that finds the controller closest to k that satisfies the CBF condition.

for the total number of undesired equilibria and the proportion of saddle points and asymptotically stable equilibria, and (vi) in the case of linear planar systems, we present an exhaustive analysis of their global stability properties. Examples throughout the paper illustrate the results.

4.1 Problem Statement

Consider a control-affine system of the form (3.1). Suppose that a locally Lipschitz nominal controller $k : \mathbb{R}^n \to \mathbb{R}^m$ is designed so that the system $\dot{\mathbf{x}} = \tilde{f}(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})$ has a unique globally asymptotically stable equilibrium, which we assume without loss of generality that is the origin. Let $\mathcal{C}$ be a set defined as in (2.6), and let h be a strict CBF of $\mathcal{C}$. We consider the function $v : \mathbb{R}^n \to \mathbb{R}^m$ defined as

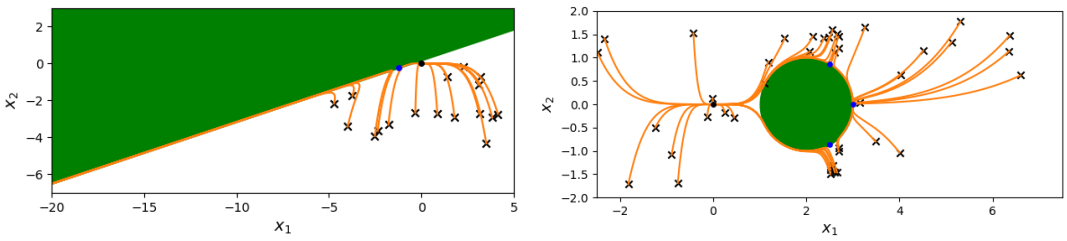
$$\begin{aligned} v(\mathbf{x}) = \arg\min_{\boldsymbol{\theta}\in\mathbb{R}^m} & \|\boldsymbol{\theta}\|^2_{G(\mathbf{x})} \\ \text{s.t. } & \nabla h(\mathbf{x})^\top(\tilde{f}(\mathbf{x}) + g(\mathbf{x})\boldsymbol{\theta}) + \alpha(h(\mathbf{x})) \geq 0, \end{aligned} \tag{4.1}$$

where $G : \mathbb{R}^n \to \mathbb{R}^{m\times m}$ is continuously differentiable and positive definite for all $\mathbf{x} \in \mathbb{R}^n$. We refer to v as a *safety filter*, and we consider the dynamical system

$$\dot{\mathbf{x}} = \tilde{f}(\mathbf{x}) + g(\mathbf{x})v(\mathbf{x}). \tag{4.2}$$

Figure 4.1 illustrates the setup of system (4.2). We make the following assumption:

Assumption 1 (Origin in the interior of $\mathcal{C}$)**.** *The origin is in the interior of the safe set, i.e., $h(\mathbf{0}_n) > 0$.*



(a) Unbounded trajectories (b) Stable undesired equilibrium

Figure 4.2: Control-affine systems with a safety filter with (a) half-plane and (b) circular obstacles. The plots show the trajectories from random initial conditions, the undesired equilibria (colored in blue), and the desired equilibrium (the origin, colored in black).

Even though the origin is globally asymptotically stable under the nominal controller k, and v is designed to minimally modify k while ensuring that $\mathcal{C}$ is forward invariant, studying the dynamical behavior of (4.2) is challenging. As noted in, e.g., [37], the filtered system does not necessarily inherit the global asymptotic stability properties of the controller k, and can even have undesired equilibria [34, 118, 4, 119, 6] (cf. Figure 4.2). Most of these works focus on studying conditions under which such undesired equilibria exist or can be confined to specific regions of interest, but do not study other dynamical properties of the closed-loop system, such as boundedness of trajectories, existence of limit cycles, or regions of attraction. In practical applications, these properties (e.g., ensuring that trajectories are bounded, unexpected limit cycles do not arise, or the region of attraction of undesired equilibria is small) is critical to guarantee a desirable performance of the closed-loop system. With this premise, the problem we address in this chapter is as follows:

Problem 2. *Given the system* (3.1) *and the safety filter* $v(\mathbf{x})$*, characterize the boundedness of trajectories, the region of attraction of the origin, existence of undesired equilibria and their regions of attraction, and the existence of limit cycles for the dynamics* (4.2)*.*

4.2 Undesired Equilibria, Bounded Trajectories, and Limit Cycles

In this section, we study the dynamical properties of (4.2), including undesired equilibria, (un)boundedness of trajectories, and limit cycles. We start by providing a precise expression for the unique optimal solution $v(\mathbf{x})$ of the problem (4.1). For brevity, define $\eta(\mathbf{x}) \coloneqq \nabla h(\mathbf{x})^\top \tilde{f}(\mathbf{x}) + \alpha(h(\mathbf{x}))$. Then, for any $\mathbf{x} \in \mathcal{C}$

$$v(\mathbf{x}) = \begin{cases} \mathbf{0}_m, & \text{if } \eta(\mathbf{x}) \geq 0, \\ \bar{u}(\mathbf{x}), & \text{if } \eta(\mathbf{x}) < 0, \end{cases} \tag{4.3}$$

where $\bar{u}(\mathbf{x}) \coloneqq -\frac{\eta(\mathbf{x}) G(\mathbf{x})^{-1} g(\mathbf{x})^\top \nabla h(\mathbf{x})}{\|g(\mathbf{x})^\top \nabla h(\mathbf{x})\|^2_{G^{-1}(\mathbf{x})}}$. We note that since h is a strict CBF, $g(\mathbf{x})^\top \nabla h(\mathbf{x}) \neq \mathbf{0}_m$ if $\eta(\mathbf{x}) < 0$ and $\mathbf{x} \in \mathcal{C}$. This implies that $\bar{u}$ (and hence v) is well defined on $\mathcal{C}$.

4.2.1 Characterization of undesired equilibria

Our first result leverages expression (4.3) to provide a necessary and sufficient condition for the existence of undesired equilibria of the filtered system (4.2).

Lemma 4.2.1. (Conditions for undesired equilibria): *Consider system* (4.2). *Let* h *be a strict CBF and suppose Assumption 1 holds. Let* $\mathbf{x}_* \in \mathbb{R}^n$ *be such that* $\tilde{f}(\mathbf{x}_*) \neq \mathbf{0}_n$. *Then,* $\mathbf{x}_*$ *is an equilibrium of* (4.2) *if and only if there exists* $\delta < 0$ *such that*

$$h(\mathbf{x}_*) = 0 \text{ and} \tag{4.4a}$$

$$\tilde{f}(\mathbf{x}_*) = \delta g(\mathbf{x}_*) G(\mathbf{x}_*)^{-1} g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*)\,. \tag{4.4b}$$

Moreover, $\mathbf{x}_*$ *is an equilibrium of* (4.2) *independently of the choice of* h *and* α.

Proof. Note that if x_* and $\delta < 0$ satisfy (4.4), then by multiplying (4.4b) by $\nabla h(\mathbf{x}_*)^\top$ we get $\|g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*)\|^2_{G^{-1}(\mathbf{x}_*)} \delta = \nabla h(\mathbf{x}_*)^\top \tilde{f}(\mathbf{x}_*)$. Now, if $g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*) = 0$, it would follow that $\nabla h(\mathbf{x}_*)^\top \tilde{f}(\mathbf{x}_*) = 0$. Since $h(\mathbf{x}_*) = 0$, this would imply that $\nabla h(\mathbf{x}_*)^\top (\tilde{f}(\mathbf{x}_*) + g(\mathbf{x}_*)\mathbf{u}) + \alpha(h(\mathbf{x}_*)) = \nabla h(\mathbf{x}_*)^\top (f(\mathbf{x}_*) + g(\mathbf{x}_*)\mathbf{u}) + \alpha(h(\mathbf{x}_*)) = 0$, for all $\mathbf{u} \in \mathbb{R}^m$, which contradicts the assumption that h is a strict CBF. Therefore,

$g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*) \neq 0$ and $\delta = \frac{\nabla h(\mathbf{x}_*)^\top \tilde{f}(\mathbf{x}_*)}{\|g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*)\|^2_{G^{-1}(\mathbf{x}_*)}}$. Then, it follows that $\eta(\mathbf{x}_*) < 0$ and $\tilde{f}(\mathbf{x}_*) + g(\mathbf{x}_*)\bar{u}(\mathbf{x}_*) = \mathbf{0}_n$. Therefore, $\mathbf{x}_*$ is an equilibrium of (4.2).

Conversely, if $\mathbf{x}_*$ is an equilibrium of (4.2), then $\tilde{f}(\mathbf{x}_*)+g(\mathbf{x}_*)\bar{u}(\mathbf{x}_*) = \mathbf{0}_n$. It follows that $0 = \nabla h(\mathbf{x}_*)^\top(\tilde{f}(\mathbf{x}_*)+g(\mathbf{x}_*)\bar{u}(\mathbf{x}_*)) = -\alpha(h(\mathbf{x}_*))$. Since $\alpha(\cdot)$ is an extended class $\mathcal{K}_\infty$ function, it must hold that $h(\mathbf{x}_*) = 0$. Note also that $\eta(\mathbf{x}_*) < 0$, since otherwise $\bar{u}(\mathbf{x}_*) = \mathbf{0}_m$ and hence $\tilde{f}(\mathbf{x}_*)+g(\mathbf{x}_*)\bar{u}(\mathbf{x}_*) = \tilde{f}(\mathbf{x}_*) = f(\mathbf{x}_*)+g(\mathbf{x}_*)k(\mathbf{x}_*) = \mathbf{0}_n$, which can only hold if $\mathbf{x}_* = \mathbf{0}_n$, contradicting Assumption 1. Hence, $\eta(\mathbf{x}_*) < 0$ and one has that $f(\mathbf{x}_*) = \frac{\eta(\mathbf{x}_*)}{\|g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*)\|^2_{G^{-1}(\mathbf{x}_*)}} g(\mathbf{x}_*)G(\mathbf{x}_*)^{-1}g(\mathbf{x}_*)^\top \nabla h(\mathbf{x}_*)$, implying (4.4b) with $\delta < 0$. Finally, the fact that $\mathbf{x}_*$ is an equilibrium of (4.2) independently of h and α follows from [120, Corollary 4.5]. □

Hereafter, given a solution $(\mathbf{x}_*, \delta_{\mathbf{x}_*})$ to (4.4), we refer to $\delta_{\mathbf{x}_*}$ as the *indicator* of $\mathbf{x}_*$. Lemma 4.2.1 characterizes the undesired equilibria of closed-loop systems obtained from safety filters. We note that related results exist in the literature: [118, Theorem 2] characterizes the undesired equilibria for a CBF-based control design that includes CLF constraints and [4, Proposition 5.1] characterizes undesired equilibria for a design that includes such CLF constraints as a penalty term in the objective function.

However, both of these designs can introduce undesired equilibria in the interior of the safe set, whereas as shown in Lemma 4.2.1, (4.2) can only introduce undesired equilibria in the boundary of the safe set.

Based on Lemma 4.2.1, we define the sets

$$\mathcal{E} \coloneqq \{\mathbf{x} \in \mathbb{R}^n : \ \exists\ \delta \in \mathbb{R} \text{ s.t. } (\mathbf{x}, \delta) \text{ solves (4.4)}\},$$
$$\hat{\mathcal{E}} \coloneqq \{\mathbf{x} \in \mathbb{R}^n : \ \exists\ \delta < 0 \text{ s.t. } (\mathbf{x}, \delta) \text{ solves (4.4)}\}.$$

We refer to $\mathcal{E}$ and $\hat{\mathcal{E}}$ as the sets of *potential undesired equilibria* and of *undesired equilibria* of (4.2), respectively. Note that $\hat{\mathcal{E}} \subset \mathcal{E}$. By Lemma 4.2.1, determining the equilibrium points of system (4.2) is equivalent to solving (4.4) and checking the sign of δ.

Under appropriate conditions, [120, Proposition 10] provides an explicit expression for the Jacobian of $\tilde{f}(\mathbf{x}) + g(\mathbf{x})v(\mathbf{x})$ at $\mathbf{x} \in \hat{\mathcal{E}}$ and shows that one of its

eigenvalues is $-\alpha'(0)$ (provided that α is differentiable), and the rest of the eigenvalues are independent of α.

If $\alpha'(0) > 0$, it follows that the Jacobian evaluated at $\mathbf{x} \in \hat{\mathcal{E}}$ always has a negative eigenvalue.

Even if we are able to identify the set of undesired equilibria, characterizing the dynamical properties of the closed-loop system (4.2) is still challenging. In the following, we provide a variety of results regarding the boundedness of trajectories, the existence of limit cycles, and the stability properties of undesired equilibria. We also investigate the possible asymptotic behaviors of trajectories of the closed-loop system (4.2).

4.2.2 Boundedness of trajectories

The following result states a set of general conditions under which the trajectories of (4.2) are bounded.

Proposition 4.2.2. (Conditions for boundedness of trajectories): *Consider system* (4.2) *and suppose that h is a strict CBF and Assumption 1 holds. Let $\partial\mathcal{C}$ be bounded. Moreover, assume that the extended class $\mathcal{K}_\infty$ function $\alpha(\cdot)$ is linear, i.e., $\alpha(z) = az$ for some $a > 0$. Then, for any compact set $\Phi \subset \mathbb{R}^n$ with $\partial\Phi \subset \mathcal{C}$, there exists $\tilde{a}_\Phi > 0$ and a compact set $\tilde{\Phi}$ containing Φ such that, by taking $a > \tilde{a}_\Phi$, $\tilde{\Phi}$ is forward invariant under* (4.2). *As a consequence, any trajectory of* (4.2) *with initial condition in $\Phi \cap \mathcal{C}$ is bounded (because it remains in $\tilde{\Phi}$ at all times).*

Proof. Since $\partial\mathcal{C}$ is bounded, either $\mathcal{C}$ is bounded or $\mathbb{R}^n \backslash \mathcal{C}$ is bounded.

Case 1: $\mathcal{C}$ bounded. In this case, $\mathcal{C}$ is actually compact, and the result holds because $\mathcal{C}$ is forward invariant under (4.2): for any compact Φ with $\partial\Phi \subset \mathcal{C}$, necessarily $\Phi \subset \mathcal{C}$ and we can take $\tilde{\Phi} = \mathcal{C}$ and any extended class $\mathcal{K}_\infty$ function.

Case 2: $\mathbb{R}^n \backslash \mathcal{C}$ is bounded. Since the system $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})$ renders the origin globally asymptotically stable, by [121, Theorem 4.17], there exists a radially unbounded Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$. Let Γ be a Lyapunov sublevel set of V containing $(\mathbb{R}^n \backslash \mathcal{C}) \cup \Phi$ and such that $h(\mathbf{x}) > 0$ for all $\mathbf{x} \in \partial\Gamma$. Note that such Γ exists because $\mathbb{R}^n \backslash \mathcal{C}$ is bounded and V is radially unbounded. Now, since $h(\mathbf{x}) > 0$

for all $\mathbf{x} \in \partial\Gamma$, there exists $\tilde{a}_\Phi$ sufficiently large such that $\eta(\mathbf{x}) = \nabla h(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})) + \tilde{a}_\Phi h(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \partial\Gamma$. Let $\tilde{\Phi} = \Gamma$. Since Γ is a Lyapunov sublevel set, this implies that Γ is forward invariant for $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})$. By taking $\alpha(z) = az$ with $a > \tilde{a}_\Phi$, and since $\nabla h(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})) + \alpha(h(\mathbf{x})) \geq 0$ for all $\mathbf{x} \in \partial\Gamma$, the safety filter is inactive in $\partial\Gamma$ and therefore Γ is also forward invariant under (4.2). □

Next we show that if the assumptions of Proposition 4.2.2 do not hold, the trajectories of (4.2) might not be bounded (as illustrated in Figure 4.2(a)). The following result provides technical conditions under which for linear systems and affine CBFs, (4.2) has unbounded trajectories.

Proposition 4.2.3. (Unbounded trajectories): *Let $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $\mathbf{a} \in \mathbb{R}^n$, $b \in \mathbb{R}$ and consider the LTI system $\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u}$, the function $h : \mathbb{R}^n \to \mathbb{R}$ given by $h(\mathbf{x}) = \mathbf{a}^\top \mathbf{x} - b$ and the set $\mathcal{C} := \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}$. Let h be a strict CBF and suppose Assumption 1 holds. Further assume that there exists $\mathbf{c} \in \mathbb{R}^n$, $\zeta_1 > 0$, and $\zeta_2 \geq 0$ satisfying $\mathbf{c} \neq \mathbf{0}_n$, $\mathbf{c}^\top B = \mathbf{0}_m^\top$, and $\mathbf{c}^\top A = \zeta_1 \mathbf{c}^\top + \zeta_2 \mathbf{a}^\top$. Then, for any locally Lipschitz controller $\hat{\mathbf{u}} : \mathbb{R}^n \to \mathbb{R}^m$, and any initial condition $\mathbf{x}_0$ in $\{\mathbf{x} \in \mathbb{R}^n : \mathbf{a}^\top \mathbf{x} \geq b,\ \zeta_1 \mathbf{c}^\top \mathbf{x} + \zeta_2 b > 0\}$, the solution of $\dot{\mathbf{x}} = A\mathbf{x} + B\hat{\mathbf{u}}(\mathbf{x})$ with initial condition at $\mathbf{x}_0$ satisfies $\lim_{t\to+\infty} \|\mathbf{x}(t;\mathbf{x}_0)\| = +\infty$.*

Proof. We note that

$$\frac{d}{dt}(\mathbf{c}^\top \mathbf{x}) = \mathbf{c}^\top (A\mathbf{x} + B\hat{\mathbf{u}}(\mathbf{x})) = (\zeta_1 \mathbf{c} + \zeta_2 \mathbf{a})^\top \mathbf{x} \geq \zeta_1 \mathbf{c}^\top \mathbf{x} + \zeta_2 b\,.$$

This implies that the set $\{\mathbf{x} \in \mathbb{R}^n : \zeta_1 \mathbf{c}^\top \mathbf{x} + \zeta_2 b \geq 0\}$ is forward invariant. Additionally, if $\zeta_1 \mathbf{c}^\top \mathbf{x}_0 + \zeta_2 b > 0$, then $\zeta_1 \mathbf{c}^\top \mathbf{x}(t;\mathbf{x}_0) + \zeta_2 b \geq \zeta_1 \mathbf{c}^\top \mathbf{x}_0 + \zeta_2 b$ and therefore $\mathbf{c}^\top \mathbf{x}(t;\mathbf{x}_0) \geq \mathbf{c}^\top \mathbf{x}_0$ for all $t \geq 0$.

It follows that

$$\mathbf{c}^\top \mathbf{x}(t;\mathbf{x}_0) = \mathbf{c}^\top \mathbf{x}_0 + \int_0^{+\infty} \frac{d}{dt} \mathbf{c}^\top \mathbf{x}(t;\mathbf{x}_0)\, dt \geq \mathbf{c}^\top \mathbf{x}_0 + \int_0^{+\infty} (\zeta_1 \mathbf{c}^\top \mathbf{x}_0 + \zeta_2 b) dt = +\infty,$$

which implies that $\lim_{t\to+\infty} \|\mathbf{x}(t;\mathbf{x}_0)\| = +\infty$. □

Remark 4.2.4. (Underactuated systems always have unbounded solutions for some safe set): In the setting of Proposition 4.2.3, if $m < n$, $\ker(B) \neq 0$ and therefore there exists $\mathbf{c} \neq \mathbf{0}_n$ such that $\mathbf{c}^\top B = \mathbf{0}_m^\top$. Then, for any $\zeta_1 > 0$ and $\zeta_2 > 0$, by letting $\mathbf{a} = \frac{1}{\zeta_2}(A^\top \mathbf{c} - \zeta_1 \mathbf{c})$ we satisfy the hypothesis of Proposition 4.2.3. Hence, for any underactuated linear system, there exists a safe set for which any controller induces unbounded solutions. On the other hand, for fully actuated systems, there does not exist $\mathbf{c} \in \mathbb{R}^n$ satisfying $\mathbf{c}^\top B \neq \mathbf{0}_m^\top$ and therefore the conditions of Proposition 4.2.3 are never met. □

Proposition 4.2.3 and Remark 4.2.4 show that in general, one cannot guarantee that the trajectories of (4.2) are bounded.

4.2.3 Limit cycles

Here we turn our attention to limit cycles. The following result ensures that, by taking a linear extended class $\mathcal{K}_\infty$ function $\alpha(x) = ax$, $a > 0$, with sufficiently large slope, closed-loop planar systems (4.2) do not have limit cycles.

Proposition 4.2.5. (No limit cycles in planar systems): *Consider system* (4.2) *with* $n = 2$. *Let* h *be a strict CBF with a linear extended class* $\mathcal{K}_\infty$ *function* $\alpha(\cdot)$, *i.e.,* $\alpha(z) = az$ *for some* $a > 0$. *Suppose Assumption 1 holds and that* $\mathbb{R}^2 \backslash \mathcal{C}$ *is comprised of a finite number of connected components. Then, there exists* $\hat{a} > 0$ *sufficiently large such that, by taking* $a > \hat{a}$, *the closed-loop system does not contain any limit cycles in* $\mathcal{C}$. *Moreover, all bounded trajectories with initial condition in* $\mathcal{C}$ *converge to an equilibrium point.*

Proof. We start by noting that, if there exists a limit cycle with at least one point in $\mathcal{C}$, then it is contained in $\mathcal{C}$ (because the set is forward invariant under (4.2)). Let γ be a limit cycle contained in $\mathcal{C}$. Note that γ corresponds to a maximal trajectory of (4.2) and cannot contain an equilibrium point. We distinguish four different cases:

(1) If γ does not encircle the origin and does not encircle any connected component of $\mathbb{R}^n \backslash \mathcal{C}$, we reach a contradiction because limit cycles must encircle

an equilibrium point [122, Corollary 6.26], and all equilibrium points other than the origin of (4.2) are in $\partial\mathcal{C}$ by Lemma 4.2.1.

(2) Suppose that γ encircles the origin, but does not encircle any connected component of $\mathbb{R}^2\backslash\mathcal{C}$. Note that since the origin is globally asymptotically stable for the nominal system, and the origin is contained in $\text{Int}(\mathcal{C})$, there exists $\mathbf{q}_1 \in \partial\mathcal{C}$ such that the solution $\mathbf{y}(t;\mathbf{q}_1)$ of the nominal system satisfies $\mathbf{y}(t;\mathbf{q}_1) \in \text{Int}(\mathcal{C})$ for all $t > 0$. Since $\mathbf{q}_1 \in \partial\mathcal{C}$, $\nabla h(\mathbf{x})^\top (f(\mathbf{x})+g(\mathbf{x})k(\mathbf{x}))|_{\mathbf{x}=\mathbf{q}_1} > 0$ and since ∇h, f, g and k are continuous there exists a neighborhood $\mathcal{N}_{\mathbf{q}_1}$ of $\mathbf{q}_1$ such that $\nabla h(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x}))|_{\mathbf{x}=\mathbf{z}} > 0$ for all $\mathbf{z} \in \mathcal{N}_{\mathbf{q}_1}$. Now, note that there exists $d_1 > 0$ such that $h(\mathbf{y}(t;\mathbf{q}_1)) > d_1$ for all $t > 0$ such that $\mathbf{y}(t;\mathbf{q}_1) \notin \mathcal{N}_{\mathbf{q}_1}$. This means that there exists $a_1 > 0$ such that $\nabla h(\mathbf{y}(t;\mathbf{q}_1))^\top (f(\mathbf{y}(t;\mathbf{q}_1)) + g(\mathbf{y}(t;\mathbf{q}_1))k(\mathbf{y}(t;\mathbf{q}_1))) + a_1 h(\mathbf{y}(t;\mathbf{q}_1)) > 0$ for all $t \geq 0$. Therefore, $\mathbf{y}(t;\mathbf{q}_1)$ is also a trajectory of (4.2) by taking α to be an extended class $\mathcal{K}_\infty$ function with slope greater than a_1, which means that it intersects with γ, violating the existence and uniqueness of solutions of (4.2). Hence, by taking $a > a_1$, we ensure such γ cannot exist.

(3) Suppose that γ encircles one or more connected components in $\mathbb{R}^2\backslash\mathcal{C}$, but not the origin, cf. Figure 4.3. Let S (resp., $\bar{S}$) be the union of the connected components encircled (resp., not encircled) by γ. Since the origin is globally asymptotically stable for the nominal system, there exists $\mathbf{q}_2$ in the boundary of S so that the solution $\mathbf{y}(t;\mathbf{q}_2)$ of the nominal system satisfies one of the following:

   (a) there exists $t_1 < 0$ with $\tilde{\mathbf{q}}_2 = \mathbf{y}(t_1;\mathbf{q}_2) \in \partial\bar{S}$ and $\mathbf{y}(t;\mathbf{q}_2) \in \text{Int}(\mathcal{C})$ for all $t \in (t_1, 0)$. In this case, there exists t_1' such that $\mathbf{y}(t_1';\mathbf{q}_2) \in \gamma$, and there exists $a_{S,2} > 0$ such that $\{\mathbf{y}(t;\mathbf{q}_2)\}_{t\in[t_1,t_1']}$ is a trajectory of (4.2) by taking a linear extended class $\mathcal{K}_\infty$ function with slope greater than $a_{S,2}$. This violates the existence and uniqueness of solutions of (4.2), because $\{\mathbf{y}(t;\mathbf{q}_2)\}_{t\in[t_1,t_1']}$ is a solution and intersects γ.

   (b) $\mathbf{y}(t;\mathbf{q}_2) \in \mathcal{C}$ for all $t < 0$. By Lemma 4.4.1, $\lim_{t\to-\infty} \|\mathbf{y}(t;\mathbf{q}_2)\| = \infty$. This means that there exists $\bar{t}_1 < 0$ such that $\mathbf{y}(\bar{t}_1;\mathbf{q}_2) \in \gamma$; This means that

there exists $\tilde{a}_{S,2} > 0$ such that $\{\mathbf{y}(t;\mathbf{q}_2)\}_{t\in[\bar{t}_1,\frac{\bar{t}_1}{2}]}$ is a trajectory of (4.2) by taking a linear extended class $\mathcal{K}_\infty$ function with slope greater than $\tilde{a}_{S,2}$. However, this solution intersects with γ, violating the existence and uniqueness of solutions of (4.2).

Hence by taking a linear extended class $\mathcal{K}_\infty$ function with slope greater than $a_{S,2}$ and $\tilde{a}_{S,2}$, we ensure such γ cannot exist.

(4) Suppose that γ encircles one or more connected components in $\mathbb{R}^2\backslash\mathcal{C}$ and the origin. Let S' (resp., $\bar{S}'$) be the subset of the connected components of $\mathbb{R}^2\backslash\mathcal{C}$ encircled (resp., not encircled) by γ. Again, since the origin is globally asymptotically stable for the nominal system, there exists $\mathbf{q}_3$ in the boundary of S' so that the solution $\mathbf{y}(t;\mathbf{q}_3)$ of the nominal system satisfies one of the following:

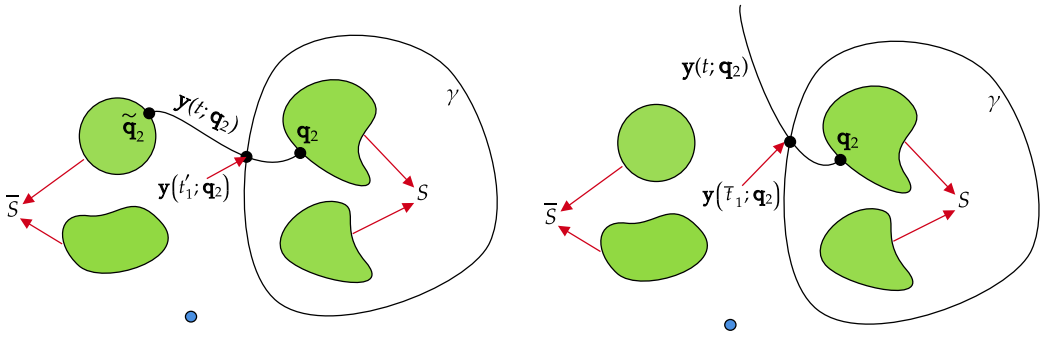
(a) there exists $t_2 < 0$ with $\mathbf{y}(t_2;\mathbf{q}_3) \in \partial\bar{S}'$ and $\mathbf{y}(t;\mathbf{q}_3) \in \mathrm{Int}(\mathcal{C})$ for all $t \in (t_2, 0)$;

(b) $\mathbf{y}(t;\mathbf{q}_3) \in \mathcal{C}$ for all $t < 0$.

By following an argument analogous to case (iii), there exists $\breve{a}_{S'} > 0$ sufficiently large such by taking a linear extended class $\mathcal{K}_\infty$ function with slope greater than $\breve{a}_{S'}$, we ensure such γ cannot exist.

Note that the values of $a_{S,2}$ and $\tilde{a}_{S,2}$ defined in 3 depend on the set of connected components of $\mathbb{R}^2\backslash\mathcal{C}$ encircled by the limit cycle. Since there is a finite number of bounded connected components, there exists a^* such that $a^* > a_{S,2}$ and $a^* > \tilde{a}_{S,2}$ for all possible sets of connected components S of $\mathbb{R}^2\backslash\mathcal{C}$. Similarly, the value $\breve{a}_{S'}$ defined in item 4 depends on S', but there exists $\breve{a}^*$ such that $\breve{a}^* > \breve{a}_{S'}$ for all possible S'. By taking $a > \hat{a} := \max\{a^*, \breve{a}^*\}$, it follows that the closed-loop system does not contain any limit cycles in $\mathcal{C}$. Finally, since no limit cycles exist in $\mathcal{C}$ for $a > \hat{a}$, by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1] all bounded trajectories with initial condition in $\mathcal{C}$ converge to an equilibrium point. □

The following example shows that limit cycles can exist for systems of the form (4.2) in dimension $n \geq 3$.



(a) Subcase (a) of item 3 (b) Subcase (b) of item 3

Figure 4.3: Sketch of the setting considered in item 3 of the proof of Proposition 4.2.5. The connected components comprising $\mathbb{R}^2\backslash\mathcal{C}$ are depicted in green, whereas the origin is represented by the blue dot.

Example 4.2.6. (Existence of limit cycles in higher dimensions): Consider the safe set $\mathcal{C} := \{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}-[x_c,0,0]^\top\|^2-r^2 \geq 0\}$. Let $B \in \mathbb{R}^{3\times 3}$ invertible, $G(\mathbf{x}) = B^\top B$, $K = \mathbb{0}_3$ and nominal controller $k(\mathbf{x}) = K\mathbf{x} \equiv \mathbf{0}_3$. Next, let $0 < p_1 < \frac{r}{r+x_c}p_2$, $p_2 > 0$, $p_3 > 0$, and define

$$A := \begin{bmatrix} -p_1 & 0 & 0 \\ 0 & -p_2 & p_3 \\ 0 & -p_3 & -p_2 \end{bmatrix}.$$

Consider the closed-loop system (4.2) obtained with $f(\mathbf{x}) = A\mathbf{x}$, $g(\mathbf{x}) = B$, $h(\mathbf{x}) = \|\mathbf{x} - [x_c,0,0]^\top\|^2 - r^2$ and $k(\mathbf{x}) \equiv 0$.

Define also $\hat{p} := \frac{x_c p_1}{p_2-p_1}$ and $\hat{q} := \sqrt{r^2-\hat{p}^2}$, then $0 < \hat{p} < r$ and $p_1 = \frac{\hat{p}}{\hat{p}+x_c}p_2$. Consider

$$\mathbf{x}_0 := \begin{bmatrix} \hat{p} \\ \hat{q} \\ \hat{q} \end{bmatrix}, \quad \hat{\mathbf{x}}(t;\mathbf{x}_0) := \begin{bmatrix} \hat{x}_1(t) \\ \hat{x}_2(t) \\ \hat{x}_3(t) \end{bmatrix} = \begin{bmatrix} x_c + \hat{p} \\ \hat{q}\sin(p_3 t) \\ \hat{q}\cos(p_3 t) \end{bmatrix}.$$

Note that for any t,

$$\nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))^\top (A+BK)\hat{\mathbf{x}}(t;\mathbf{x}_0) = -2\begin{bmatrix} \hat{p} \\ \hat{q}\sin(p_3 t) \\ \hat{q}\cos(p_3 t) \end{bmatrix}^\top \begin{bmatrix} \frac{\hat{p}}{\hat{p}+x_c}p_2 & 0 & 0 \\ 0 & p_2 & -p_3 \\ 0 & p_3 & p_2 \end{bmatrix} \hat{\mathbf{x}}(t;\mathbf{x}_0) = -2r^2 p_2 < 0.$$

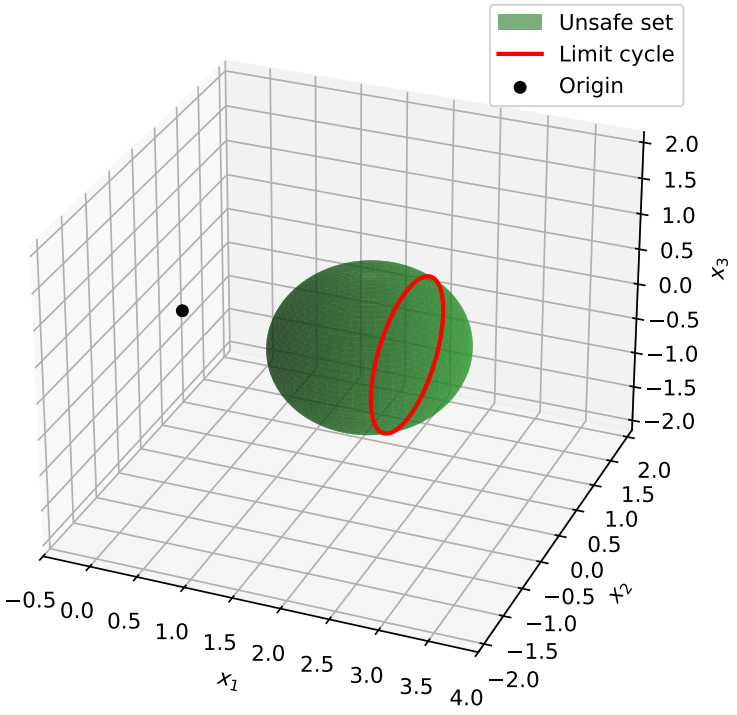


Figure 4.4: Depiction of the setting considered in Example 4.2.6, with parameters $x_c = 2$, $r = 1$, $p_1 = 1$, $p_2 = 6$, $p_3 = 1$. The obstacle is depicted in green, the limit cycle $\hat{\mathbf{x}}$ in red, and the origin in black.

Moreover, let

$$\kappa(t) = \frac{\nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))^\top (A+BK)\hat{\mathbf{x}}(t;\mathbf{x}_0) + \alpha(h(\hat{\mathbf{x}}(t;\mathbf{x}_0)))}{\nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))^\top BG^{-1}B^\top \nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))}$$

and note that since $K = \mathbb{0}_3$,

$$\begin{aligned}
&(A+BK)\hat{\mathbf{x}}(t;\mathbf{x}_0) - \kappa(t)BG^{-1}B^\top \nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0)) \\
=&A\hat{\mathbf{x}}(t;\mathbf{x}_0) - \frac{\nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))^\top A\hat{\mathbf{x}}(t;\mathbf{x}_0)}{\nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))^\top \nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0))} \nabla h(\hat{\mathbf{x}}(t;\mathbf{x}_0)) \\
=&\begin{bmatrix} -\hat{p}p_2 \\ -p_2\hat{q}\sin(p_3 t) + p_3\hat{q}\cos(p_3 t) \\ -p_2\hat{q}\sin(p_3 t) - p_3\hat{q}\cos(p_3 t) \end{bmatrix} + p_2 \begin{bmatrix} \hat{p}_1 \\ \hat{q}\sin(p_3 t) \\ \hat{q}\cos(p_3 t) \end{bmatrix} \\
=&\begin{bmatrix} 0 \\ p_3\hat{q}\cos(p_3 t) \\ -p_3\hat{q}\sin(p_3 t) \end{bmatrix} = \frac{d}{dt}\begin{bmatrix} x_c + \hat{p} \\ \hat{q}\sin(p_3 t) \\ \hat{q}\cos(p_3 t) \end{bmatrix} = \frac{d}{dt}\begin{bmatrix} \hat{x}_1(t) \\ \hat{x}_2(t) \\ \hat{x}_3(t) \end{bmatrix}
\end{aligned}$$

Hence $\hat{\mathbf{x}}(t;\mathbf{x}_0)$ is a valid trajectory of the closed-loop system (4.2) and it is a limit cycle. Note also that since $\hat{\mathbf{x}}(t) \in \partial\mathcal{C}$ for all $t \geq 0$, by [120, Corollary 4.5] this trajectory exists for any choice of h and α. Figure 4.4 depicts the limit cycle $\hat{\mathbf{x}}$. △

4.2.4 Structure of the set of undesired equilibria

In this section, we investigate the set of undesired equilibria of (4.2). The following example shows that in general, this set can be a continuum.

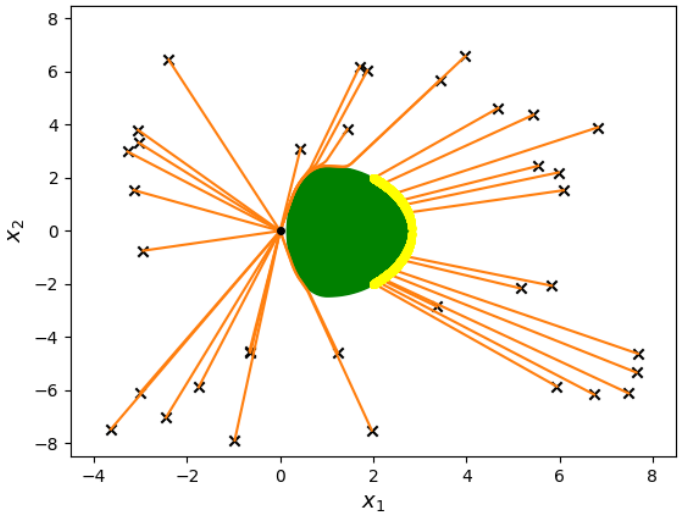


Figure 4.5: Plot of different trajectories of (4.2). Trajectories are depicted in orange. The unsafe set is colored in green. Black crosses denote initial conditions, the black dot denotes the origin, and the yellow region denotes a continuum of undesired equilibria.

Example 4.2.7. (Continuum of undesired equilibria): Let $n = 2$, $m = 1$ and consider (4.2) with

$$f(\mathbf{x}) = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}\mathbf{x}, \quad g(\mathbf{x}) = B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad h(\mathbf{x}) = \begin{cases} (x_1+1)^2 + x_2, & x_1 \geq -1, \\ x_2, & -2 < x_1 < -1, \\ (x_1+2)^2 + x_2, & x_1 \leq -2, \end{cases}$$

and $\alpha(s) = 10s$. Note that h is continuously differentiable. Moreover,

$$\nabla h(\mathbf{x})^\top B = \begin{cases} 2\begin{bmatrix} x_1 + 1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq 0, & x_1 \geq -1, \\ 2\begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq 0, & -2 < x_1 < -1, \\ 2\begin{bmatrix} x_1 + 2 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq 0, & x_1 \leq -2, \end{cases}$$

Therefore, h is a strict CBF. Next, we show that the set $\{t(1,0) : -2 \leq t \leq -1\}$ is contained in the set of undesired equilibria for any linear stabilizing controller $k(\mathbf{x}) = k_1 x_1 + k_2 x_2$, $G : \mathbb{R}^2 \to \mathbb{R}$ and extended class $\mathcal{K}_\infty$ function α. Since k is a stabilizing controller, it follows that $f(\mathbf{x}) + Bk(\mathbf{x})$ is Hurwitz and therefore $-2 + k_2 < 0$, $1 + k_1 > 0$. For any $\sigma \in [-2, -1]$, the point $\mathbf{x}_\sigma = (\sigma, 0) \in \mathbb{R}^2$ satisfies (4.4) with associated indicator equal to $\frac{G(\mathbf{x}_\sigma)}{(1+k_1)\sigma} < 0$. Hence, the set $\{\sigma(1,0) : -2 \leq \sigma \leq -1\}$ is contained in the set of undesired equilibria for any linear stabilizing controller $k(\mathbf{x}) = k_1 x_1 + k_2 x_2$, $G : \mathbb{R}^2 \to \mathbb{R}$ and extended class $\mathcal{K}_\infty$ function α. Figure 4.5 shows some of the trajectories for the corresponding closed-loop system (4.2). Since the undesired equilibria are not isolated, the study of their stability properties requires using the notion of *semistability* [124]. △

The following result provides conditions under which a continuum of undesired equilibria of (4.2) does not exist.

Lemma 4.2.8. (Sufficient conditions for isolated equilibria): *An undesired equilibrium $\mathbf{x}_*$ is isolated if the Jacobian of (4.2) evaluated at $\mathbf{x}_*$ does not have imaginary eigenvalues. If $\partial\mathcal{C}$ is bounded, then each undesired equilibria of (4.2) is isolated if and only if $|\hat{\mathcal{E}}| < \infty$.*

Proof. Given an undesired equilibrium $\mathbf{x}_*$, if the Jacobian of (4.2) evaluated at $\mathbf{x}_*$ does not have imaginary eigenvalue, then there exists a neighborhood of $\mathbf{x}_*$ such that the linearization of (4.2) around $\mathbf{x}_*$ does not contain any equilibrium point other than itself. By the Hartman-Grobman Theorem [101, Section 2.8], there

also exists a neighborhood of $\mathbf{x}_*$ for which (4.2) does not contain any undesired equilibrium and hence $\mathbf{x}_*$ is isolated.

Consider the case when $\partial\mathcal{C}$ is bounded. Clearly, if $|\hat{\mathcal{E}}| < \infty$ (i.e., the number of undesired equilibria is finite), then each of the undesired equilibria is isolated. Conversely, if the number of undesired equilibria is infinite, consider an infinite sequence of undesired equilibria $\{\mathbf{x}_{*,i}\}_{i=1}^{+\infty}$. Since $\partial\mathcal{C}$ is compact, there exists a convergent subsequence $\{\mathbf{x}_{*,i_k}\}_{k=1}^{+\infty}$ such that $\lim_{k\to\infty} \mathbf{x}_{*,i_k} = \mathbf{q}_*$. Since (4.2) is continuous under the assumption that h is a strict CBF (cf. [103, Lemma III.2]), $0 = \lim_{k\to\infty} f(\mathbf{x}_{*,i_k}) + g(\mathbf{x}_{*,i_k})v(\mathbf{x}_{*,i_k}) = f(\mathbf{x}_*) + g(\mathbf{q}_*)v(\mathbf{x}_*)$ and hence $\mathbf{x}_*$ is an equilibrium, which is non-isolated. □

While Lemma 4.2.8 provides sufficient conditions for the existence of isolated undesired equilibria, finding their number is, in general, challenging. However, this is possible for the special case of planar systems, as we show next.

Proposition 4.2.9. (Number and stability properties of undesired equilibria for a planar system with bounded obstacle): *Let h be a strict CBF and suppose Assumption 1 holds. Let $\mathbb{R}^2\backslash\mathcal{C}$ be a bounded connected set. Consider* (4.2) *with $n = 2$ and assume its undesired equilibria $\hat{\mathcal{E}} = \{\mathbf{x}_*^{(i)}\}_{i=1}^{k} \subset \partial\mathcal{C}$ are either asymptotically stable or saddle points. Then, k is odd, and $\frac{k+1}{2}$ equilibria are saddle points and $\frac{k-1}{2}$ are asymptotically stable.*

Proof. Let $\mathcal{L} \subset [k]$ be the index set of undesired equilibria that are saddle points. We show that $|\mathcal{L}| = \frac{k+1}{2}$. Figure 4.6 serves as visual aid for the different elements employed in the proof. Let Φ be a compact set containing the origin and $\mathbb{R}^2\backslash\mathcal{C}$ in its interior. This implies that $\partial\Phi \subset \mathcal{C}$. By Propositions 4.2.2 and 4.2.5, there exists $a_\Phi > 0$ and a compact set $\tilde{\Phi}$ containing Φ such that (4.2), with extended class $\mathcal{K}_\infty$ function with slope greater than a_Φ, makes $\tilde{\Phi}$ forward invariant and $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycles. Since [120, Proposition 11] ensures that the stability properties of undesired equilibria are independent of α, we can assume without loss of generality that α takes this form. Now, for $j \in \mathcal{L}$, let γ_j be a subset of the one-dimensional local stable manifold of (4.2) at $\mathbf{x}_*^{(j)}$ such that:

(1) γ_j corresponds to a maximal trajectory of (4.2);

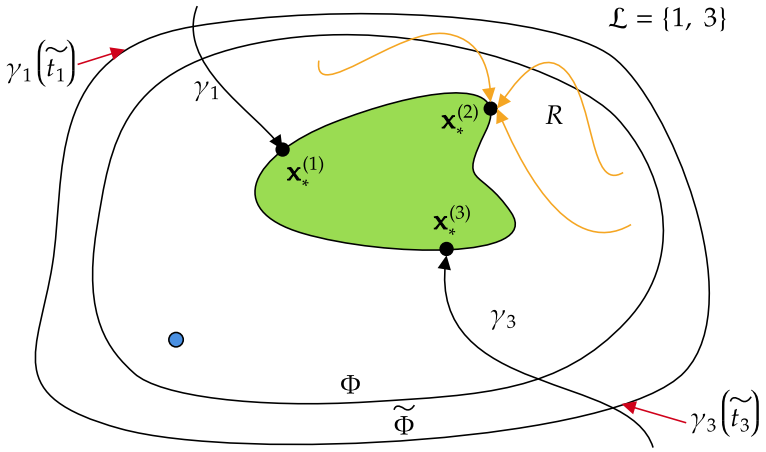


Figure 4.6: Sketch of the setting considered in the proof of Proposition 4.2.9. The unsafe set is depicted in green, whereas the origin is represented by the blue dot.

(2) there exists $T > 0$ with $\gamma_j(t) \in \mathrm{Int}(\mathcal{C})$ for all $t > T$.

Note that such γ_j always exists because the stable manifold is a union of trajectories and the stable manifold of (4.2) at $\mathbf{x}_*^{(j)}$ is tangent to $\nabla h(\mathbf{x}_*^{(j)})$. The fact that the stable manifold of (4.2) at $\mathbf{x}_*^{(j)}$ is tangent to $\nabla h(\mathbf{x}_*^{(j)})$ follows from the fact that $\nabla h(\mathbf{x}_*^{(j)})$ is an eigenvector of the Jacobian of (4.2) evaluated at $\mathbf{x}_*^{(j)}$ with negative eigenvalue (cf. [120, Proposition 6.2]), and the Stable Manifold Theorem [101, Section 2]. By Lemma 4.4.3, since $\tilde{\Phi}$ is forward invariant and $\tilde{\Phi} \cap \mathcal{C}$ does not contain limit cycles, there exists at least one $j \in \mathcal{L}$ and $\tilde{t}_j \in \mathbb{R}$ such that $\gamma_j(\tilde{t}_j) \in \partial\tilde{\Phi}$ and $\gamma_j(t) \notin \tilde{\Phi}$ for all $t < t_j$.

Moreover by Lemma 4.4.2(i), γ_j cannot be tangent to $\mathcal{C}$ for any $j \in \mathcal{L}$. Therefore $\{\gamma_j\}_{j\in\mathcal{L}}$ divide $\tilde{\Phi} \cap \mathcal{C}$ into $|\mathcal{L}|$ regions (note that this would not be the case if there was not at least one $j \in \mathcal{L}$ and $\tilde{t}_j \in \mathbb{R}$ such that $\gamma_j(\tilde{t}_j) \in \partial\tilde{\Phi}$ and $\gamma_j(t) \notin \tilde{\Phi}$ for all $t < t_j$), each of which is an open connected set. Let R be any one of such regions. We now show that $\mathrm{Cl}(R)$ contains exactly one asymptotically stable equilibrium point.

Indeed, first suppose that there is no asymptotically stable equilibrium point in $\mathrm{Cl}(R)$. Let $\breve{\gamma}$ be any trajectory with initial condition in $\mathrm{Cl}(R)$. By the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], since $\tilde{\Phi}$ is forward invariant, $\breve{\gamma}$ converges to either a limit cycle or an equilibrium point. It cannot converge to a

limit cycle because $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycles. Moreover, if $\bar{\mathbf{x}}_*$ and $\tilde{\mathbf{x}}_*$ are the equilibrium points in $\{\mathbf{x}_*^{(j)}\}_{j=1}^k$ whose stable manifolds define the boundary of R, $\breve{\gamma}$ cannot converge to an equilibrium other than $\bar{\mathbf{x}}_*$ or $\tilde{\mathbf{x}}_*$, since otherwise $\breve{\gamma}$ would intersect the stable manifolds of $\bar{\mathbf{x}}_*$ or $\tilde{\mathbf{x}}_*$, which would contradict the uniqueness of solutions of (4.2). But it can also not converge to $\bar{\mathbf{x}}_*$ or $\tilde{\mathbf{x}}_*$: if, for example, $\breve{\gamma}$ converged to $\bar{\mathbf{x}}_*$, there would be two different trajectories converging to $\bar{\mathbf{x}}_*$ with different tangent vectors at $\bar{\mathbf{x}}_*$, which would contradict the fact that $\bar{\mathbf{x}}_*$ is a saddle point. Therefore, $\mathrm{Cl}(R)$ contains at least one asymptotically stable equilibrium.

Next suppose that there are multiple asymptotically stable undesired equilibria in $\mathrm{Cl}(R)$. By [121, Theorem 8.1], the boundary of the regions of attraction of asymptotically stable equilibria is formed by trajectories. Let $\tilde{\gamma}$ be one such trajectory with initial condition in R. Note that since R is contained in $\tilde{\Phi}$ and $\tilde{\Phi}$ is forward invariant, $\tilde{\gamma}$ is bounded. By the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], this trajectory must converge to an equilibrium point or a limit cycle. It can not converge to a limit cycle because $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycles. It can not converge to an equilibrium point because it is not in any region of attraction of an asymptotically stable equilibrium, there are no saddle points in R, and it can not converge to $\bar{\mathbf{x}}_*$ (resp. $\tilde{\mathbf{x}}_*$), because otherwise $\bar{\mathbf{x}}_*$ (resp. $\tilde{\mathbf{x}}_*$) would have two trajectories converging to it with different tangent vectors, which would contradict the fact that $\bar{\mathbf{x}}_*$ (resp. $\tilde{\mathbf{x}}_*$) is a saddle point.

Therefore, we conclude that in each of the $|\mathcal{L}|$ regions formed by $\{\gamma_j\}_{j\in\mathcal{L}}$, there is exactly one asymptotically stable equilibrium in their boundary. Since there are $k - |\mathcal{L}|$ other undesired equilibria, and since the origin is asymptotically stable, this means that $|\mathcal{L}| = k - |\mathcal{L}| + 1$. Hence, $|\mathcal{L}| = \frac{k+1}{2}$. Note also that by [120, Proposition 10], the stability properties of undesired equilibria are independent of the choice of extended class $\mathcal{K}_\infty$ function α. Hence, even though in our arguments we have chosen a specific extended class $\mathcal{K}_\infty$ function α, the statement holds for any such α.

□

Under the assumptions of Proposition 4.2.9, since $\mathbb{R}^2 \backslash \mathcal{C}$ is bounded, [17, Proposition 3] implies that there does not exist a safe globally asymptotically stabilizing

controller. If no limit cycles exist (for example, under the conditions of Proposition 4.2.5), by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], this implies that there must exist at least one undesired equilibrium, and hence $k \geq 1$. Note also that as shown in [120, Proposition 6.2], under a large class of CBFs, the stability properties of the undesired equilibria remain the same.

Next we give a result similar to Proposition 4.2.9 for the case when the safe set $\mathcal{C}$ is compact and connected.

Proposition 4.2.10. (Number of undesired equilibria for compact connected safe set): *Let h be a strict CBF and suppose Assumption 1 holds. Let $\mathcal{C}$ be a compact connected set. Consider* (4.2) *with $n = 2$ and assume its undesired equilibria $\hat{\mathcal{E}} = \{\mathbf{x}_*^{(i)}\}_{i=1}^k \subset \partial\mathcal{C}$ are either asymptotically stable or saddle points. Then, k is even, and $\frac{k}{2}$ equilibria are saddle points and $\frac{k}{2}$ equilibria are asymptotically stable.*

Proof. The proof follows a similar argument to that of Proposition 4.2.9. Let $\mathcal{L} \subset [k]$ be the set of indices of undesired saddle points. We show that $|\mathcal{L}| = \frac{k}{2}$. For $j \in \mathcal{L}$, let γ_j be a subset of the one-dimensional local stable manifold of (4.2) at $\mathbf{x}_*^{(j)}$ such that

(1) γ_j corresponds to a maximal trajectory of (4.2);

(2) there exists $T > 0$ with $\gamma_j(t) \in \mathrm{Int}(\mathcal{C})$ for all $t > T$.

Note that for each $j \in \mathcal{L}$, either there exists $\tilde{t}_j \in \mathbb{R}$ such that $\gamma_j(\tilde{t}_j) \in \partial\mathcal{C}$ and $\gamma_j(t) \notin \mathcal{C}$ for $t < \tilde{t}_j$ or $\lim_{t\to-\infty} \gamma_j(t) = \mathbf{x}'_*$, with $\mathbf{x}'_*$ an undesired equilibrium that is a saddle point. Indeed, otherwise, since $\mathcal{C}$ is bounded, by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1] $\lim_{t\to-\infty} \gamma_j(t)$ would converge to a limit cycle or another equilibrium point. However, by Proposition 4.2.5, there exists $\hat{a} > 0$ such that (4.2) with linear extended class $\mathcal{K}_\infty$ function with slope greater than $\hat{a}$ does not have any limit cycles in $\mathcal{C}$. Since [120, Proposition 11] ensures that the stability properties of undesired equilibria are independent of α, we can assume without loss of generality that $\lim_{t\to-\infty} \gamma_j(t)$ does not converge to a limit cycle. Moreover, $\lim_{t\to-\infty} \gamma_j(t)$ cannot converge to an asymptotically stable equilibrium, since it belongs to the one-dimensional local stable manifold of $\mathbf{x}_*^{(j)}$.

Now we note that, since for all $j \in \mathcal{L}$, either there exists $\tilde{t}_j$ such that $\gamma_j(\tilde{t}_j) \in \partial\mathcal{C}$ and $\gamma_j(t) \notin \mathcal{C}$ for $t < \tilde{t}_j$ or $\lim_{t\to-\infty} \gamma_j(t) = \mathbf{x}'_*$, with $\mathbf{x}'_*$ an undesired equilibrium that is a saddle point, the trajectories $\{\gamma_j\}_{j\in\mathcal{L}}$ divide $\mathcal{C}$ into $|\mathcal{L}| + 1$ connected sets in $\mathcal{C}$. By an argument analogous to the one in the proof of Proposition 4.2.9, in each of those sets there must exist exactly one asymptotically stable equilibrium. Since the origin is asymptotically stable under (4.2), this implies that the number of undesired equilibria that are saddle points is equal to the number of undesired equilibria that are asymptotically stable, proving $|\mathcal{L}| = \frac{k}{2}$. □

Note that by [120, Proposition 11], the Jacobian of (4.2) evaluated at an undesired equilibrium has at least one negative eigenvalue. Therefore, the assumption in Propositions 4.2.9 and 4.2.10 that all undesired equilibria are either asymptotically stable or saddle points is satisfied if at any undesired equilibrium the other eigenvalue of the Jacobian is nonzero. If the other eigenvalue is zero and the equilibrium is degenerate, the point is asymptotically stable if the trajectories in its central manifold converge to it and it is a saddle point if the trajectories in its central manifold diverge from it.

We also note that Propositions 4.2.9 and 4.2.10 provide information about the number and the stability properties of undesired equilibria even in the case where the algebraic equations (4.4) defining the undesired equilibria are difficult to solve. We also point out that both results require $\partial\mathcal{C}$ to be bounded and hence, by Lemma 4.2.8, the assumption that the number of equilibria is finite is equivalent to each of them being isolated.

We finalize this section by introducing a class of safe sets that do not introduce undesired equilibria.

Proposition 4.2.11. (Class of safe sets with global asymptotic stability of origin): *Let $V : \mathbb{R}^n :\to \mathbb{R}$ be a global Lyapunov function for the nominal system $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})$. Let $c > 0$ and suppose $h(\mathbf{x}) := c - V(\mathbf{x})$ is a strict CBF of $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}$. Then, the origin is asymptotically stable with region of attraction containing $\mathcal{C}$. In particular, (4.2) does not contain any undesired equilibria.*

Proof. Let us first show that the safety filter is inactive at all points in $\mathcal{C}$. Indeed, for all $\mathbf{x} \in \mathcal{C}$, $\eta(\mathbf{x}) = \nabla h(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})) + \alpha(h(\mathbf{x})) = -\nabla V(\mathbf{x})^\top (f(\mathbf{x}) +$

$g(\mathbf{x})k(\mathbf{x})) + \alpha(h(\mathbf{x})) \geq 0$. Therefore, $v(\mathbf{x}) = \mathbf{0}_m$ for all $\mathbf{x} \in \mathcal{C}$. This implies that for all $\mathbf{x} \in \mathcal{C}$, $\nabla V(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x}) + g(\mathbf{x})v(\mathbf{x})) < 0$ for all $\mathbf{x} \in \mathcal{C}\backslash\{\mathbf{0}_n\}$, and therefore all trajectories with initial condition in $\mathcal{C}\backslash\{\mathbf{0}_n\}$ converge to the origin, i.e., the origin is asymptotically stable with region of attraction containing $\mathcal{C}$. In particular, this implies that no undesired equilibria exist (i.e., $\hat{\mathcal{E}} = \varnothing$), since otherwise trajectories with initial condition in such undesired equilibria do not converge to the origin. □

4.3 Dynamical Properties of Safety Filters for Linear Planar Systems

In this section, we focus on linear planar systems. Due to their simpler structure, solving (4.4) leads to additional results and insights, compared to the general treatment presented in the previous section. Consider the LTI planar system

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u}, \tag{4.5}$$

where $\mathbf{x} = [x_1, x_2]^\top \in \mathbb{R}^2$, $\mathbf{u} \in \mathbb{R}^m$, with $m \in \{1, 2\}$, $A \in \mathbb{R}^{2\times 2}$, and $B \in \mathbb{R}^{2\times m}$ having full column rank. We make the following assumption.

Assumption 2 (Stabilizability)**.** *The system* (4.5) *is stabilizable. Moreover,* $\mathbf{u} = -K\mathbf{x}$*,* $K \in \mathbb{R}^{2\times m}$*, is a stabilizing controller such that* $\tilde{A} = A - BK$ *is Hurwitz.* □

In this setup, the system (4.2) is then customized as follows.

$$\dot{\mathbf{x}} = F(\mathbf{x}) \coloneqq (A - BK)\mathbf{x} + Bv(\mathbf{x}), \tag{4.6}$$

where the safety filter is given by

$$v(\mathbf{x}) = \begin{cases} 0, & \text{if } \eta(\mathbf{x}) \geq 0, \\ -\frac{\eta(\mathbf{x})G(\mathbf{x})^{-1}B^\top \nabla h(\mathbf{x})}{\|B^\top \nabla h(\mathbf{x})\|^2_{G^{-1}(\mathbf{x})}}, & \text{if } \eta(\mathbf{x}) < 0, \end{cases} \tag{4.7}$$

with $\eta(\mathbf{x}) \coloneqq \nabla h(\mathbf{x})^\top (A - BK)\mathbf{x} + \alpha(h(\mathbf{x}))$.

As shown in [120, Proposition 6.2], the stability properties of the undesired equilibria in the different results of this section hold for a large class of choices of the CBF h and the function α.

4.3.1 Bounded safe set

Here we discuss various results and examples for the case where the safe set is compact and contains the origin. We start by showing that for linear, planar underactuated systems and safe sets that are parametrizable in polar coordinates by a continuously differentiable function, the system (4.6) does not have undesired equilibria.

Proposition 4.3.1. (No undesired equilibria for underactuated planar systems and safe sets parametrizable in polar coordinates): *Consider* (4.5) *with* $m = 1$ *(i.e., the system is underactuated), and suppose that Assumptions 1 and 2 hold. Let* $r : \mathbb{R} \to \mathbb{R}_{>0}$ *be a continuously differentiable,* 2π*-periodic function, and such that*

$$\partial\mathcal{C} = \{(r(\theta)\cos(\theta), r(\theta)\sin(\theta)) : \theta \in [0, 2\pi]\}, \tag{4.8}$$

and let h *be a strict CBF of* $\mathcal{C}$*. Then,* (4.6) *does not have any undesired equilibria for any* $K \in \mathbb{R}^2$ *and* $\alpha \in \mathbb{R}_{>0}$*.*

Proof. For convenience, denote

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \; B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \; K = \begin{bmatrix} k_1 & k_2 \end{bmatrix},$$

in (4.5) and let $\beta = a_{11}b_2 - b_1a_{21}$, $\gamma = a_{22}b_1 - b_2a_{12}$. Further define $R : \mathbb{R}^2 \backslash \{\mathbf{0}_2\} \to \mathbb{R}$ as

$$R(\mathbf{y}) = \begin{cases} r(\frac{\pi}{2})^2 & \text{if } y_1 = 0, \; y_2 > 0, \\ r(\frac{3\pi}{2})^2 & \text{if } y_1 = 0, \; y_2 < 0, \\ r(\arctan(\frac{y_2}{y_1}))^2 & \text{otherwise,} \end{cases}$$

We recall the following three facts:

(1) By [120, Corollary 4.5], undesired equilibria are independent of the choice of CBF;

(2) By Lemma 4.4.4, since h is a strict CBF of $\mathcal{C}$, any CBF of $\mathcal{C}$ is a strict CBF of $\mathcal{C}$;

(3) By [23, Theorem 3], since $\mathcal{C}$ is safe, any continuously differentiable function whose 0-superlevel is $\mathcal{C}$ is a CBF of $\mathcal{C}$.

These facts imply that, without loss of generality, we can assume that h is such that in a neighborhood $\mathcal{N}_c$ of $\partial\mathcal{C}$, $h(\mathbf{y}) = -\|\mathbf{y}\|^2 + R(\mathbf{y})$ for all $\mathbf{y} \in \mathcal{N}_c$, and that such h is a strict CBF. Note that for all $\mathbf{x} \in \partial\mathcal{C}$ with $x_1 \neq 0$, we have

$$\nabla h(\mathbf{x}) = \begin{pmatrix} -2x_1 + 2r(\arctan(\frac{x_2}{x_1}))r'(\arctan(\frac{x_2}{x_1}))\frac{-x_2}{x_1^2+x_2^2} \\ -2x_2 + 2r(\arctan(\frac{x_2}{x_1}))r'(\arctan(\frac{x_2}{x_1}))\frac{x_1}{x_1^2+x_2^2} \end{pmatrix}. \tag{4.9}$$

Since ∇h is continuous, if $x_1 = 0$ and $x_2 > 0$, we have

$$\nabla h(0, x_2) = \begin{pmatrix} -2x_1 + 2r(\arctan(\frac{\pi}{2})))r'(\arctan(\frac{\pi}{2}))\frac{-1}{x_2} \\ -2x_2 \end{pmatrix}, \tag{4.10}$$

whereas if $x_1 = 0$ and $x_2 < 0$,

$$\nabla h(0, x_2) = \begin{pmatrix} -2x_1 + 2r(\arctan(\frac{3\pi}{2})))r'(\arctan(\frac{3\pi}{2}))\frac{-1}{x_2} \\ -2x_2 \end{pmatrix}. \tag{4.11}$$

Therefore, (4.9) is valid also for $x_1 = 0$ by defining $\arctan(\frac{x_2}{x_1}) = \frac{\pi}{2}$ if $x_1 = 0$ and $x_2 > 0$, and $\arctan(\frac{x_2}{x_1}) = \frac{3\pi}{2}$ if $x_1 = 0$ and $x_2 < 0$. From (4.4), the undesired equilibria lie in $\partial\mathcal{C}$, and therefore are of the form $(r(\theta^*)\cos(\theta^*), r(\theta^*)\sin(\theta^*))$. Furthermore, from (4.4) and (4.9), we have

$$\begin{pmatrix} a_{11} + b_1k_1 & a_{12} + b_1k_2 \\ a_{21} + b_2k_1 & a_{22} + b_2k_2 \end{pmatrix} \begin{pmatrix} r(\theta^*)\cos(\theta^*) \\ r(\theta^*)\sin(\theta^*) \end{pmatrix} = \delta \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^\top \nabla h \begin{pmatrix} r(\theta^*)\cos(\theta^*) \\ r(\theta^*)\sin(\theta^*) \end{pmatrix}.$$

It follows that θ^* satisfies

$$b_2 \begin{pmatrix} a_{11} + b_1k_1 & a_{12} + b_1k_2 \end{pmatrix} \begin{pmatrix} r(\theta^*)\cos(\theta^*) \\ r(\theta^*)\sin(\theta^*) \end{pmatrix} = b_1 \begin{pmatrix} a_{21} + b_2k_1 & a_{22} + b_2k_2 \end{pmatrix} \begin{pmatrix} r(\theta^*)\cos(\theta^*) \\ r(\theta^*)\sin(\theta^*) \end{pmatrix},$$

which implies that θ^* satisfies $\gamma\sin(\theta^*) = \beta\cos(\theta^*)$. Note that there exist exactly two values θ^* in $[0, 2\pi]$ solving $\gamma\sin(\theta^*) = \beta\cos(\theta^*)$. Hence, there exist exactly two potential undesired equilibria (i.e., $\mathcal{E}$ has cardinality 2). Let $\mathbf{x}_*^{(1)}$, $\mathbf{x}_*^{(2)}$ be such undesired equilibria, with θ_1^* and θ_2^* being their associated θ^* values. From

Lemma 4.2.1, $\mathbf{x}_*^{(1)}$ is an undesired equilibria if and only if $\eta(\mathbf{x}_*^{(1)}) < 0$, or equivalently,

$$\begin{aligned}\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})\Big((a_{11}-b_1k_1)\cos(\theta_1^*)+(a_{12}-b_1k_2)\sin(\theta_1^*)\Big)+\\ \frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)})\Big((a_{21}-b_2k_1)\cos(\theta_1^*)+(a_{22}-b_2k_2)\sin(\theta_1^*)\Big)<0.\end{aligned} \tag{4.12}$$

If $\gamma \neq 0$, $\sin(\theta_1^*) = \frac{\beta}{\gamma}\cos(\theta_1^*)$, and (4.12) is equivalent to

$$\begin{aligned}\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})\frac{\cos(\theta_1^*)}{\gamma}\Big(\gamma(a_{11}-b_1k_1)+\beta(a_{12}-b_1k_2)\Big)+\\ \frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)})\frac{\cos(\theta_1^*)}{\gamma}\Big(\gamma(a_{21}-b_2k_1)+\beta(a_{22}-b_2k_2)\Big)<0.\end{aligned}$$

On the other hand, if $\gamma = 0$, $\cos(\theta_1^*) = 0$, and (4.12) is equivalent to

$$\sin(\theta_1^*)\Big(\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})(a_{12}-b_1k_2)+\frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)})(a_{22}-b_2k_2)\Big)<0.$$

Note also that $\gamma = \beta = 0$ leads to no undesired equilibria. Indeed, using the definitions of β and γ,

$$\gamma(a_{11}-b_1k_1)+\beta(a_{12}-b_1k_2)=b_1(\det(A)-\gamma k_1-\beta k_2), \tag{4.13a}$$

$$\gamma(a_{21}-b_2k_1)+\beta(a_{22}-b_2k_2)=b_2(\det(A)-\gamma k_1-\beta k_2), \tag{4.13b}$$

which implies that $b_1\det(A) = b_2\det(A) = 0$ if $\gamma = \beta = 0$. If $\det(A) = 0$, then $\det(A+BK) = \det(A) - \gamma k_1 - \beta k_2 = 0$ for all K, which contradicts Assumption 2. Hence, $b_1 = b_2 = 0$, in which case (4.4) implies that $(A-BK)\mathbf{x}_*^{(1)} = (A-BK)\mathbf{x}_*^{(2)} = \mathbf{0}_2$, which can only hold if $\mathbf{x}_*^{(1)} = \mathbf{x}_*^{(2)} = \mathbf{0}_2$ and they are not undesired equilibrium. Hence the rest of the proof focuses on the case $\beta^2+\gamma^2 > 0$. By the Routh-Hurwitz criterion [125], since $A-BK$ is Hurwitz and is a 2×2 matrix, $\det(A-BK) = \det(A) - \gamma k_1 - \beta k_2 > 0$. Hence, if $\gamma \neq 0$, by using (4.13), (4.12) is equivalent to

$$\frac{\cos(\theta_1^*)}{\gamma}\Big(\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})b_1+\frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)})b_2\Big)<0.$$

On the other hand, if $\gamma = 0$, by using (4.13), (4.12) is equivalent to

$$\sin(\theta_1^*)\Big(\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})\frac{b_1}{\beta}+\frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)})\frac{b_2}{\beta}\Big)<0.$$

Using (4.9), we get that if $\gamma \neq 0$, (4.12) is equivalent to

$$\Big(\frac{\cos(\theta_1^*)}{\gamma}\Big)^2\Big(-r(\theta_1^*)(b_1\gamma + b_2\beta)+r'(\theta_1^*)(-b_1\beta + b_2\gamma)\Big)<0, \tag{4.14}$$

whereas if $\gamma = 0$, $\cos(\theta_1^*) = 0$, which means that $\sin^2(\theta_1^*) = 1$, and again using (4.9), (4.12) is equivalent to

$$\frac{1}{\beta}\Big(-r'(\theta_1^*)b_1 - r(\theta_1^*)b_2\sin^2(\theta_1^*)\Big) = \frac{1}{\beta}\Big(-r'(\theta_1^*)b_1 - r(\theta_1^*)b_2\Big)<0, \tag{4.15}$$

Note that similar expressions to (4.14) and (4.15) hold for θ_2^*. In particular, this means that if $\gamma \neq 0$, the sign of $-r(\theta_1^*)(b_1\gamma + b_2\beta) + r'(\theta_1^*)(-b_1\beta + b_2\gamma)$ and $-r(\theta_2^*)(b_1\gamma + b_2\beta) + r'(\theta_2^*)(-b_1\beta + b_2\gamma)$ is the same, and if $\gamma = 0$, the sign of $-r'(\theta_1^*)b_1 - r(\theta_1^*)b_2$ and $-r'(\theta_2^*)b_1 - r(\theta_2^*)b_2$ is the same.

Next, we compute the eigenvalues of the Jacobian of (4.2) at $\mathbf{x}_*^{(1)}$. By [120, Proposition 11], one of its eigenvalues is $-\alpha'(0)$. By using the expression of the Jacobian of (4.2) at $\mathbf{x}_*^{(1)}$ also provided in [120, Proposition 11], and using the fact that the trace is the sum of the eigenvalues, we obtain that the other eigenvalue is

$$\lambda_{\mathbf{x}_*^{(1)}} := \frac{\beta\frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(1)}) + \gamma\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)})}{b_1\frac{\partial h}{\partial x_1}(\mathbf{x}_*^{(1)}) + b_2\frac{\partial h}{\partial x_2}(\mathbf{x}_*^{(2)})}.$$

Using (4.9), we get that if $\gamma \neq 0$,

$$\lambda_{\mathbf{x}_*^{(1)}} = \frac{r(\theta_1^*)(\beta^2+\gamma^2)}{r(\theta_1^*)(b_1\gamma + b_2\beta) - r'(\theta_1^*)(-b_1\beta + b_2\gamma)}, \tag{4.16}$$

whereas if $\gamma = 0$,

$$\lambda_{\mathbf{x}_*^{(1)}} = \frac{\beta r(\theta_1^*)}{r'(\theta_1^*)b_1 + r(\theta_1^*)b_2}. \tag{4.17}$$

Now, since if $\gamma \neq 0$, the sign of $-r(\theta_1^*)(b_1\gamma+b_2\beta)+r'(\theta_1^*)(-b_1\beta+b_2\gamma)$ and $-r(\theta_2^*)(b_1\gamma+b_2\beta) + r'(\theta_2^*)(-b_1\beta + b_2\gamma)$ is the same, and if $\gamma = 0$ the sign of $r'(\theta_1^*)b_1 + r(\theta_1^*)b_2$ and $r'(\theta_2^*)b_1 + r(\theta_2^*)b_2$ is the same, $\mathbf{x}_*^{(1)}$ and $\mathbf{x}_*^{(2)}$ have the same stability properties. Note also that since r is strictly positive by definition, $r(\theta_1^*) > 0$, and since we are discussing the case $\beta^2 + \gamma^2 > 0$, $\mathbf{x}_*^{(1)}$ and $\mathbf{x}_*^{(2)}$ cannot be degenerate undesired equilibria. However, according to Proposition 4.2.10, since $\mathcal{C}$ is compact, connected, and contains the origin, if there exist two undesired equilibria, one must be a saddle

point and the other one must be asymptotically stable, which is a contradiction with the fact that $\mathbf{x}_*^{(1)}$ and $\mathbf{x}_*^{(2)}$ have the same stability properties. This implies that $\mathbf{x}_*^{(1)}$ and $\mathbf{x}_*^{(2)}$ cannot be undesired equilibria and therefore (4.6) does not have any, i.e., $\hat{\mathcal{E}} = \varnothing$. □

Figure 4.7 illustrates different examples of safe sets satisfying the assumptions in Proposition 4.3.1. The following example shows that the conclusions of Proposition 4.3.1 do not hold if (4.5) is fully actuated.

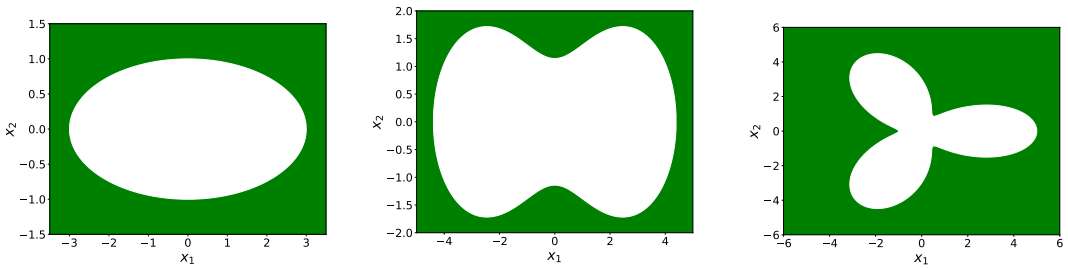


Figure 4.7: Examples of safe sets satisfying the assumptions of Proposition 4.3.1 The unsafe region is colored in green and the safe set in white. For the left figure, $r(\theta) = \frac{1}{\sqrt{3\cos^2(\theta)+\sin^2(\theta)}}$, for the center figure, $r(\theta) = 3\sqrt{\cos(2\theta) + \sqrt{(1.03)^4 - \sin^2(\theta)}}$, and for the right figure, $r(\theta) = 3+2\cos(3\theta)$.

Example 4.3.2. (Undesired equilibrium in convex and bounded safe set, fully actuated system): Consider the planar single integrator, i.e., (4.6) with $A = \mathbb{0}_2$, $B = \mathbf{I}_2$, and let $K = \begin{bmatrix} 5 & -8 \\ 2 & -3 \end{bmatrix}$, $G(\mathbf{x}) = \mathbf{I}_2$, $h(\mathbf{x}) = 10 - x_1^2 - (x_2 - 2)^2$, and $\alpha(s) = 50s$. Note that $-K$ is Hurwitz. By numerically solving the conditions in (4.4), it follows that $(3, 3)$ and $(3.161, 2.123)$ are undesired equilibria of (4.6). Moreover, using the expression of the Jacobian in [120, Proposition 11], we deduce that $(3, 3)$ is asymptotically stable and $(3.161, 2.123)$ is a saddle point. This is illustrated in Figure 4.8. △

We also note that a critical assumption in Proposition 4.3.1 is that the boundary of the safe set can be parametrized as in (4.8). In the following example, we show that if such a parametrization does not exist, the closed-loop system (4.6) can have undesired equilibria even if the system is underactuated and h is a strict CBF.

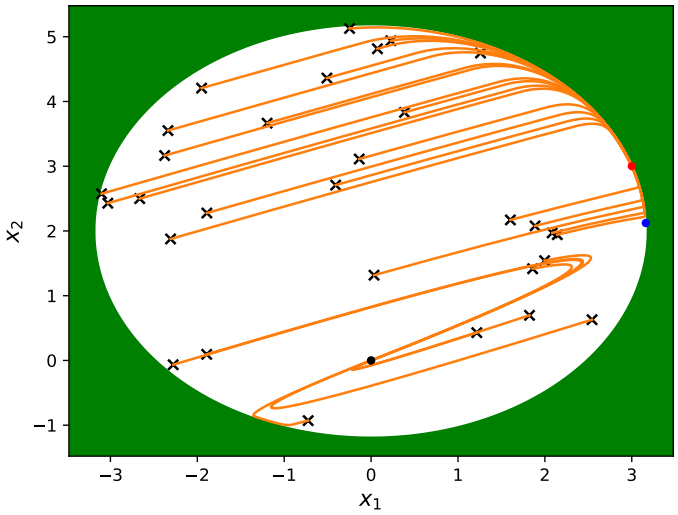


Figure 4.8: Plot of different trajectories (in orange) for Example 4.3.2. The unsafe set is colored in green. Black crosses denote initial conditions, the black dot denotes the origin, the red dot denotes an asymptotically stable undesired equilibrium, and the blue dot denotes an undesired equilibrium that is a saddle point.

Example 4.3.3. (Undesired equilibrium in sets not parametrizable in polar coordinates): Consider (4.6) with

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \; B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \; K = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}^\top,$$

$$h(\mathbf{x}) = b^4 - \left\| \mathbf{x} - \begin{bmatrix} a - c_1 \\ c_2 \end{bmatrix} \right\|^2 \left\| \mathbf{x} + \begin{bmatrix} a + c_1 \\ -c_2 \end{bmatrix} \right\|^2, \; \alpha(s) = 50s,$$

where $a_{11} = 1.878$, $a_{12} = -6.247$, $a_{21} = -3.189$, $a_{22} = 6.731$, $b_1 = 4.166$, $b_2 = -8.172$, $k_1 = 1.495$, $k_2 = -1.515$, $a = 6.587$, $b = 6.591$, $c_1 = -5$, $c_2 = 0$. The boundary of $\mathcal{C}$ cannot be described as in (4.8). Note that since B is a column vector, (4.6) is independent of G. By numerically solving the conditions in (4.4), it follows that $(5.431, 0.487)$ and $(4.651, 0.417)$ are undesired equilibria of (4.6). Moreover, using the expression of the Jacobian in [120, Proposition 10], it follows that $(5.431, 0.487)$ is asymptotically stable and $(4.651, 0.417)$ is a saddle point. This is illustrated in Figure 4.9. △

The stability properties of undesired equilibria remain the same for a large

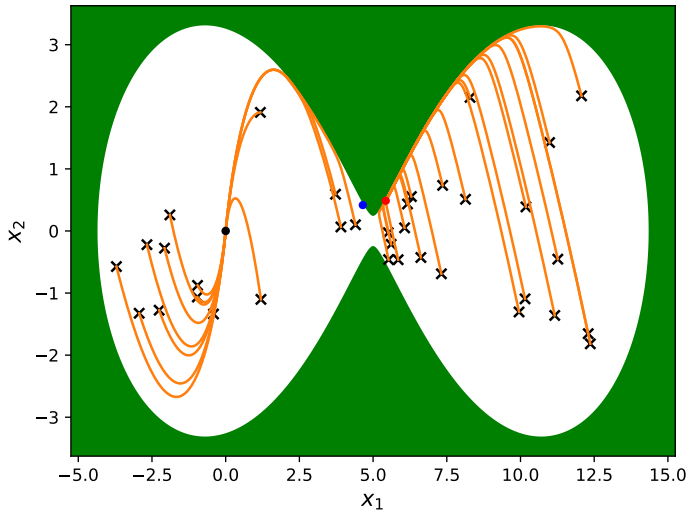


Figure 4.9: Plot of different trajectories (in orange) for Example 4.3.3. The unsafe set is colored in green. Black crosses denote initial conditions, the black dot denotes the origin, the red dot denotes an asymptotically stable undesired equilibrium, and the blue dot denotes an undesired equilibrium that is a saddle point.

class of CBFs, cf. [120, Proposition 6.2], and therefore the asymptotically stable undesired equilibria defined in Examples 4.3.2 and 4.3.3 exist for a large class of CBFs, not just the ones defined therein.

4.3.2 Bounded unsafe set

Here we study the case where the unsafe set is bounded. In this case, recall (cf. our discussion after Proposition 4.2.9) that [17, Proposition 3] implies that there does not exist a safe globally asymptotically stabilizing controller. If no limit cycles exist (for example, under the conditions of Proposition 4.2.5), by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], this implies that there must exist at least one undesired equilibrium. We next provide two examples that illustrate how system (4.6) for linear planar plants can give rise in this case to asymptotically stable undesired equilibria, similarly to Examples 4.3.2 and 4.3.3.

Example 4.3.4. (Nonconvex obstacle with asymptotically stable undesired equilibria): Consider the single integrator in the plane, i.e., (4.6) with $A = \mathbb{0}_2$, $B = \mathbf{I}_2$,

and

$$K = \begin{bmatrix} -k_1 & 0 \\ 0 & -k_2 \end{bmatrix}, \; h(\mathbf{x}) = -b^4 + \left\| \mathbf{x} - \begin{bmatrix} a \\ c_2 \end{bmatrix} \right\|^2 \left\| \mathbf{x} + \begin{bmatrix} a \\ -c_2 \end{bmatrix} \right\|^2, \; \alpha(s) = 10s,$$

with $k_1 > 0$, $k_2 > 0$, $a > 0$, $b > 0$, $c_2 > 0$ and $\frac{b}{a} \in (1, \sqrt{2})$. It follows that $\mathbf{x}_* = (0, \sqrt{-a^2 + b^2} + c_2)$ and $\delta_{\mathbf{x}_*} = -\frac{c_2 + \sqrt{-a^2+b^2}}{2\sqrt{-a^2+b^2}b^2} < 0$ solve (4.4) and therefore $\mathbf{x}_* \in \hat{\mathcal{E}}$ is an undesired equilibrium. Moreover, by leveraging [120, Proposition 11], the Jacobian of (4.6) evaluated at $\mathbf{x}_*$ is equal to

$$J(\mathbf{x}_*) = \begin{bmatrix} k_2(b^2 - 2a^2)\frac{c_2 + \sqrt{-a^2+b^2}}{\sqrt{-a^2+b^2}b^2} & 0 \\ 0 & -\alpha'(0) \end{bmatrix}.$$

Note that $J(\mathbf{x}_*)$ is a diagonal matrix and since $\alpha'(0) > 0$, $k_2 > 0$, $c_2 > 0$, and $\frac{b}{a} < \sqrt{2}$, all eigenvalues of $J(\mathbf{x}_*)$ are negative and hence $\mathbf{x}_*$ is asymptotically stable. Figure 4.10 shows different trajectories of the closed-loop system obtained with $k_1 = 1$, $k_2 = 1$, $a = 3$, $b = 1.05a$, $c_2 = 4$.

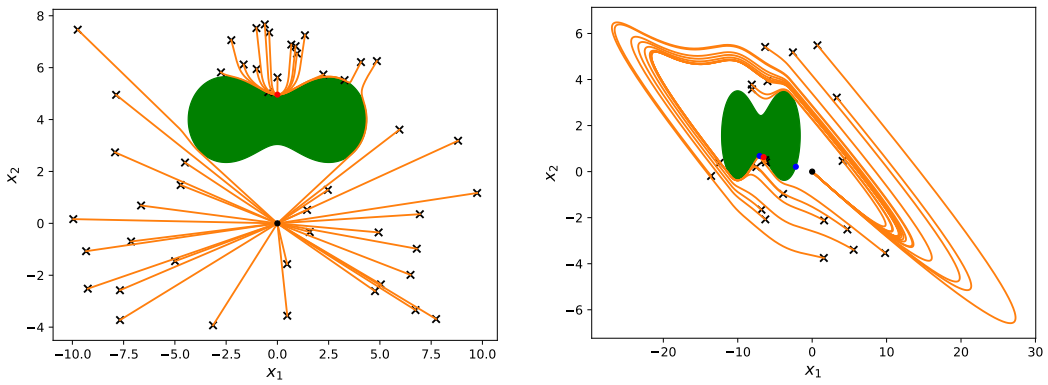


Figure 4.10: Plot of different trajectories of (4.6) for the single integrator system (left) and the underactuated system in (right) in Example 4.3.4. The unsafe set is colored in green. Trajectories are depicted in orange. Black crosses denote initial conditions, the black dot denotes the origin, and the red dot denotes the asymptotically stable undesired equilibrium.

Next we present a similar example for a linear underactuated system. Consider (4.6) with

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \; B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \; K = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix},$$

$$h(\mathbf{x}) = -b^4 + \left\| \mathbf{x} - \begin{bmatrix} a - c_1 \\ c_2 \end{bmatrix} \right\|^2 \left\| \mathbf{x} + \begin{bmatrix} a + c_1 \\ -c_2 \end{bmatrix} \right\|^2, \; \alpha(s) = 10s,$$

where $a_{11} = 0.268$, $a_{12} = 2.866$, $a_{21} = 0.151$, $a_{22} = 1.526$, $b_1 = 0.350$, $b_2 = -0.151$, $k_1 = -41.72$, $k_2 = -174.8$, $a = 3.684$, $b = 3.785$, $c_1 = 6.891$, $c_2 = 1.565$. Note that since B is a column vector, (4.6) is independent of G. By numerically solving the conditions in (4.4), we obtain three undesired equilibria, two of which, located at $(-7.062, 0.682)$ and $(-2.197, 0.212)$, are saddle points and another, located at $(-6.519, 0.629)$, which is asymptotically stable. Figure 4.10 shows that some of the trajectories of (4.6) converge to $(-6.519, 0.629)$, while some others converge to the origin. △

Example 4.3.4 shows that the closed-loop system (4.6) can have asymptotically stable undesired equilibria. A natural question is to ask whether changing the nominal controller would make these equilibria disappear. The following example answers this question in the negative, showing that asymptotically stable undesired equilibria can exist for all nominal stabilizing controllers.

Example 4.3.5. (Asymptotically stable equilibria can exist for all linear nominal controllers): Consider a linear underactuated system:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \; B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \; K = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}.$$

Given $c_1 > 0$, $c_2 > 0$, $r_1 > 0$, $r = c_1 - r_1$ and $R = c_1 + r_1$, suppose that $R < c_2$ and $r < c_1$. Consider also the sets

$$\begin{aligned}
\mathcal{O}_1 &:= \{(x_1, x_2) \in \mathbb{R}^2 : h_1(x) := -(x_1 + c_1)^2 - (x_2 - c_2)^2 + r_1^2 > 0, \quad h_2(x) = x_2 - c_2 > 0\}, \\
\mathcal{O}_2 &:= \{(x_1, x_2) \in \mathbb{R}^2 : h_3(x) := -x_1^2 - (x_2 - c_2)^2 + (c_1 + r_1)^2 > 0, \\
&\qquad h_4(x) = -x_1^2 - (x_2 - c_2)^2 + (c_1 - r_1)^2 < 0, \quad h_5(x) = c_2 - x_2 > 0\}, \\
\mathcal{O}_3 &:= \{(x_1, x_2) \in \mathbb{R}^2 : h_6(x) = r_1^2 - (x_1 - c_1)^2 - x_2^2 > 0, \quad h_7(x) = x_2 - c_2 > 0\},
\end{aligned}$$

and define the safe set $\mathcal{C} = \mathbb{R}^2 \backslash (\mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_3)$, and $h : \mathbb{R}^2 \to \mathbb{R}$ be such that $\mathcal{C} = \{x \in \mathbb{R}^2 : h(x) \geq 0\}$, $\partial\mathcal{C} = \{x \in \mathbb{R}^2 : h(x) = 0\}$. By letting $a_{11} = -0.169$, $a_{21} = -1.989$, $a_{12} = -3$, $a_{22} = -1.4$, $b_1 = -2.355$, $b_2 = -1.707$, $c_1 = 6.1$, $c_2 = 10.027$, $r_1 = 2.129$, it follows that $\mathbf{x}_* = (3.157, 7.619)$ is an asymptotically stable undesired equilibrium for any nominal stabilizing controller $\mathbf{u} = -K\mathbf{x}$. We provide a more detailed justification

about this in Example 4.4.6 of the Appendix. We note also that our argument does not preclude the existence of nonlinear nominal stabilizing controllers for which there does not exist any asymptotically stable undesired equilibrium. △

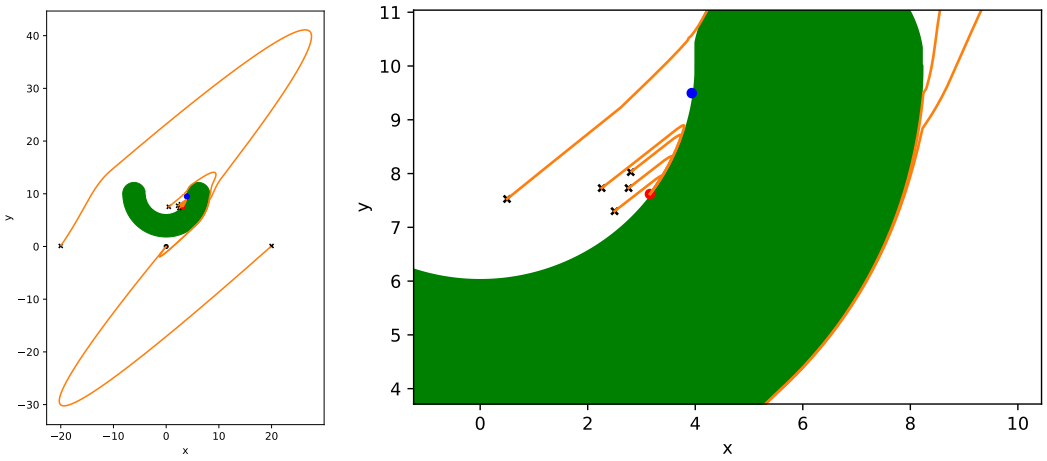


Figure 4.11: Plot of different trajectories of (4.6) for the underactuated system in Example 4.3.4. The unsafe set is colored in green. Trajectories are depicted in orange. Black crosses denote initial conditions, the black dot denotes the origin, the red dot denotes an asymptotically stable undesired equilibrium, and the blue dot denotes an undesired equilibrium that is a saddle point. The plot on the left is a zoomed-in version of the plot on the right.

4.3.3 Ellipsoidal unsafe sets

Despite the title of this section, in the following we focus on studying the dynamical properties of safety filters for LTI systems and *circular* obstacles. Accordingly, we consider the circular unsafe set:

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^2 : h(\mathbf{x}) = \|\mathbf{x} - \mathbf{x}_c\|^2 - r^2 \geq 0\},$$

with $\mathbf{x}_c = (x_{c,1}, x_{c,2}) \in \mathbb{R}^2$ the center. This is justified by the following result, which shows that the undesired equilibria of (4.6) and their stability properties for general ellipsoidal obstacles are equivalent to those of a system with circular obstacles.

Proposition 4.3.6. (Safety filters with ellipsoidal and circular obstacles have the same dynamical properties): *Let* $\mathbf{x}_c \in \mathbb{R}^2$, $P \in \mathbb{R}^{2\times 2}$ *positive definite,* $h(\mathbf{x}) = (\mathbf{x} -$

$\mathbf{x}_c)^\top P(\mathbf{x}-\mathbf{x}_c)-1$, *and* $\mathcal{C}:=\{\mathbf{x}\in\mathbb{R}^n : h(\mathbf{x})\geq 0\}$. *Suppose that* h *is a strict CBF and Assumption 1 holds. Further suppose that* $P=E^\top E$, *with* $E\in\mathbb{R}^{2\times 2}$ *also positive definite, and define* $\hat{\mathbf{x}}_c=E\mathbf{x}_c$, $\hat{h}(\hat{\mathbf{x}})=(\hat{\mathbf{x}}-\hat{\mathbf{x}}_c)^\top(\hat{\mathbf{x}}-\hat{\mathbf{x}}_c)-1$ *and* $\hat{\mathcal{C}}=\{\mathbf{x}\in\mathbb{R}^n : \hat{h}(\mathbf{x})\geq 0\}$. *Moreover, let* $\hat{A}=EAE^{-1}$, $\hat{B}=EB$, $\hat{G}(\hat{\mathbf{x}})=G(E^{-1}\hat{\mathbf{x}})$ *and* $\hat{\eta}(\hat{\mathbf{x}})=\nabla\hat{h}(\hat{\mathbf{x}})^\top(\hat{A}-\hat{B}KE^{-1})\hat{\mathbf{x}}+\alpha(\hat{h}(\hat{\mathbf{x}}))$. *Consider the system*

$$\dot{\hat{\mathbf{x}}}=\hat{F}(\hat{\mathbf{x}}):=(\hat{A}-\hat{B}KE^{-1})\hat{\mathbf{x}}+\hat{B}\hat{v}(\hat{\mathbf{x}}), \tag{4.18}$$

where

$$\hat{v}(\hat{\mathbf{x}})=\begin{cases}0, & \text{if } \hat{\eta}(\hat{\mathbf{x}})\geq 0,\\ -\frac{\hat{\eta}(\hat{\mathbf{x}})\hat{G}(\hat{\mathbf{x}})^{-1}(\hat{\mathbf{x}})\hat{B}^\top\nabla\hat{h}(\hat{\mathbf{x}})}{\|\hat{B}^\top\nabla\hat{h}(\hat{\mathbf{x}})\|^2_{\hat{G}(\hat{\mathbf{x}})^{-1}}}, & \text{if } \hat{\eta}(\hat{\mathbf{x}})<0\end{cases} \tag{4.19}$$

Then,

(1) $\hat{\mathcal{C}}$ *is forward invariant under system* (4.18) *and* $\mathcal{C}$ *is forward invariant under system* (4.6)*;*

(2) system (4.18) *is locally Lipschitz and system* (4.6) *is locally Lipschitz;*

(3) (A,B) *is stabilizable if and only if* $(\hat{A},\hat{B})$ *is stabilizable;*

(4) $\hat{\mathbf{x}}_*\in\mathbb{R}^2$ *is an undesired equilibrium of* (4.18) *if and only if* $\mathbf{x}_*:=E^{-1}\hat{\mathbf{x}}_*$ *is an undesired equilibrium of* (4.6)*;*

(5) the Jacobian of $\hat{F}$ *at* $\hat{\mathbf{x}}_*$ *and the Jacobian of* F *at* $\mathbf{x}_*$ *are similar.*

Proof. Re: *1*, by construction, system (4.18) satisfies $\nabla\hat{h}(\hat{\mathbf{x}})^\top\hat{F}(\hat{\mathbf{x}})+\alpha(\hat{h}(\hat{\mathbf{x}}))\geq 0$ for all $\hat{\mathbf{x}}\in\hat{\mathcal{C}}$; similarly, system (4.6) satisfies $\nabla h(\mathbf{x})^\top F(\mathbf{x})+\alpha(h(\mathbf{x}))\geq 0$ for all $\mathbf{x}\in\mathcal{C}$. These two conditions imply, respectively, that $\hat{\mathcal{C}}$ is forward invariant under system (4.18) and $\mathcal{C}$ is forward invariant under system (4.6) [23, Theorem 2].

Re: *2*, let us prove that for all $\hat{\mathbf{x}}\in\hat{\mathcal{C}}$, there exists $\hat{\mathbf{u}}\in\mathbb{R}^m$ such that $\nabla\hat{h}(\hat{\mathbf{x}})^\top(\hat{A}\hat{\mathbf{x}}+\hat{B}\hat{\mathbf{u}})+\alpha(h(\hat{\mathbf{x}}))>0$, which implies by [103, Lemma III.2] that (4.18) is locally Lipschitz. Indeed, suppose that $(EB)^\top(\hat{\mathbf{x}}-\hat{\mathbf{x}}_c)=0$. Since for any $\hat{\mathbf{x}}\in\mathbb{R}^n$, there exists $\mathbf{x}\in\mathbb{R}^n$ such that $\hat{\mathbf{x}}=E\mathbf{x}$ and h is a strict CBF, we have $0=(EB)^\top(\hat{\mathbf{x}}-\hat{\mathbf{x}}_c)=B^\top E^\top E(\mathbf{x}-\mathbf{x}_c)=BP(\mathbf{x}-\mathbf{x}_c)=0$, which means that $(\hat{\mathbf{x}}-\hat{\mathbf{x}}_c)^\top EAE^{-1}\hat{\mathbf{x}}=$

$(\mathbf{x}-\mathbf{x}_c)^\top E^\top EA\mathbf{x} = (\mathbf{x}-\mathbf{x}_c)^\top P^\top A\mathbf{x} > 0$. Hence for all $\hat{\mathbf{x}} \in \hat{\mathcal{C}}$, there exists $\hat{\mathbf{u}} \in \mathbb{R}^m$ such that $\nabla\hat{h}(\hat{\mathbf{x}})^\top(\hat{A}\hat{\mathbf{x}} + \hat{B}\mathbf{u}) + \alpha(h(\hat{\mathbf{x}})) > 0$, from which it follows that (4.18) is locally Lipschitz.

Re: *3*, this follows from the observation that if $A - BK$ is Hurwitz then $\hat{A} - \hat{B}KE^{-1} = E(A - BK)E^{-1}$ is also Hurwitz. This is because E is nonsingular and similar matrices have the same eigenvalues [115, Corollary 1.3.4].

Re: *4*, note that $\hat{\mathbf{x}}_*$ satisfies the conditions in Lemma 4.2.1 for (4.18) if and only if $\mathbf{x}_*$ satisfies the conditions in Lemma 4.2.1 for (4.6).

Re: *5*, we note that $F(E^{-1}\hat{\mathbf{x}}) = E^{-1}\hat{F}(\hat{\mathbf{x}})$ for any $\hat{\mathbf{x}} \in \mathbb{R}^2$. Since the safety filter is active at undesired equilibria, $\eta(\mathbf{x}_*) < 0$. Now, let J be the Jacobian of (4.6) at $\mathbf{x}_*$, and let $\hat{J}$ be the Jacobian of (4.18) at $\hat{\mathbf{x}}_*$. By the chain rule, $\hat{J} = EJE^{-1}$, which implies that J and $\hat{J}$ are similar. □

Underactuated LTI planar systems

In the under-actuated case, we write

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \; B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \; K = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}^\top. \tag{4.20}$$

Throughout the section, we let $\beta = a_{11}b_2 - b_1a_{21}$, $\gamma = a_{22}b_1 - b_2a_{12}$, and $T_3 = -\gamma x_{c,2} + \beta x_{c,1}$. We note also that since in this case G is a scalar, (4.6) is independent of G. The following results give conditions on h and system (4.20) that ensure that Assumption 1 holds and h is a strict CBF.

Lemma 4.3.7 (Conditions for Assumption 1)**.** *Assumption 1 holds if and only if* $\|\mathbf{x}_c\|^2 > r^2$.

The proof of this result is straightforward.

Proposition 4.3.8 (Conditions for h to be a strict CBF)**.** *Let* $\alpha_0 > 0$, $T_1 := b_2\beta + b_1\gamma + \frac{1}{2}\alpha_0(b_2^2 + b_1^2)$, *and* $T_2 := (\beta x_{c,1} - \gamma x_{c,2})^2 + 2\alpha_0 r^2 T_1$. *Suppose that* $r > 0$, $b_1^2 + b_2^2 > 0$, $T_1 > 0$, *and*

$$\frac{r}{\sqrt{b_2^2 + b_1^2}} > \frac{|T_3| + \sqrt{T_2}}{2T_1}.$$

Then, h is a strict CBF with the linear extended class $\mathcal{K}_\infty$ function $\alpha(s) = \alpha_0 s$.

Proof. We need to ensure that all $\mathbf{x} \in \mathbb{R}^2$ such that $h(\mathbf{x}) \geq 0$ and $B^\top(\mathbf{x} - \mathbf{x}_c) = 0$, satisfy $2(\mathbf{x} - \mathbf{x}_c)A\mathbf{x} + \alpha(h(\mathbf{x})) > 0$. First suppose $b_1 \neq 0$. Equivalently, we need to ensure that

$$\begin{aligned}&(x_2 - x_{c,2})^2\Big((a_{11} + \frac{\alpha_0}{2})\frac{b_2^2}{b_1^2} - \frac{b_2}{b_1}(a_{12} + a_{21}) + a_{22} + \frac{\alpha_0}{2}\Big)\\ &+(x_2 - x_{c,2})\Big(a_{22}x_{c,2} - \frac{b_2}{b_1}a_{11}x_{c,1} - \frac{b_2}{b_1}a_{12}x_{c,2} + a_{21}x_{c,1}\Big) - \frac{1}{2}\alpha_0 r^2 > 0\end{aligned} \tag{4.21}$$

whenever $(x_2 - x_{c,2})^2 \geq r^2/((b_2^2/b_1^2) + 1)$. This follows by assumption. The condition $T_1 > 0$ ensures that the coefficient of $x_2 - x_{c,2}$ of (4.21) is positive, and the condition $T_2 > 0$ ensures that the discriminant of (4.21) is positive. Now, by calculating the roots of the quadratic equation in $x_2 - x_{c,2}$ we observe that the rest of the conditions in the statement ensure that (4.21) holds whenever $(x_2 - x_{c,2})^2 \geq r^2/((b_2^2/b_1^2) + 1)$. The case $b_1 = 0$ follows by a similar argument. □

The following result shows that for circular obstacles and linear planar underactuated systems, (4.4) can be solved explicitly, characterizing the undesired equilibria of the closed-loop system.

Proposition 4.3.9. (Equilibria in Underactuated Systems with Circular Obstacles): *Suppose that Assumptions 1, 2 and the conditions in Proposition 4.3.8 hold. Define* $\mathbf{x}_{*,+} := (\gamma z_+, \beta z_+)$ *and* $\mathbf{x}_{*,-} := (\gamma z_-, \beta z_-)$, *where*

$$\begin{aligned}z_+ &= \frac{\gamma x_{c,1} + \beta x_{c,2} + \sqrt{r^2(\gamma^2 + \beta^2) - T_3^2}}{\gamma^2 + \beta^2},\\ z_- &= \frac{\gamma x_{c,1} + \beta x_{c,2} - \sqrt{r^2(\gamma^2 + \beta^2) - T_3^2}}{\gamma^2 + \beta^2}.\end{aligned}$$

Then, $\gamma x_{c,1} + \beta x_{c,2} \neq 0$, *and*

(1) if $\gamma x_{c,1} + \beta x_{c,2} < 0$, $\hat{\mathcal{E}} = \{\mathbf{x}_{*,+}\}$ *is the only undesired equilibrium of the closed-loop system* (4.6). *Moreover,* $\mathbf{x}_{*,+}$ *is a saddle point;*

(2) if $\gamma x_{c,1} + \beta x_{c,2} > 0$, $\hat{\mathcal{E}} = \{\mathbf{x}_{*,-}\}$ *is the only undesired equilibrium of the closed-loop system* (4.6). *Moreover,* $\mathbf{x}_{*,-}$ *is a saddle point.*

Proof. The fact that $\gamma x_{c,1}+\beta x_{c,2} \neq 0$ is shown in Lemma 4.4.5. The same result also implies that the expressions for $\mathbf{x}_{*,+}$ and $\mathbf{x}_{*,-}$ are well defined (note that if $\gamma^2+\beta^2 = 0$, then Assumption 2 would not hold). Moreover, it follows from Lemma 4.2.1 that $\mathcal{E} = \{\mathbf{x}_{*,+}, \mathbf{x}_{*,-}\}$ is the set of potential undesired equilibria for system (4.6) when the system data is of the form (4.20). In order to ensure that $\mathbf{x}_{*,+}$ is an undesired equilibrium of the closed-loop system, the condition $(\mathbf{x}-\mathbf{x}_c)^\top(A-BK)\mathbf{x}|_{\mathbf{x}=\mathbf{x}_{*,+}} < 0$ should hold. By using the expression of $\mathbf{x}_{*,+}$, the condition is equivalent to

$$z_+ T_4\Big(b_1(\gamma z_+ - x_{c,1}) + b_2(\beta z_+ - x_{c,2})\Big) < 0, \tag{4.22}$$

where $T_4 = a_{11}a_{22} - a_{12}a_{21} - k_1\gamma - k_2\beta$. Since $A-BK$ is Hurwitz, $a_{11}a_{22} - a_{12}a_{21} - \gamma k_1 - \beta k_2 > 0$. This implies that $T_4 > 0$ and therefore (4.22) is equivalent to

$$z_+(b_1(\gamma z_+ - x_{c,1}) + b_2(\beta z_+ - x_{c,2})) < 0. \tag{4.23}$$

Now, let us show that $b_1(\gamma z_+ - x_{c,1}) + b_2(\beta z_+ - x_{c,2}) > 0$. Indeed, this is equivalent to

$$T_3(\gamma b_2 - \beta b_1) + (\gamma b_1 + \beta b_2)\sqrt{r^2(\gamma^2+\beta^2) - T_3^2} > 0,$$

and since $\gamma b_1 + \beta b_2 > 0$ as argued in the proof of Lemma 4.4.5, this could only not hold if $T_3(\gamma b_2 - \beta b_1) < 0$ and $(\gamma b_1+\beta b_2)^2(r^2(\gamma^2+\beta^2)-T_3^2) \leq T_3^2(\gamma b_2 - \beta b_1)^2$. However, this last condition is in contradiction with (4.26) in the proof of Lemma 4.4.5. Therefore, (4.23) holds if and only if $z_+ < 0$, which is equivalent to: $\gamma x_{c,1}+\beta x_{c,2} < 0$ and

$$|\gamma x_{c,1} + \beta x_{c,2}| > \sqrt{r^2(\gamma^2+\beta^2) - T_3^2}. \tag{4.24}$$

Note that since $r^2(\gamma^2+\beta^2) - T_3^2 = (x_{c,1}\gamma + x_{c,2}\beta)^2 - (\gamma^2+\beta^2)(x_{c,1}^2 + x_{c,2}^2 - r^2) < (x_{c,1}\gamma + x_{c,2}\beta)^2$ (where in the last inequality we have used the fact that $x_{c,1}^2 + x_{c,2}^2 > r^2$), it follows that the last of the inequalities in (4.24) always holds. Therefore, $\mathbf{x}_{*,+}$ is an undesired equilibrium of the closed-loop system if and only if $\gamma x_{c,1}+\beta x_{c,2} < 0$. The fact that $\mathbf{x}_{*,+}$ is the unique undesired equilibrium and is a saddle point follows from Proposition 4.2.9. An analogous argument shows that $\mathbf{x}_{*,-}$ is the unique undesired equilibrium if and only if $\gamma x_{c,1} + \beta x_{c,2} > 0$, in which case it is a saddle point. □

Note that the statement of Proposition 4.3.9 is consistent with Proposition 4.2.9, since it also states that, provided that all the undesired equilibria are not degenerate, their number is odd.

Remark 4.3.10. (Almost global asymptotic stability): The Stable Manifold Theorem [101, Ch. 2.7] ensures that if $\mathbf{x}_*$ is a saddle point in $\mathbb{R}^2$, the local stable manifold is 1-dimensional. Therefore, it has measure zero. Moreover, the global stable manifold must also have measure zero. If this were not the case, solutions would have to intersect. However this is not possible due to the uniqueness of solutions. Hence the global stable manifold is exactly equal to $\{\mathbf{x}_0 \in \mathbb{R}^n : \lim_{t\to\infty} \mathbf{x}(t;\mathbf{x}_0) = \mathbf{0}_n\}$. It follows that the set of initial conditions whose associated trajectory converges to $\mathbf{x}_*$ has measure zero. Hence, by appropriately tuning the class $\mathcal{K}_\infty$ function to rule out limit cycles (cf. Proposition 4.2.5), the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1] implies that the origin is almost globally asymptotically stable (i.e., asymptotically stable with a region of attraction equal to $\mathbb{R}^2$ minus a set of measure zero). □

Fully actuated LTI planar systems

Here we consider the system (4.6) and assume that $n = 2$, $m = 2$, and $B \in \mathbb{R}^{2\times 2}$ is invertible; in this case h is a strict CBF and Assumption 2 is satisfied. Throughout the section, $\tilde{A} = A - BK$. The following result summarizes the different possible undesired equilibria of (4.6) in the special case where $\mathbf{x}_c$, the center of the circular unsafe set, is an eigenvector of $\tilde{A}$.

Proposition 4.3.11. (Characterization of undesired equilibria): *Suppose Assumption 1 is satisfied, B is invertible, and $\tilde{A}$ is Hurwitz. Suppose also that $\mathbf{x}_c$ is an eigenvector of $\tilde{A}$. Then one of the following is true:*

(1) $|\mathcal{E}| = 2$, $|\hat{\mathcal{E}}| = 1$, and $\hat{\mathcal{E}}$ consists of a degenerate equilibrium;

(2) $|\mathcal{E}| = 2$, $|\hat{\mathcal{E}}| = 1$, and $\hat{\mathcal{E}}$ consists of a saddle point;

(3) $|\mathcal{E}| = 3$, $|\hat{\mathcal{E}}| = 2$, and $\hat{\mathcal{E}}$ consists of a saddle point and a degenerate equilibrium;

$\tilde{A}$ diagonalizable,	SP	DE	ASE
$(\mathbf{v}_i^\top \mathbf{v}_j)^2 < 1 - \frac{(\lambda_i-\lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2}$	1	0	0
$(\mathbf{v}_i^\top \mathbf{v}_j)^2 = 1 - \frac{(\lambda_i-\lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2}$	1	1	0
$(\mathbf{v}_i^\top \mathbf{v}_j)^2 > 1 - \frac{(\lambda_i-\lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2}$	2	0	1

(a)

$\tilde{A}$ non-diagonalizable	SP	DE	ASE
$(\mathbf{v}_1^\top \mathbf{v}_2)^2 < 1 - \frac{r^2}{\lambda^2 \|\mathbf{x}_c\|^2}$	1	0	0
$(\mathbf{v}_1^\top \mathbf{v}_2)^2 = 1 - \frac{r^2}{\lambda^2 \|\mathbf{x}_c\|^2}$	1	1	0
$(\mathbf{v}_1^\top \mathbf{v}_2)^2 > 1 - \frac{r^2}{\lambda^2 \|\mathbf{x}_c\|^2}$	2	0	1

(b)

Table 4.1: Characterization of undesired equilibria (SP: saddle point, DE: degenerate equilibrium, ASE: asymptotically stable equilibrium) when $\mathbf{x}_c$ is an eigenvector of $\tilde{A}$. In (a), $\tilde{A}$ is diagonalizable, i.e., $\tilde{A}\mathbf{x}_c = \lambda_i \mathbf{x}_c$, $\mathbf{v}_i = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\tilde{A}\mathbf{v}_j = \lambda_j \mathbf{v}_j$, $\|\mathbf{v}_j\| = 1$, $i, j = \{1, 2\}$, and $\{\mathbf{v}_i, \mathbf{v}_j\}$ linearly independent. We assume that $\frac{(\lambda_i-\lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2} \neq 1$. In (b), $\tilde{A}$ is not diagonalizable, i.e., $\tilde{A}\mathbf{v}_2 = \lambda \mathbf{v}_2 + \mathbf{v}_1$, $\mathbf{v}_1 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\tilde{A}\mathbf{x}_c = \lambda \mathbf{x}_c$, and $\|\mathbf{v}_2\| = 1$.

(4) $|\mathcal{E}| = 4$, $|\hat{\mathcal{E}}| = 3$, *and* $\hat{\mathcal{E}}$ *consists of an asymptotically stable equilibrium and two saddle points.*

The proof of Proposition 4.3.11 is provided in the Appendix. Table 4.1 outlines the majority of the cases discussed in the proof of Proposition 4.3.11. For different numerical examples illustrating the different cases outlined in Table 4.1, we refer the reader to [6, Figure 1]. We build on this result to show that the eigenvalues of $\tilde{A}$ do not determine the stability properties of undesired equilibria.

Proposition 4.3.12. (Spectrum of $\tilde{A}$ does not determine stability properties of undesired equilibria): *Suppose Assumption 1 is satisfied and B is invertible. Then for any given negative λ_1 and λ_2, there exists $K_1 \in \mathbb{R}^{2\times 2}$ and $K_2 \in \mathbb{R}^{2\times 2}$ in the set $\{K \in \mathbb{R}^{2\times 2} : \lambda_1, \lambda_2 = spec(A - BK)\}$, such that (4.6) with $K = K_1$ has an undesired asymptotically stable equilibrium and (4.6) with $K = K_2$, has a single undesired equilibrium, which is a saddle point.*

Proof. First let us construct K_1. Start by supposing that $\lambda_1 = \lambda_2$. Let $\mathbf{v}_1 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$ and $\theta = \arccos\sqrt{Q_1}$, $Q_1 := \max\{0, 1 - \frac{r^2}{2\lambda_1^2 \|\mathbf{x}_c\|}\}$. Then, $\mathbf{v}_1^\top \mathbf{v}_2 = \cos(\theta) \|\mathbf{v}_1\|^2 = \cos(\theta)$. We let

$$K_1 := B^{-1}\Big(A - \begin{bmatrix}\mathbf{v}_1 & \mathbf{v}_2\end{bmatrix}\begin{bmatrix}\lambda_1 & 1\\ 0 & \lambda_1\end{bmatrix}\begin{bmatrix}\mathbf{v}_1 & \mathbf{v}_2\end{bmatrix}^{-1}\Big).$$

By the third row of Table 4.1(b), (4.6) has an undesired asymptotically stable equilibrium. Next, suppose that $\lambda_1 \neq \lambda_2$. Let $\mathbf{v}_1 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\mathbf{v}_2 = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mathbf{v}_1$, where $\theta = \arccos\sqrt{Q_2}$, $Q_2 := \max\{0, 1 - \frac{(\lambda_1-\lambda_2)^2 r^2}{2\lambda_1^2\|\mathbf{x}_c\|^2}\}$. Then $\mathbf{v}_1^\top \mathbf{v}_2 = \cos\theta \|\mathbf{v}_1\|_2^2 = \cos\theta$ and

$$K_1 := B^{-1}\Big(A - \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix}^{-1}\Big).$$

By the third row of Table 4.1(a), (4.6) has an undesired asymptotically stable equilibrium.

To construct K_2, we assume without loss of generality that $\lambda_1 \leq \lambda_2$. Note that since both λ_1 and λ_2 are negative, $1 - \frac{(\lambda_i-\lambda_j)^2 r^2}{\lambda_i^2\|\mathbf{x}_c\|^2} > 0$. Let $\mathbf{v}_i = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\mathbf{v}_j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \mathbf{v}_i$, so that $\mathbf{v}_i^\top \mathbf{v}_j = 0$ and define

$$K_2 := B^{-1}\Big(A - \begin{bmatrix} \mathbf{v}_i & \mathbf{v}_j \end{bmatrix} \begin{bmatrix} \lambda_i & 0 \\ 0 & \lambda_j \end{bmatrix} \begin{bmatrix} \mathbf{v}_i & \mathbf{v}_j \end{bmatrix}^{-1}\Big).$$

By the first row of Table 4.1(a), (4.6) has a single undesired equilibrium and it is a saddle point. □

Interestingly, even though one can characterize the global stability properties of the origin based on the eigenvalues of $\tilde{A}$ for the system without a safety filter, this is no longer the case for the system with a safety filter. On the other hand, as a consequence of Proposition 4.3.12, we deduce that it is always possible to choose a nominal controller $\mathbf{u} = -K\mathbf{x}$ such that $\tilde{A}$ has negative eigenvalues and the set of trajectories of (4.6) that do not converge to the origin has measure zero (cf. Remark 4.3.10). Note that, as shown in [120, Proposition 10] and Table 4.1, the extended class $\mathcal{K}_\infty$ function only affects the rate of decay in the stable manifold of the undesired equilibria and it does not affect the existence and stability of undesired equilibria. Therefore, the choice of nominal controller $\mathbf{u} = -K\mathbf{x}$ determines in which of the cases we fall into. Ideally, such nominal controller should be designed so that there exists only one undesired equilibrium and it is a saddle point.

We conclude this section studying the case when $\mathbf{x}_c$ is not an eigenvector of $\tilde{A}$, which requires a more involved technical analysis. The following result characterizes the number of undesired equilibria under appropriate sufficient conditions.

Proposition 4.3.13. (Number of undesired equilibria when $\mathbf{x}_c$ is not an eigenvector): *Suppose Assumption 1 is satisfied, B is invertible, $G(\mathbf{x}) = B^\top B$, $\tilde{A}$ is Hurwitz and $\mathbf{x}_c$ is not an eigenvector of $\tilde{A}$. Then $1 \leq |\hat{\mathcal{E}}| \leq 3$ and $|\mathcal{E} \setminus \hat{\mathcal{E}}| \geq 1$. In addition, if $\lambda_1 \leq \lambda_2$, there exists $\mathbf{x}_* \in \hat{\mathcal{E}}$ with indicator $\delta < \frac{\lambda_1}{2}$.*

The proof of Proposition 4.3.13 is given in the Appendix.

The following result establishes the stability properties of undesired equilibria in the case where $\mathbf{x}_c$ is not an eigenvector under some additional assumptions.

Proposition 4.3.14. (Stability properties of undesired equilibria when $\mathbf{x}_c$ is not an eigenvector): *Suppose Assumption 1 is satisfied, B is invertible, $G(\mathbf{x}) = B^\top B$, $\tilde{A}$ is Hurwitz with two real eigenvalues $\lambda_1 < \lambda_2$ and $\mathbf{x}_c$ is not an eigenvector of $\tilde{A}$. Then there is no undesired equilibrium with indicator $\delta \in \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$. Moreover, if $\mathbf{v}_1$ and $\mathbf{v}_2$ are the eigenvectors associated with λ_1 and λ_2, respectively, and $\mathbf{v}_1^\top \mathbf{v}_2 \geq 0$, $\|\mathbf{v}_1\| = \|\mathbf{v}_2\| = 1$, and $\mathbf{x}_c = \beta_1 \mathbf{v}_1 + \beta_2 \mathbf{v}_2$, the following holds.*

(i) If $\beta_1^2 + \beta_1\beta_2 \mathbf{v}_1^\top \mathbf{v}_2 \geq 0$, then for any undesired equilibrium $\mathbf{x}_*$ with indicator $\delta_{\mathbf{x}_*}$ such that $\delta < \frac{\lambda_1}{2}$, $\mathbf{x}_*$ is a saddle point.

(ii) If $\beta_1\beta_2 \mathbf{v}_2^\top \mathbf{v}_1 + \beta_2^2 \geq 0$, then for any undesired equilibrium $\mathbf{x}_*$ with indicator $\delta_{\mathbf{x}_*}$ such that $\frac{\lambda_2}{2} < \delta < 0$, $\mathbf{x}_*$ is asymptotically stable.

(iii) Define $F_1 : \mathbb{R} \to \mathbb{R}$ as:

$$F_1(\delta) := -|\lambda_1 - 2\delta|^2|\lambda_2 - 2\delta|^2 r^2 + |\lambda_1\beta_1|^2|\lambda_2 - 2\delta|^2 + |\lambda_2\beta_2|^2|\lambda_1 - 2\delta|^2 \tag{4.25}$$
$$+ \lambda_1^*\beta_1^*\lambda_2\beta_2(\lambda_2 - 2\delta)^*(\lambda_1 - 2\delta)\mathbf{v}_1^*\mathbf{v}_2 + \lambda_1\beta_1\lambda_2^*\beta_2^*(\lambda_2 - 2\delta)(\lambda_1 - 2\delta)^*\mathbf{v}_2^*\mathbf{v}_1.$$

If the third-order polynomial $\frac{dF_1(\delta)}{d\delta}$ has only one real root[1] and $\beta_1^2 + \beta_1\beta_2 \mathbf{v}_1^\top \mathbf{v}_2 \geq 0$, then there exists only one undesired equilibrium and it is a saddle point.

The proof of Proposition 4.3.14 is given in the Section 4.4.

[1]For third-order polynomial $ax^3 + bx^2 + cx + d$, its discriminant is defined as $18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$. If $a \neq 0$ and the discriminant is negative, the third-order polynomial only has one real root.

4.4 Appendix

Here we provide a number of supporting results for the technical treatment in this Chapter.

4.4.1 Auxiliary results for Section 4.2

Here we provide auxiliary results for Section 4.2.

Lemma 4.4.1. (Trajectories of globally asymptotically stable system): *Let* $F : \mathbb{R}^n \to \mathbb{R}^n$ *be locally Lipschitz, and suppose that the origin is globally asymptotically stable for the differential equation* $\dot{\mathbf{x}} = F(\mathbf{x})$. *Then, for any* $\mathbf{x}_0 \in \mathbb{R}^n \backslash \{\mathbf{0}_n\}$, *it holds that* $\lim_{t \to -\infty} \|\mathbf{x}(t; \mathbf{x}_0)\| = \infty$.

Proof. Since F is locally Lipschitz and the origin is globally asymptotically stable, by [121, Theorem 4.17] there exists a smooth, positive definite, and radially unbounded function $V : \mathbb{R}^n \to \mathbb{R}$ and a continuous positive definite function $W : \mathbb{R}^n \to \mathbb{R}$ such that $\nabla V(\mathbf{x})^\top f(\mathbf{x}) \leq -W(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$. Now, let $t \geq 0$ and note that $\frac{d}{dt} V(\mathbf{x}(-t; \mathbf{x}_0)) = -\nabla V(\mathbf{x}(-t; \mathbf{x}_0))^\top f(\mathbf{x}(-t; \mathbf{x}_0)) \geq W(\mathbf{x}(-t; \mathbf{x}_0)) \geq 0$. Hence, $V(\mathbf{x}(-t; \mathbf{x}_0)) \geq V(\mathbf{x}_0)$. By letting $\bar{w} = \min_{\{\mathbf{y} \in \mathbb{R}^n : V(\mathbf{y}) \geq V(\mathbf{x}_0)\}} W(\mathbf{y})$, it follows that $\frac{d}{dt} V(\mathbf{x}(-t; \mathbf{x}_0)) \geq \bar{w} > 0$ for all $t \geq 0$. This implies that $\lim_{t \to \infty} V(\mathbf{x}(-t; \mathbf{x}_0)) = \infty$ and since V is radially unbounded, the result follows. □

Lemma 4.4.2. (Convergence and tangency properties of stable manifold): *Let* h *be a strict CBF and suppose Assumption 1 holds. Let* $\mathbb{R}^2 \backslash \mathcal{C}$ *be a bounded connected set. Consider* (4.2) *with* $n = 2$ *and let* $\mathbf{x}_*$ *be an undesired equilibrium of* (4.2) *which is a saddle point. Let* γ *be a subset of the one-dimensional local stable manifold of* $\mathbf{x}_*$ *such that* γ *corresponds to a maximal trajectory of* (4.2) *and there exists* $T > 0$ *with* $\gamma(t) \in Int(\mathcal{C})$ *for all* $t > T$. *Then,*

(1) γ *is not tangent to* $\partial\mathcal{C}$ *at any point;*

(2) if (ω_-, ∞) *is the interval of definition of* γ, *then*

(a) if $\omega_- = -\infty$, *then either* $\lim_{t \to -\infty} \|\gamma(t)\| = \infty$, $\lim_{t \to -\infty} \|\gamma(t)\| = \mathbf{x}'_*$, *with* $\mathbf{x}'_*$ *another equilibrium of* (4.2), *or* $\lim_{t \to -\infty} \|\gamma(t)\|$ *converges to a limit cycle;*

(b) if $\omega_- > -\infty$*, then* $\lim_{t\to\omega_-} \gamma(t) \notin \mathcal{C}$.

Proof. To show 1, we reason by contradiction. Figure 4.12 serves as visual aid for the different elements defined in the proof. Suppose that γ is tangent to $\partial\mathcal{C}$ at a point $\bar{\mathbf{q}}$. Then, $\bar{\mathbf{q}} = \gamma(t_{\bar{\mathbf{q}}})$ for some $t_{\bar{\mathbf{q}}} \in \mathbb{R}$, and there exists $T_{\bar{\mathbf{q}}} > 0$ small enough with $\gamma(t) \in \text{Int}(\mathcal{C})$ for all $t \in (t_{\bar{\mathbf{q}}} - T_{\bar{\mathbf{q}}}, t_{\bar{\mathbf{q}}})$. Now, note that there exists a sufficiently small neighborhood $\mathcal{N}_{\bar{\mathbf{q}}}$ of $\bar{\mathbf{q}}$ such that one of the arches ζ between $\partial\mathcal{C}$ and γ defined by $\mathcal{N}_{\bar{\mathbf{q}}}$ is such that all trajectories of (4.2) with initial condition in ζ stay between $\partial\mathcal{C}$ (because $\mathcal{C}$ is forward invariant) and γ (because of uniqueness of solutions), and stay inside $\mathcal{N}_{\bar{\mathbf{q}}}$ at all times (by continuity of the vector field (4.2), $\gamma'(t_{\bar{\mathbf{q}}}) \neq \mathbf{0}_n$, and because $\mathcal{N}_{\bar{\mathbf{q}}}$ is sufficiently small). However, it is not possible that such trajectories stay inside the region defined by ζ, $\partial\mathcal{C}$ and γ by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], because $\bar{\mathbf{q}}$ is not an equilibrium point and the region defined by ζ, $\partial\mathcal{C}$ and γ does not contain limit cycles, because such limit cycle would encircle only points in the interior of $\mathcal{C}$ [**?**, Corollary 6.26]. Hence, we have reached a contradiction, which means that γ is not tangent to $\partial\mathcal{C}$ at any point. Let us now show 2. Part (a) follows by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], whereas part (b) follows from the fact that if $\lim_{t\to\omega_-} \gamma(t) \in \mathcal{C}$, since (4.2) is well-defined at all points in the safe set, then γ is well-defined as $t \to \omega_-$, and the interval of definition of γ can be increased, contradicting the assumption that γ is a maximal solution. □

Lemma 4.4.3. (Existence of stable manifold exiting set with no limit cycles): *Let h be a strict CBF and suppose Assumption 1 holds. Let $\mathbb{R}^2\backslash\mathcal{C}$ be a bounded connected set. Consider* (4.2) *with $n = 2$ and let $\{\mathbf{x}_*^{(i)}\}_{i=1}^k \subset \partial\mathcal{C}$ be its set of undesired equilibria. Denote by $\mathcal{L} \subset [k]$ the index set of undesired equilibria that are saddle points and let $\tilde{\Phi}$ be a compact forward invariant set containing the origin and $\mathbb{R}^2\backslash\mathcal{C}$ and such that $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycles. For each $j \in \mathcal{L}$, let γ_j be a subset of the one-dimensional local stable manifold of* (4.2) *at $\mathbf{x}_*^{(j)}$ such that γ_j corresponds to a maximal trajectory and there exists $T > 0$ with $\gamma_j(t) \in Int(\mathcal{C})$ for all $t > T$. Then, there exists at least one $j \in \mathcal{L}$ and $\tilde{t}_j \in \mathbb{R}$ such that $\gamma_j(\tilde{t}_j) \in \partial\tilde{\Phi}$ and $\gamma_j(t) \notin \tilde{\Phi}$ for all $t < t_j$.*

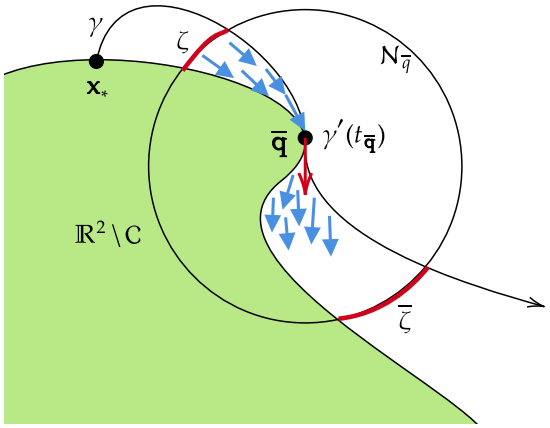


Figure 4.12: Sketch of the setting considered in the proof of Lemma 4.4.2. The unsafe set is depicted in green, whereas the closed-loop vector field at the point of tangency is the red arrow, the blue arrows denote the vector field elsewhere, and the arches ζ and $\bar{\zeta}$ are depicted in red.

Proof. Let us reason by contradiction. If the statement does not hold, then using Lemma 4.4.2(ii), we deduce that for all $j \in \mathcal{L}$, one of the following holds:

(1) there exists $t_j > 0$ such that $\lim_{t \to -t_j} \gamma_j(t) \in \mathbb{R}^2 \setminus \mathcal{C}$;

(2) $\gamma_j(t)$ converges to a limit cycle in $\tilde{\Phi} \cap \mathcal{C}$;

(3) $\lim_{t \to -\infty} \gamma_j(t) = \mathbf{x}_*^{(\bar{j})}$ for some $\bar{j} \in [k]$.

Since $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycles, case 2 is not possible. If for all $j \in \mathcal{L}$, either 1 or 3 hold, there exists a compact set $\tilde{\mathcal{O}}$, whose boundary is comprised of $\partial(\mathbb{R}^2 \setminus \mathcal{C})$ and the union of the trajectories γ_j for all $j \in \mathcal{L}$. If all trajectories with initial condition in $\tilde{\Phi} \setminus \tilde{\mathcal{O}}$ converge to the origin, that contradicts [17, Proposition 3], which shows that there cannot exist a continuous dynamical system, forward invariant in a set whose complement is compact, and with such set being the region of attraction of an asymptotically stable equilibrium. Note also that if $\tilde{\Phi} \setminus \tilde{\mathcal{O}}$ contains trajectories belonging to the regions of attraction of different asymptotically stable equilibria, by [121, Theorem 8.1], there exists a trajectory of (4.2) in the boundary of these regions of attraction. By definition, this trajectory does not belong to any region of attraction and by the Poincaré-Bendixson Theorem [123, Chapter 7, Thm. 4.1], this trajectory can only converge to a limit cycle. However,

$\tilde{\Phi}$ is forward invariant and $\tilde{\Phi} \cap \mathcal{C}$ does not contain any limit cycle, hence reaching a contradiction. □

4.4.2 Auxiliary results for Section 4.3

This section provides a number of supporting results for the technical treatment of Section 4.3. We start with an auxiliary result used in the proof of Proposition 4.3.1.

Lemma 4.4.4. (If a strict CBF exists, all CBFs are strict): *Let $\mathcal{C}$ be a compact set and assume h is a strict CBF of $\mathcal{C}$. Then any other CBF $\tilde{h}$ of $\mathcal{C}$ is also strict.*

Proof. By [120, Lemma 2.2], there exists a function $\zeta : \partial\mathcal{C} \to \mathbb{R}_{>0}$ such that $\nabla\tilde{h}(\mathbf{x}) = \zeta(\mathbf{x})\nabla h(\mathbf{x})$ for all $\mathbf{x}$ in $\mathcal{C}$. Since h is strict, for all $\mathbf{x} \in \partial\mathcal{C}$, there exist $\mathbf{u}_\mathbf{x} \in \mathbb{R}^m$ such that $\nabla h(\mathbf{x})^\top(f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}_\mathbf{x}) > 0$. This implies that $\nabla\tilde{h}(\mathbf{x})^\top(f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}_\mathbf{x}) = \zeta(\mathbf{x})\nabla h(\mathbf{x})^\top(f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}_\mathbf{x}) > 0$ for all $\mathbf{x} \in \partial\mathcal{C}$. Now, since $\nabla\tilde{h}$, f, and g are continuous, there exists a neighborhood $\mathcal{N}_\mathbf{x}$ of each $\mathbf{x} \in \partial\mathcal{C}$ such that $\nabla\tilde{h}(\mathbf{y})^\top(f(\mathbf{y}) + g(\mathbf{y})\mathbf{u}_\mathbf{x}) > 0$ for all $\mathbf{y} \in \mathcal{N}_\mathbf{x}$. Therefore, there exists a neighborhood $\mathcal{N}$ of $\partial\mathcal{C}$ where the CBF condition for $\tilde{h}$ is strictly feasible. Now, since $\mathcal{C}$ is compact, we can choose α as a linear function with a sufficiently large slope to ensure that $\nabla\tilde{h}(\mathbf{x})^\top(f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}_\mathbf{x}) + \alpha(\tilde{h}(\mathbf{x})) > 0$ holds for all $\mathbf{x} \in \mathcal{C}\backslash\mathcal{N}$ and hence for all $\mathbf{x} \in \mathcal{C}$, making $\tilde{h}$ a strict CBF. □

We next give a technical result used in the proof of Proposition 4.3.9. We use the same notation.

Lemma 4.4.5 (Conditions for β and γ)**.** *Let Assumption 2 hold. Furthermore, suppose that the conditions in Proposition 4.3.8 hold. Then, $r^2(\gamma^2 + \beta^2) - T_3^2 > 0$, and in particular $\gamma^2 + \beta^2 > 0$. Moreover, if Assumption 1 holds, then $\gamma x_{c,1} + \beta x_{c,2} \neq 0$.*

Proof. Let us show that $r^2(\gamma^2 + \beta^2) - T_3^2 > 0$, which implies that $\gamma^2 + \beta^2 > 0$. By noting that $|T_3| + \sqrt{T_2} > 0$, and squaring both sides of the condition $\frac{r}{\sqrt{b_1^2+b_2^2}} > \frac{|T_3|+\sqrt{T_2}}{2T_1}$ in Proposition 4.3.8, we get: $\left(\frac{2T_1 r}{\sqrt{b_1^2+b_2^2}} - |T_3|\right)^2 > T_2$, which is equivalent to

$\frac{4T_1^2r^2}{b_1^2+b_2^2} + T_3^2 - \frac{4T_1r|T_3|}{\sqrt{b_1^2+b_2^2}} > T_3^2 + 2\alpha_0 r^2 T_1$. Rearranging terms, this yields

$$|T_3| < \frac{(b_2\beta + b_1\gamma)r}{\sqrt{b_1^2+b_2^2}}. \tag{4.26}$$

Note that (4.26) requires $b_2\beta + b_1\gamma > 0$ since otherwise the conditions in (4.26) would not be feasible for any T_3. Now, by using condition (4.26) and applying the Cauchy-Schwartz inequality, we get $T_3 > -\sqrt{b_1^2+b_2^2}r$, $T_3 < \sqrt{b_1^2+b_2^2}r$, from which it follows that $r^2(\gamma^2+\beta^2) - T_3^2 > 0$. Finally suppose that $\|\mathbf{x}_c\|^2 > r^2$ and $\gamma x_{c,1} + \beta x_{c,2} = 0$. Note that $T_3^2 = (-\gamma x_{c,2} + \beta x_{c,1})^2 = (-\gamma x_{c,2} + \beta x_{c,1})^2 + (\gamma x_{c,1} + \beta x_{c,2})^2 = (\gamma^2+\beta^2)\|\mathbf{x}_c\|^2$. Since $\|\mathbf{x}_c\|^2 > r^2$, this implies that $r^2(\gamma^2+\beta^2) - T_3^2 < 0$, which is a contradiction. □

Next we add details to the Example 4.3.5. In particular, we elaborate further on the stability properties of undesired equilibria.

Example 4.4.6. (Example 4.3.5 continued): First, since the boundary of $\mathcal{C}$ is given by a union of semicircles, by following an argument similar to that of the proof of Proposition 4.3.8, one has that the following are sufficient conditions for h to be a strict CBF:

$$T_1 > 0,\ b_1^2 + b_2^2, \tag{4.27a}$$

$$\frac{r_1}{\sqrt{b_2^2+b_1^2}} > \frac{\frac{b_1}{|b_1|}(-\gamma c_2 - \beta c_1) + \sqrt{(\gamma c_2 + \beta c_1)^2 + 2\alpha_0 r_1^2 T_1}}{2T_1}, \tag{4.27b}$$

$$-\frac{r}{\sqrt{b_2^2+b_1^2}} > \frac{\frac{b_1}{|b_1|}(-\gamma c_2) - \sqrt{\gamma^2 c_2^2 + 2\alpha_0 r^2 T_1}}{2T_1}, \tag{4.27c}$$

$$\frac{r_1}{\sqrt{b_2^2+b_1^2}} > \frac{\frac{b_1}{|b_1|}(-\gamma c_2 + \beta c_1) + \sqrt{(-\gamma c_2 + \beta c_1)^2 + 2\alpha_0 r_1^2 T_1}}{2T_1}, \tag{4.27d}$$

$$-\frac{R}{\sqrt{b_2^2+b_1^2}} < \frac{\frac{b_1}{|b_1|}(-\gamma c_2) - \sqrt{\gamma^2 c_2^2 + 2\alpha_0 R^2 T_1}}{2T_1} \tag{4.27e}$$

where $\beta = a_{11}b_2 - b_1a_{21}$, $\gamma = a_{22}b_1 - b_2a_{12}$, and $T_1 := b_2\beta + b_1\gamma + \frac{1}{2}\alpha_0(b_2^2+b_1^2)$. Further, suppose that $r^2(\gamma^2+\beta^2) - \gamma^2c_2^2 \geq 0$, and let

$$z_{+,2} = \frac{\beta c_2 + \sqrt{r^2(\gamma^2+\beta^2) - \gamma^2 c_2^2}}{\gamma^2+\beta^2}.$$

It follows that the point $\mathbf{x}_{*,+,2} = (\gamma z_{+,2}, \beta z_{+,2})$ is in $\partial\mathcal{C}$ and satisfies (4.4) for some $\delta \in \mathbb{R}$; this, in turn, means that $\mathbf{x}_{*,+,2} \in \mathcal{E}$. To show whether $\mathbf{x}_{*,+,2}$ is an undesired equilibrium, we need to check if that $-(\mathbf{x}_{*,+,2} - \mathbf{x}_c)^\top (A - BK)\mathbf{x}_{*,+,2} < 0$. By using the expression of $\mathbf{x}_{*,+,2}$, this condition is equivalent to

$$z_{+,2} T_4 \big(b_1 \gamma z_{+,2} + b_2(\beta z_{+,2} - c_2)\big) > 0, \tag{4.28}$$

where $T_4 = a_{11}a_{22} - a_{12}a_{21} - k_1\gamma - k_2\beta$. Since $A - BK$ is Hurwitz, $T_4 > 0$, and therefore (4.28) is independent of K and equivalent to

$$z_{+,2} \Big(b_1 \gamma z_{+,2} + b_2(\beta z_{+,2} - c_2)\Big) > 0, \tag{4.29}$$

Now, note that Example 4.3.5 satisfies (4.29). Therefore, $\mathbf{x}_{*,+,2} = (3.157, 7.619)$ is an undesired equilibrium for any K. To show that it is asymptotically stable, note that Example 4.3.5 satisfies

$$(-\gamma c_2)(\gamma b_2 - \beta b_1) + (\gamma b_1 + \beta b_2)\sqrt{r^2(\gamma^2 + \beta^2) - \gamma^2 c_2^2} < 0. \tag{4.30}$$

Then, by following the same argument as in the proof of [6, Proposition 4], the Jacobian of (4.6) at $\mathbf{x}_{*,+,2}$ is

$$J(\mathbf{x}_{*,+,2}) = A - \frac{B}{(\mathbf{x}_c - \mathbf{x}_{*,+,2})^\top B}((\mathbf{x}_{*,+,2} - \mathbf{x}_c)^\top (A + \alpha_0 \mathbf{I}_n),$$

and (4.30) implies that J has two negative eigenvalues. Moreover, since J is independent of K, this implies that $\mathbf{x}_{*,+,2} = (3.157, 7.619)$ in Example 4.3.5 is asymptotically stable for any choice of linear stabilizing nominal controller. △

The following results concern Section 4.3.3, i.e., the case when the LTI system is fully actuated. We employ the same notation. We start by stating two auxiliary results that determine the eigenvalue other than $-\alpha'(0)$ of the Jacobian.

Lemma 4.4.7. (Eigenvalue of the Jacobian when $\tilde{A}$ is not diagonalizable): *Assume that $\lambda_1 = \lambda_2$ and $\tilde{A}$ is not diagonalizable. Then, there exists $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{R}^2$ such that $\|\mathbf{v}_1\|_2 = \|\mathbf{v}_2\|_2 = 1$, $\tilde{A}\mathbf{v}_1 = \lambda_1 \mathbf{v}_1$ and $\tilde{A}\mathbf{v}_2 = \lambda_2 \mathbf{v}_2 + \mathbf{v}_1$. For any $\mathbf{x}_* \in \hat{\mathcal{E}}$, if the associated indicator $\delta_{\mathbf{x}_*} \neq \frac{\lambda_1}{2}$, $\mathbf{x}_c = \beta_1 \mathbf{v}_1 + \beta_2 \mathbf{v}_2$ and $\mathbf{x}_* = \beta_3 \mathbf{v}_1 + \beta_4 \mathbf{v}_2$, then it holds*

that $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}} + \frac{2\delta_{\mathbf{x}_*}\beta_2}{(\lambda_1 - 2\delta_{\mathbf{x}_*})^2}$, $\beta_4 - \beta_2 = \frac{-\lambda_1\beta_2}{\lambda_1 - 2\delta_{\mathbf{x}_*}}$ *and the eigenvalue other than* $-\alpha'(0)$ *of the Jacobian of* (4.2) *at* $\mathbf{x}_*$ *is*

$$\lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_4 - \beta_2)}{r^2}((\beta_3 - \beta_1) + (\beta_4 - \beta_2)\mathbf{v}_2^\top \mathbf{v}_1).$$

Proof. Let $J(\mathbf{x})$ be the Jacobian of (4.2) evaluated at $\mathbf{x}$. If we write $J(\mathbf{x}_*)\mathbf{v}_1 = d_{11}\mathbf{v}_1 + d_{21}\mathbf{v}_2$ and $J(\mathbf{x}_*)\mathbf{v}_2 = d_{12}\mathbf{v}_1 + d_{22}\mathbf{v}_2$, then the other eigenvalue of $J(\mathbf{x}_*)$ is equal to $d_{11} + d_{22} + \alpha'(0)$.

Using the expression for the Jacobian in [120, Proposition 11],

$$\begin{aligned}
d_{11} = &-\frac{(\beta_3 - \beta_1)\alpha'(0)}{r^2}((\beta_3 - \beta_1) + (\beta_4 - \beta_2)\mathbf{v}_2^\top \mathbf{v}_1) + \\
&\lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_3 - \beta_1)(\lambda_1 - 2\delta_{\mathbf{x}_*})}{r^2}((\beta_3 - \beta_1) + (\beta_4 - \beta_2)\mathbf{v}_2^\top \mathbf{v}_1), \\
d_{22} = &-\frac{(\beta_4 - \beta_2)\alpha'(0)}{r^2}((\beta_3 - \beta_1)\mathbf{v}_1^\top \mathbf{v}_2 + (\beta_4 - \beta_2)) \\
&- \frac{(\beta_4 - \beta_2)(\lambda_1 - 2\delta_{\mathbf{x}_*})}{r^2}((\beta_3 - \beta_1)\mathbf{v}_1^\top \mathbf{v}_2 + (\beta_4 - \beta_2)) \\
&+ \lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_4 - \beta_2)}{r^2}((\beta_3 - \beta_1) + (\beta_4 - \beta_2)\mathbf{v}_2^\top \mathbf{v}_1)
\end{aligned}$$

Since $(\mathbf{x}_*, \delta_{\mathbf{x}_*})$ is an solution of (4.4), it follows that $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}} + \frac{2\delta_{\mathbf{x}_*}\beta_2}{(\lambda_1 - 2\delta_{\mathbf{x}_*})^2}$ and $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}$, by (4.4a); additionally, by (4.4b), one has that

$$\left\| \left(\frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}} + \frac{2\delta_{\mathbf{x}_*}\beta_2}{(\lambda_1 - 2\delta_{\mathbf{x}_*})^2} \right) \mathbf{v}_1 + \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}} \mathbf{v}_2 \right\|^2 - r^2 = 0.$$

Thus, it follows that:

$$d_{11} + d_{22} + \alpha'(0) = \lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_4 - \beta_2)}{r^2}((\beta_3 - \beta_1) + (\beta_4 - \beta_2)\mathbf{v}_2^\top \mathbf{v}_1).$$

□

Lemma 4.4.8. (The other eigenvalue of Jacobian when $\tilde{A}$ is diagonalizable): *Assume that* $\lambda_1 \neq \lambda_2$. *Then, there exists* $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{C}^2$ *such that* $\|\mathbf{v}_1\|_2 = \|\mathbf{v}_2\|_2 = 1$, $\tilde{A}\mathbf{v}_1 = \lambda_1\mathbf{v}_1$ *and* $\tilde{A}\mathbf{v}_2 = \lambda_2\mathbf{v}_2$. *Additionally, for any* $\mathbf{x}_* \in \hat{\mathcal{E}}$, *if the associated indicator* $\delta_{\mathbf{x}_*} \notin \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$, $\mathbf{x}_c = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2$ *and* $\mathbf{x}_* = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$, *it holds that* $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}}$, $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}$ *and the eigenvalues other than* $-\alpha'(0)$ *of the Jacobian of* (4.2) *at* $\mathbf{x}_*$ *is*

$$\lambda_1 + \lambda_2 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_3 - \beta_1)\lambda_1}{r^2}\Delta_1 - \frac{(\beta_4 - \beta_2)\lambda_2}{r^2}\Delta_2,$$

where $\Delta_1 := (\beta_3-\beta_1)^*+(\beta_4-\beta_2)^*\mathbf{v}_2^*\mathbf{v}_1$, $\Delta_2 := (\beta_3-\beta_1)^*\mathbf{v}_1^*\mathbf{v}_2+(\beta_4-\beta_2)^*$. *Equivalently, the eigenvalue other than* $\alpha'(0)$ *can be expressed as* $\lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_3-\beta_1)(\lambda_1-\lambda_2)}{r^2}\Delta_1$ *and* $\lambda_2 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_4-\beta_2)(\lambda_2-\lambda_1)}{r^2}\Delta_2$.

Proof. If we write $J(\mathbf{x}_*)\mathbf{v}_1 = d_{11}\mathbf{v}_1 + d_{21}\mathbf{v}_2$ and $J(\mathbf{x}_*)\mathbf{v}_2 = d_{12}\mathbf{v}_1 + d_{22}\mathbf{v}_2$, then the other eigenvalue of $J(\mathbf{x}_*)$ is equal to $d_{11} + d_{22} + \alpha'(0)$. Using the expression for the Jacobian in [120, Proposition 11],

$$\begin{aligned} d_{11} = \lambda_1 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_3 - \beta_1)\alpha'(0)}{r^2}((\beta_3 - \beta_1)^* + (\beta_4 - \beta_2)^*\mathbf{v}_2^*\mathbf{v}_1) \\ - \frac{(\beta_3 - \beta_1)(\lambda_1 - 2\delta_{\mathbf{x}_*})}{r^2}((\beta_3 - \beta_1)^* + (\beta_4 - \beta_2)^*\mathbf{v}_2^*\mathbf{v}_1), \end{aligned}$$

and

$$\begin{aligned} d_{22} = \lambda_2 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_4 - \beta_2)\alpha'(0)}{r^2}((\beta_3 - \beta_1)^*\mathbf{v}_1^*\mathbf{v}_2 + (\beta_4 - \beta_2)^*) \\ - \frac{(\beta_4 - \beta_2)(\lambda_2 - 2\delta_{\mathbf{x}_*})}{r^2}((\beta_3 - \beta_1)^*\mathbf{v}_1^*\mathbf{v}_2 + (\beta_4 - \beta_2)^*). \end{aligned}$$

Note that since $(\mathbf{x}_*, \delta_{\mathbf{x}_*})$ is a solution of (4.4), it follows that $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}}$, $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}$, and

$$\left\| \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}}\mathbf{v}_1 + \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}\mathbf{v}_2 \right\|^2 - r^2 = 0.$$

Then,

$$\begin{aligned} d_{11} + d_{22} + \alpha'(0) = \lambda_1 + \lambda_2 - 2\delta_{\mathbf{x}_*} - \frac{(\beta_3 - \beta_1)\lambda_1}{r^2}((\beta_3 - \beta_1)^* + (\beta_4 - \beta_2)^*\mathbf{v}_2^*\mathbf{v}_1) \\ - \frac{(\beta_4 - \beta_2)\lambda_2}{r^2}((\beta_3 - \beta_1)^*\mathbf{v}_1^*\mathbf{v}_2 + (\beta_4 - \beta_2)^*). \end{aligned}$$

By leveraging $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}}$ and $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}$, we get the two remaining expressions. □

To prove Proposition 4.3.11, we need to determine the Jacobian evaluated at the undesired equilibrium and analyze its spectrum. Applying [120, Proposition 6.2] and Lemma 4.2.1 to system (4.6), we have the following result.

Lemma 4.4.9. (The Jacobian evaluated at undesired equilibria): *Suppose Assumption 1 is satisfied, B is invertible, and $G = B^\top B$. The Jacobian of* (4.6) *at any undesired equilibrium $\mathbf{x}_*$ is*

$$J(\mathbf{x}_*) = \tilde{A} - 2\delta_{\mathbf{x}_*}\mathbf{I} - \frac{(\mathbf{x}_* - \mathbf{x}_c)(\mathbf{x}_* - \mathbf{x}_c)^\top}{\|\mathbf{x}_* - \mathbf{x}_c\|^2}(\tilde{A} - (2\delta_{\mathbf{x}_*} - \alpha'(0))\mathbf{I}).$$

Proof of Proposition 4.3.11:

Denote λ the eigenvalue associated with $\mathbf{x}_c$. Then $\lambda = \lambda_i$, $i = 1$ or 2; and both λ_1 and λ_2 are real. We first determine the solution for (4.4) with $\delta \notin \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$. Since $\delta \notin \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$, by the first equation in (4.4), it follows that $\mathbf{x}_* = \frac{2\delta}{2\delta - \lambda}\mathbf{x}_c$. Plugging this in the second equation in (4.4), we can solve for δ. This leads to the potential undesired equilibria $\mathbf{x}_{*,-} := (1 + \frac{r}{\|\mathbf{x}_c\|})\mathbf{x}_c)$, with associated value of δ equal to $\frac{\lambda}{2} + \frac{\lambda\|x_c\|}{2r}$, and $\mathbf{x}_{*,+} := (1 - \frac{r}{\|\mathbf{x}_c\|})\mathbf{x}_c)$, with associated value of δ equal to $\frac{\lambda}{2} - \frac{\lambda\|x_c\|}{2r}$. We note that the value of δ associated with $\mathbf{x}_{*,-}$ is negative and the value of δ associated with $\mathbf{x}_{*,-}$ is positive, so $\mathbf{x}_{*,-}$ is an undesired equilibrium while $\mathbf{x}_{*,+}$ is not an undesired equilibrium. By Lemma 4.4.9 , the Jacobian at $\mathbf{x}_{*,-}$ is

$$J(\mathbf{x}_{*,-}) = \tilde{A} - 2\delta\mathbf{I} - \frac{\mathbf{x}_c\mathbf{x}_c^\top}{\|\mathbf{x}_c\|^2}(\tilde{A} - (2\delta - \alpha'(0))\mathbf{I}).$$

where $\delta = \frac{\lambda_1}{2} + \frac{\lambda_1\|\mathbf{x}_c\|}{2r}$.

In the following, we determine if there exist solutions of (4.4) with $\delta \in \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$ and discuss the stability of the corresponding undesired equilibria case by case.

Case 1: $\tilde{A}$ is not diagonalizable.

In this case, we first show that $\mathbf{x}_{*,-}$ is always a saddle point. We note that we must have $\lambda_1 = \lambda_2$. Let $\mathbf{v}_1 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\mathbf{v}_2$ be a vector such that $\|\mathbf{v}_2\| = 1$, $\tilde{A}\mathbf{v}_2 = \lambda_1\mathbf{v}_2 + \mathbf{v}_1$. If we write $\mathbf{x}_c = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2$, then $\beta_1 = \|\mathbf{x}_c\|$ and $\beta_2 = 0$. By Lemma 4.4.7, it follows that the Jacobian at $\mathbf{x}_{*,-}$ has an eigenvalue equal to $\lambda_2 - 2\delta_{\mathbf{x}_{*,-}} = \lambda_1 - \lambda_1 - \frac{\lambda_1\|\mathbf{x}_c\|}{r} > 0$, implying that $\mathbf{x}_{*,-}$ is a saddle point.

Next, we determine if there exists a solution with $\delta = \frac{\lambda_1}{2}$. We write $\mathbf{x}_* = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$. Hence the first equation of (4.4) with $\delta = \frac{\lambda_1}{2}$ can be rewritten as $\beta_4 = -\lambda_1\|\mathbf{x}_c\|$. Plugging the value of β_4 into the second equation of (4.4), and defining $\hat{\beta}_3 := \beta_3 - \|\mathbf{x}_c\|$ and $\tau_1 := \lambda_1\|\mathbf{x}_c\|$, it follows that

$$\hat{\beta}_3^2 - 2\tau_1\mathbf{v}_1^\top\mathbf{v}_2\hat{\beta}_3 + \tau_1^2 - r^2 = 0. \tag{4.31}$$

Note that the discriminant of the quadratic equation (4.31) is

$$\Delta := 4\left(\tau_1^2(\mathbf{v}_1^\top \mathbf{v}_2)^2 - \tau_1^2 + r^2\right) = 4\left(\tau_1^2((\mathbf{v}_1^\top \mathbf{v}_2)^2 - 1) + r^2\right)$$

This leads to the following three subcases.

Case 1.1 if $(\mathbf{v}_1^\top \mathbf{v}_2)^2 < 1 - r^2/\tau_1^2 = 1 - \frac{r^2}{\lambda_1^2 \|\mathbf{x}_c\|^2}$, there does not exist a solution associated with $\delta = \frac{\lambda_1}{2}$.

Case 1.2 if $(\mathbf{v}_1^\top \mathbf{v}_2)^2 = 1 - r^2/\tau_1^2 = 1 - \frac{r^2}{\lambda_1^2 \|\mathbf{x}_c\|^2}$, then there exists one solution $\mathbf{x}_{*,1} = (\tau_1 \mathbf{v}_1^\top \mathbf{v}_2 + \|\mathbf{x}_c\|)\mathbf{v}_1 - \tau_1 \mathbf{v}_2$ with $\delta_{\mathbf{x}_{*,1}} = \frac{\lambda_1}{2}$, equal to

$$\mathbf{x}_{*,1} = (\tau_1 \mathbf{v}_1^\top \mathbf{v}_2 + \|\mathbf{x}_c\|)\mathbf{v}_1 - \tau_1 \mathbf{v}_2$$

Since $(\mathbf{x}_{*,1} - \mathbf{x}_c)^\top \mathbf{v}_1 = 0$ and $(\tilde{A} - 2\delta_{\mathbf{x}_{*,1}}\mathbf{I})\mathbf{v}_1 = 0$, it follows that $J(\mathbf{x}_{*,1})^\top \mathbf{v}_1 = 0$, by Lemma 4.4.9. Therefore in this case, there is another undesired equilibrium $\mathbf{x}_{*,1}$, at which the Jacobian has a negative eigenvalue and a zero eigenvalue.

Case 1.3 if $(\mathbf{v}_1^\top \mathbf{v}_2)^2 > 1 - r^2/\tau_1^2 = 1 - \frac{r^2}{\lambda_1^2 \|\mathbf{x}_c\|^2}$, there exist two solutions $\hat{\beta}_3 = \hat{\beta}_3^{(1)}$ and $\hat{\beta}_3 = \hat{\beta}_3^{(2)}$ for (4.31). This implies that there exist two extra undesired equilibria given by $\mathbf{x}_{*,2} = (\hat{\beta}_3^{(1)} + \|\mathbf{x}_c\|)\mathbf{v}_1 - \tau_1 \mathbf{v}_2$ and $\mathbf{x}_{*,3} = (\hat{\beta}_3^{(2)} + \|\mathbf{x}_c\|)\mathbf{v}_1 - \tau_1 \mathbf{v}_2$.

Notice that in this sub-case, $\hat{\beta}_3^{(1)} + \hat{\beta}_3^{(2)} = 2\tau_1 \mathbf{v}_1^\top \mathbf{v}_2$, we can assume that $\hat{\beta}_3^{(1)} < \tau_1 \mathbf{v}_1^\top \mathbf{v}_2$ and $\hat{\beta}_3^{(1)} > \tau_1 \mathbf{v}_1^\top \mathbf{v}_2$.

Using the same technique in the proof of Lemma 4.4.8, we can show that $J(\mathbf{x}_{*,2})$, has an eigenvalue $\frac{\tau_1}{r^2}(\hat{\beta}_3^{(1)} - \tau_1 \mathbf{v}_1^\top \mathbf{v}_2) > 0$; and $J(\mathbf{x}_{*,3})$ has an eigenvalue $\frac{\tau_1}{r^2}(\hat{\beta}_3^{(2)} - \tau_1 \mathbf{v}_1^\top \mathbf{v}_2) < 0$.

Hence in this case, there are another two undesired equilibria, one of which is stable and the other one is saddle point.

Case 2: $\tilde{A}$ is diagonalizable and $\lambda_1 \le \lambda_2 < 0$, $\tilde{A}\mathbf{x}_c = \lambda_1 \mathbf{x}_c$

In this case, we first show that $\mathbf{x}_{*,-}$ is always a saddle point. Let $\mathbf{v}_1 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\mathbf{v}_2$ be an eigenvector associated with λ_2 satisfying $\|\mathbf{v}_2\| = 1$, $\mathbf{v}_1^\top \mathbf{v}_2 \ge 0$. If we write $\mathbf{x}_c = \beta_1 \mathbf{v}_1 + \beta_2 \mathbf{v}_2$, then $\beta_1 = \|\mathbf{x}_c\|$ and $\beta_2 = 0$. By Lemma 4.4.8, it follows that the Jacobian at $\mathbf{x}_{*,-}$ has an eigenvalue equal to $\lambda_2 - \lambda_1 - \frac{\lambda_1 \|\mathbf{x}_c\|}{r} > 0$, implying that $\mathbf{x}_{*,-}$ is a saddle point. Next, we determine if there exists a solution with $\delta \in \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$. We write $\mathbf{x}_* = \beta_3 \mathbf{v}_1 + \beta_4 \mathbf{v}_2$ and then the first equation of (4.4) can be rewritten as

$$\begin{aligned} (\lambda_1 - 2\delta)(\beta_3 - \|\mathbf{x}_c\|) &= -\lambda_1 \|\mathbf{x}_c\| \\ (\lambda_2 - 2\delta)\beta_4 &= 0 \end{aligned} \tag{4.32}$$

from which it follows that $\delta \neq \frac{\lambda_1}{2}$.

If $\delta = \frac{\lambda_2}{2}$, from the first equation of (4.32) it follows that $\beta_3 = \frac{-\lambda_2\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}$. Plugging the value of β_3 into the equation $h(\mathbf{x}) = 0$ from (4.4), and by defining $\tau_2 := \frac{\lambda_1\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}$, it follows that

$$\beta_4^2 - 2\tau_2\mathbf{v}_1^\top\mathbf{v}_2\beta_4 + \tau_2^2 - r^2 = 0. \tag{4.33}$$

Note that the discriminant of quadratic equation (4.33) is

$$\Delta := 4\left(\tau_2^2(\mathbf{v}_1^\top\mathbf{v}_2)^2 - \tau_2^2 + r^2\right) = 4\left(\tau_2^2((\mathbf{v}_1^\top\mathbf{v}_2)^2 - 1) + r^2\right),$$

which leads to the following three subcases.

Case 2.1 if $(\mathbf{v}_1^\top\mathbf{v}_2)^2 < 1 - r^2/\tau_2^2 = 1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_1^2\|\mathbf{x}_c\|^2}$, there does not exist a solution associated with $\delta = \frac{\lambda_2}{2}$.

Case 2.2 if $(\mathbf{v}_1^\top\mathbf{v}_2)^2 = 1 - r^2/\tau_2^2 = 1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_1^2\|\mathbf{x}_c\|^2}$, then there exists an undesired equilibrium

$$\mathbf{x}_{*,4} = \frac{-\lambda_2\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}\mathbf{v}_1 + \frac{\lambda_1\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}\mathbf{v}_1^\top\mathbf{v}_2\mathbf{v}_2$$

with corresponding δ equal to $\frac{\lambda_2}{2}$. We note that $(\mathbf{x}_{*,4} - \mathbf{x}_c)^\top\mathbf{v}_2 = 0$ and $(\tilde{A} - 2\delta_{\mathbf{x}_{*,4}}\mathbf{I})\mathbf{v}_2 = 0$. Hence, by Lemma 4.4.9, we have $J(\mathbf{x}_{*,4})\mathbf{v}_2 = 0$. Thus in this case, the Jacobian evaluated at $\mathbf{x}_{*,4}$ has a negative eigenvalue and a zero eigenvalue.

Case 2.3 if $(\mathbf{v}_1^\top\mathbf{v}_2)^2 > 1 - r^2/\tau_2^2 = 1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_1^2\|\mathbf{x}_c\|^2}$, there exist two solutions $\beta_4 = \beta_4^{(1)}$ and $\beta_4 = \beta_4^{(2)}$ for (4.31). Then there exist two undesired equilibria $\mathbf{x}_{*,5} = \frac{-\lambda_2\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}\mathbf{v}_1 + \beta_4^{(1)}\mathbf{v}_2$ and $\mathbf{x}_{*,6} = \frac{-\lambda_2\|\mathbf{x}_c\|}{\lambda_1-\lambda_2}\mathbf{v}_1 + \beta_4^{(2)}\mathbf{v}_2$ with associated value of δ equal to $\frac{\lambda_2}{2}$. Notice that in this sub-case, $\beta_4^{(1)} + \beta_4^{(2)} = 2\tau_2\mathbf{v}_1^\top\mathbf{v}_2 > 0$ and $\beta_4^{(1)}\beta_4^{(2)} = \tau_2^2 - r^2 > 0$, we can assume that $0 < \beta_4^{(1)} < \tau_2\mathbf{v}_1^\top\mathbf{v}_2$ and $\beta_4^{(2)} > \tau_2\mathbf{v}_1^\top\mathbf{v}_2$. It follows that $-\tau_2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(1)} + \tau_2^2 - r^2 = -\beta_4^{(1)}\beta_4^{(1)} + \tau_2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(1)} > 0$ and $-\tau_2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(2)} + \tau_2^2 - r^2 = -\beta_4^{(2)}\beta_4^{(2)} + \tau_2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(2)} < 0$. Using the same technique in the proof of Lemma 4.4.7, we can show that $J(\mathbf{x}_{*,4})$ has an eigenvalue $\frac{\lambda_2-\lambda_1}{r^2}(\tau_2^2 - \tau_2^2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(1)} - r^2) > 0$, and $J(\mathbf{x}_{*,5})$ has an eigenvalue $\frac{\lambda_2-\lambda_1}{r^2}(\tau_2^2 - \tau_2^2\mathbf{v}_1^\top\mathbf{v}_2\beta_4^{(2)} - r^2) < 0$. Hence in this case, there are two extra undesired equilibria, one of which is stable and the other one is a saddle point.

Case 3: $\tilde{A}$ diagonalizable, $\lambda_1 < \lambda_2 < 0$, $\tilde{A}\mathbf{x}_c = \lambda_2\mathbf{x}_c$.

Let $\mathbf{v}_2 = \frac{\mathbf{x}_c}{\|\mathbf{x}_c\|}$, $\mathbf{v}_1$ be an eigenvector associated with λ_1 and $\|\mathbf{v}_1\| = 1$, $\mathbf{v}_1^\top\mathbf{v}_2 \geq 0$. If we write $\mathbf{x}_c = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2$, then $\beta_2 = \|\mathbf{x}_c\|$ and $\beta_1 = 0$. By Lemma 4.4.8, it follows

that the Jacobian at $\mathbf{x}_{*,-}$ has an eigenvalue equal to $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r}$. We determine the sign of $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r}$ later. First, let us determine if there exists a solution with $\delta \in \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$. We write $\mathbf{x}_c = \|\mathbf{x}_c\|\mathbf{v}_2$, $\mathbf{x} = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$ and then from (4.4) it follows that

$$\begin{aligned}(\lambda_1 - 2\delta)\beta_3 &= 0\\ (\lambda_2 - 2\delta)(\beta_4 - \|\mathbf{x}_c\|) &= -\lambda_2\|\mathbf{x}_c\|,\end{aligned} \tag{4.34}$$

from which it follows that $\delta \neq \frac{\lambda_2}{2}$. If $\delta = \frac{\lambda_1}{2}$, it follows from (4.34) that $\beta_4 = \frac{-\lambda_1\|\mathbf{x}_c\|}{\lambda_2-\lambda_1}$. Plugging the value of β_4 into the equation $h(\mathbf{x}) = 0$ from (4.4), and by letting $\tau_3 := \frac{\lambda_2\|\mathbf{x}_c\|}{\lambda_2-\lambda_1}$, it follows that

$$\beta_3^2 - 2\tau_3\mathbf{v}_1^\top\mathbf{v}_2\beta_3 + \tau_3^2 - r^2 = 0. \tag{4.35}$$

Note that the discriminant of quadratic equation (4.35) is

$$\Delta := 4\left(\tau_3^2(\mathbf{v}_1^\top\mathbf{v}_2)^2 - \tau_3^2 + r^2\right) = 4\left(\tau_3^2((\mathbf{v}_1^\top\mathbf{v}_2)^2 - 1) + r^2\right),$$

which leads to the following three subcases.

Case 3.1 if $(\mathbf{v}_1^\top\mathbf{v}_2)^2 < 1 - r^2/\tau_3^2 = 1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_2^2\|\mathbf{x}_c\|^2}$, there does not exist a solution associated with $\delta = \frac{\lambda_1}{2}$. Recall also that the eigenvalue (other than $-\alpha'(0)$) of Jacobian at $\mathbf{x}_{*,-}$ is $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r}$. In this subcase, we have $1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_2^2\|\mathbf{x}_c\|^2} > (\mathbf{v}_1^\top\mathbf{v}_2)^2 \geq 0$, which implies that $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r} > 0$. Hence in this case, we only have one undesired equilibrium $\mathbf{x}_{*,-}$, which is a saddle point.

Case 3.2 if $(\mathbf{v}_1^\top\mathbf{v}_2)^2 = 1 - r^2/\tau_3^2 = 1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_2^2\|\mathbf{x}_c\|^2} \neq 0$, there exists an undesired equilibrium equal to

$$\mathbf{x}_{*,7} = \frac{\lambda_2\|\mathbf{x}_c\|}{\lambda_2 - \lambda_1}\mathbf{v}_1^\top\mathbf{v}_2\mathbf{v}_1 - \frac{\lambda_1\|\mathbf{x}_c\|}{\lambda_2 - \lambda_1}\mathbf{v}_2,$$

with associated δ equal to $\delta = \frac{\lambda_1}{2}$. We note that $(\mathbf{x}_{*,7} - \mathbf{x}_c)^\top\mathbf{v}_1 = 0$ and $(\tilde{A} - 2\delta_{\mathbf{x}_{*,7}}\mathbf{I})\mathbf{v}_2 = 0$. Hence, by Lemma 4.4.9, we get that $J(\mathbf{x}_{*,7})\mathbf{v}_1 = 0$. Therefore, $\mathbf{x}_{*,7}$ is an undersirable equilibrium and a degenerate equilibrium. Recall that the eigenvalue (other than $-\alpha'(0)$) of the Jacobian at $\mathbf{x}_{*,-}$ is $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r}$. In this subcase, we still have $1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_2^2\|\mathbf{x}_c\|^2} = (\mathbf{v}_1^\top\mathbf{v}_2)^2 > 0$, which implies that $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r} > 0$. Hence in this subcase, there are two undesired equilibria $\mathbf{x}_{*,-}$ and $\mathbf{x}_{*,7}$, where $\mathbf{x}_{*,-}$ is an saddle point and $\mathbf{x}_{*,7}$ is a degenerate equilibrium.

Case 3.3 if $(\mathbf{v}_1^\top \mathbf{v}_2)^2 = 1 - r^2/\tau_3^2 = 1 - \frac{(\lambda_1-\lambda_2)^2 r^2}{\lambda_2^2 \|\mathbf{x}_c\|^2} = 0$, there exists one solution associated with $\delta = \frac{\lambda_1}{2}$, which is

$$\mathbf{x}_{*,8} = -\frac{\lambda_1 \|\mathbf{x}_c\|}{\lambda_2 - \lambda_1}\mathbf{v}_2.$$

Notice that $1 - \frac{(\lambda_1-\lambda_2)^2 r^2}{\lambda_2^2 \|\mathbf{x}_c\|^2} = 0$ implies that $\frac{-\lambda_2}{\lambda_2-\lambda_1} = \frac{r}{\|\mathbf{x}_c\|}$, from which it follows that

$$\mathbf{x}_{*,8} = -\frac{\lambda_1 \|\mathbf{x}_c\|}{\lambda_2 - \lambda_1}\mathbf{v}_2 = (1 - \frac{\lambda_2}{\lambda_2 - \lambda_1})\mathbf{x}_c = (1 + \frac{r}{\|\mathbf{x}_c\|})\mathbf{x}_c = \mathbf{x}_{*,-},$$

and $\lambda_1 - \lambda_2 - \frac{\lambda_2 \|\mathbf{x}_c\|}{r} = 0$. Thus in this case, there is only one undesired equilibrium $\mathbf{x}_{*,-}$, which is a degenerate equilibrium.

Case 3.4 if $(\mathbf{v}_1^\top \mathbf{v}_2)^2 > 1 - r^2/\tau_3^2 = 1 - \frac{(\lambda_1-\lambda_2)^2 r^2}{\lambda_2^2 \|\mathbf{x}_c\|^2}$, there exist two solutions $\beta_3 = \beta_3^{(1)}$ and $\beta_3 = \beta_3^{(2)}$ for (4.35). Then there exist two extra undesired equilibria: $\mathbf{x}_{*,9} = \beta_3^{(1)}\mathbf{v}_1 - \frac{\lambda_1 \|\mathbf{x}_c\|}{\lambda_2-\lambda_1}\mathbf{v}_2$ and $\mathbf{x}_{*,10} = \beta_3^{(2)}\mathbf{v}_1 - \frac{\lambda_1 \|\mathbf{x}_c\|}{\lambda_2-\lambda_1}\mathbf{v}_2$. Notice that in this sub-case, we have $\beta_3^{(1)} + \beta_3^{(2)} = 2\tau_3 \mathbf{v}_1^\top \mathbf{v}_2 < 0$. Then we can assume that $\beta_3^{(1)} < \tau_3 \mathbf{v}_1^\top \mathbf{v}_2$ and $\beta_3^{(2)} > \tau_2 \mathbf{v}_1^\top \mathbf{v}_2$. Using the same technique in the proof of Lemma 4.4.7, we can show that the $J(\mathbf{x}_{*,9})$ has an eigenvalue

$$\frac{\lambda_1 - \lambda_2}{r^2}(\tau_3^2 - \tau_3 \mathbf{v}_1^\top \mathbf{v}_2 \beta_3^{(1)} - r^2);$$

and $J(\mathbf{x}_{*,10})$ has an eigenvalue

$$\frac{\lambda_1 - \lambda_2}{r^2}(\tau_3^2 - \tau_3 \mathbf{v}_1^\top \mathbf{v}_2 \beta_3^{(2)} - r^2).$$

Recall that the Jacobian evaluated at $\mathbf{x}_{*,-}$ has an eigenvalue $\lambda_1 - \lambda_2 - \frac{\lambda_2 \|\mathbf{x}_c\|}{r}$, and then we only need to determine the sign of these three eigenvalues case by case.

Case 3.4.1 If $0 < \tau_3^2 - r^2 = \frac{\lambda_2^2 \|\mathbf{x}_c\|^2}{(\lambda_2-\lambda_1)^2} - r^2$, it is easy to check that $\lambda_1 - \lambda_2 - \frac{\lambda_2 \|\mathbf{x}_c\|}{r} > 0$. In addition, similar to **Case 3.3**, we can show that $\{\frac{\lambda_1-\lambda_2}{r^2}(\tau_3^2 - \tau_3 \mathbf{v}_1^\top \mathbf{v}_2 \beta_3^{(i)} - r^2) : \ i = 1, 2\}$ contains one positive number and one negative number. Thus in this case, there are three undesired equilibria in total, two of which are saddle points and one of which is asymptotically stable.

Case 3.4.2 If $0 = \tau_3^2 - r^2 = \frac{\lambda_2^2 \|\mathbf{x}_c\|^2}{(\lambda_2-\lambda_1)^2} - r^2$, it follows that $\lambda_1 - \lambda_2 - \frac{\lambda_2 \|\mathbf{x}_c\|}{r} = 0$. In addition, we have $\beta_3^{(2)} = 0$ and the point $\mathbf{x}_{*,10} = \beta_3^{(2)}\mathbf{v}_1 - \frac{\lambda_1 \|\mathbf{x}_c\|}{\lambda_2-\lambda_1}\mathbf{v}_2$ is equal to $\mathbf{x}_{*,-}$.

The point $\mathbf{x}_{*,9} = \beta_3^{(1)}\mathbf{v}_1 - \frac{\lambda_1\|\mathbf{x}_c\|}{\lambda_2-\lambda_1}\mathbf{v}_2$ is a saddle point since the eigenvalue

$$\begin{aligned}&\frac{\lambda_1-\lambda_2}{r^2}(\tau_3^2 - \tau_3\mathbf{v}_1^\top\mathbf{v}_2\beta_3^{(1)} - r^2) = 2\frac{\lambda_2-\lambda_1}{r^2}\tau_3^2(\mathbf{v}_1^\top\mathbf{v}_2)^2\\ &> 2\frac{\lambda_2-\lambda_1}{r^2}\tau_3^2\left(1 - \frac{(\lambda_1-\lambda_2)^2r^2}{\lambda_2^2\|\mathbf{x}_c\|^2}\right) > 0.\end{aligned}$$

Thus in this case, there are two undesired equilibria $\mathbf{x}_{*,-}$ and $\mathbf{x}_{*,9}$, where $\mathbf{x}_{*,-}$ is a degenerate equilibrium and $\mathbf{x}_{*,9}$ is an saddle point .

Case 3.4.3 If $0 > \tau_3^2 - r^2 = \frac{\lambda_2^2\|\mathbf{x}_c\|^2}{(\lambda_2-\lambda_1)^2} - r^2$, it is easy to check that $\lambda_1 - \lambda_2 - \frac{\lambda_2\|\mathbf{x}_c\|}{r} < 0$, which implies that $\mathbf{x}_{*,-}$ is asymptotically stable. By $\beta_3^{(1)}\beta_3^{(2)} = \tau_3^2 - r^2 < 0$ and $\beta_3^{(1)} < \tau_3\mathbf{v}_1^\top\mathbf{v}_2 < 0$, it follows that $\beta_3^{(2)} > 0$. Using the fact that $\beta_3^{(1)} < \tau_3\mathbf{v}_1^\top\mathbf{v}_2 < 0$, we can show that

$$\frac{\lambda_1-\lambda_2}{r^2}(\tau_3^2 - \tau_3\mathbf{v}_1^\top\mathbf{v}_2\beta_3^{(1)} - r^2) > 0.$$

On the other hand, using the fact that $\beta_3^{(1)} > 0 > \tau_3\mathbf{v}_1^\top\mathbf{v}_2$, we can show that

$$\frac{\lambda_1-\lambda_2}{r^2}(\tau_3^2 - \tau_3\mathbf{v}_1^\top\mathbf{v}_2\beta_3^{(2)} - r^2) > 0.$$

Thus in this case, there are three undesired equilibria in total, two of which are saddle points and one of which is asymptotically stable.

Table 4.1 summarizes the cases discussed in the proof, except for **Case 3.3** and **Case 3.4.2**. □

Proof of Proposition 4.3.13

Denote the eigenvalues of $\tilde{A}$ as λ_1, $\lambda_2 \in \mathbb{C}$. We note that the conditions in (4.4) can be rewritten as follows:

$$\begin{aligned}&(\tilde{A} - 2\delta\mathbf{I}_{2\times2})(\mathbf{x}-\mathbf{x}_c) = -\tilde{A}\mathbf{x}_c \text{ and,}\\ &\|\mathbf{x}-\mathbf{x}_c\|^2 - r^2 = 0\,.\end{aligned} \tag{4.36}$$

Next, we consider two cases.

• *Case #1* ($\tilde{A}$ is diagonalizable): Recall that $\mathbf{x}_c$ is not an eigenvector, so it holds that $\lambda_1 \neq \lambda_2$. Let $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{C}^2$ be eigenvectors such that $\tilde{A}\mathbf{v}_1 = \lambda_1\mathbf{v}_1$, $\tilde{A}\mathbf{v}_2 = \lambda_2\mathbf{v}_2$, $\|\mathbf{v}_1\| = \|\mathbf{v}_2\| = 1$. Write $\mathbf{x}_c$ as $\mathbf{x}_c = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2$ and $\mathbf{x} = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$. Hence, the first equation in (4.36) can be rewritten as:

$$\begin{aligned}(\lambda_1 - 2\delta)(\beta_3 - \beta_1) &= -\lambda_1\beta_1\\ (\lambda_2 - 2\delta)(\beta_4 - \beta_2) &= -\lambda_2\beta_2\,.\end{aligned} \tag{4.37}$$

Note that $\beta_1 \neq 0$ and $\beta_2 \neq 0$ as $\mathbf{x}_c$ is not an eigenvector of $A - BK$; it follows that there is no solution with $\delta \in \{\frac{\lambda_1}{2}, \frac{\lambda_2}{2}\}$. For any solution $(\mathbf{x}, \delta_{\mathbf{x}})$ of (4.36), we have that $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}}}$, $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}}}$ and $\left\| \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}}}\mathbf{v}_1 + \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}}}\mathbf{v}_2 \right\|^2 - r^2 = 0$, which is equivalent to $F_1(\delta) = 0$, where $F_1(\delta)$ is defined in (4.25).

We first note that $F_1(\delta) = 0$ can have at most 4 solutions. Therefore, there are at most four solutions for (4.36). In addition, notice that $F_1(-\infty) < 0$, $F_1(+\infty) < 0$ and $F_1(0) = (\|\mathbf{x}_c\|^2 - r^2)\|\lambda_1\lambda_2\|^2 > 0$, it follows that there exists at least one solution of (4.36) with positive δ and at least one solution with negative δ. If $\lambda_1 \leq \lambda_2$, we have $F_1(-\infty) < 0$, and $F_1(\frac{\lambda_1}{2}) > 0$ and there exists at least one solution for (4.36) with $\delta < \frac{\lambda_1}{2}$.

- *Case* #2 ($\tilde{A}$ is not diagonalizable): In this case, we have $\lambda_1 = \lambda_2$. Note that both eigenvalues are negative and $\mathbf{x}_c$ is not an eigenvector of $\tilde{A}$. Let $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbb{R}^2$ be vectors of length 1, such that $\tilde{A}\mathbf{v}_1 = \lambda_1\mathbf{v}_1$, $\tilde{A}\mathbf{v}_2 = \lambda_1\mathbf{v}_2 + \mathbf{v}_1$. We write $\mathbf{x}_c = \beta_1\mathbf{v}_1 + \beta_2\mathbf{v}_2$ and $\mathbf{x}_* = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$. Hence, the first equation in (4.36) can be rewritten as

$$\begin{aligned} (\lambda_1 - 2\delta)(\beta_3 - \beta_1) + (\beta_4 - \beta_2) &= -\lambda_1\beta_1 - \beta_2 \\ (\lambda_2 - 2\delta)(\beta_4 - \beta_2) &= -\lambda_2\beta_2\,. \end{aligned} \tag{4.38}$$

Note that $\beta_2 \neq 0$ as $\mathbf{x}_c$ is not an eigenvector of $\tilde{A}$; it follows that there is no solution with $2\delta = \lambda_1$. For any solution $(\mathbf{x}_*, \delta_{\mathbf{x}_*})$ of equation (4.36), we have $\beta_3 - \beta_1 = \frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}} + \frac{2\delta_{\mathbf{x}_*}\beta_2}{(\lambda_1 - 2\delta_{\mathbf{x}_*})^2}$, $\beta_4 - \beta_2 = \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}$ and $\left\| \left(\frac{-\lambda_1\beta_1}{\lambda_1 - 2\delta_{\mathbf{x}_*}} + \frac{2\delta_{\mathbf{x}}\beta_2}{(\lambda_1 - 2\delta_{\mathbf{x}_*})^2} \right)\mathbf{v}_1 + \frac{-\lambda_2\beta_2}{\lambda_2 - 2\delta_{\mathbf{x}_*}}\mathbf{v}_2 \right\|^2 - r^2 = 0$, which is equivalent to $F_2(\delta_{\mathbf{x}_*}) = 0$, where F_2 is defined as

$$\begin{aligned} F_2(\delta) &:= -(\lambda_1 - 2\delta)^4 r^2 + (\lambda_1\beta_2)^2(\lambda_1 - 2\delta)^2 \\ &+ 2(\lambda_1\beta_1(\lambda_1 - 2\delta)^2 - 2\delta(\lambda_1 - 2\delta)\beta_2)\lambda_1\beta_2\mathbf{v}_1^\top\mathbf{v}_2 \\ &+ (2\delta\beta_2 - \lambda_1(\lambda_1 - 2\delta)\beta_1)^2. \end{aligned}$$

We first note that $F_2(\delta) = 0$ can have at most 4 solutions. Therefore, there are four solutions at most for (4.36). In addition, notice that $F_2(+\infty) < 0$ and $F_2(0) = (\|\mathbf{x}_c\|^2 - r^2)\lambda_1^4 > 0$; it follows that there exists at least a solution for (4.36) with positive δ. Similarly, we have that $\frac{1}{(\lambda_1 - 2\delta)^4}F_2(\delta) < 0$ as $\delta \to -\infty$, and $\frac{1}{(\lambda_1 - 2\delta)^4}F_2(\delta) \to +\infty$ as $\delta \to \frac{\lambda_1}{2}^-$; then. there exists at least one solution for (4.36) with negative $\delta < \frac{\lambda_1}{2}$. □

Proof of Proposition 4.3.14

Let $\mathbf{x}_* \in \hat{\mathcal{E}}$ with indicator $\delta_{\mathbf{x}_*} < \frac{\lambda_1}{2}$, and write $\mathbf{x}_* = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$; then, it follows by Lemma 4.4.8 that the Jacobian evaluated at $\mathbf{x}_*$ has an eigenvalue greater than $\frac{(\lambda_2-\lambda_1)}{r^2}\frac{-\lambda_1}{\lambda_1-2\delta_{\mathbf{x}_*}}((\beta_3-\beta_1)\beta_1 + (\beta_4-\beta_2)\beta_1\mathbf{v}_2^\top\mathbf{v}_1)$. Notice that $\frac{(\lambda_2-\lambda_1)}{r^2}\frac{-\lambda_1}{\lambda_1-2\delta_{\mathbf{x}_*}} > 0$ and

$$\begin{aligned}(\beta_3-\beta_1)\beta_1 + (\beta_4-\beta_2)\beta_1\mathbf{v}_2^\top\mathbf{v}_1 &= \frac{-\lambda_1}{\lambda_1-2\delta_{\mathbf{x}_*}}\beta_1^2 + \frac{-\lambda_2}{\lambda_2-2\delta_{\mathbf{x}_*}}\beta_1\beta_2\mathbf{v}_2^\top\mathbf{v}_1 \\ &\geq \frac{-\lambda_2}{\lambda_2-2\delta_{\mathbf{x}_*}}(\beta_1^2 + \beta_1\beta_2\mathbf{v}_2^\top\mathbf{v}_1) \geq 0\,.\end{aligned}$$

Hence, the Jacobian evaluated at $\mathbf{x}_*$ has a positive eigenvalue and, thus, $\mathbf{x}_*$ is a saddle point. On the other hand, for any $\mathbf{x}_* \in \hat{\mathcal{E}}$ with indicator $\frac{\lambda_2}{2} < \delta_{\mathbf{x}_*} < 0$, write $\mathbf{x}_* = \beta_3\mathbf{v}_1 + \beta_4\mathbf{v}_2$; then, by Lemma 4.4.7, it follows that the Jacobian evaluated at $\mathbf{x}_*$ has an eigenvalue less than $\frac{(\lambda_2-\lambda_1)}{r^2}\frac{2\lambda_2}{\lambda_2-2\delta_{\mathbf{x}_*}}((\beta_3-\beta_1)\beta_2\mathbf{v}_1^\top\mathbf{v}_2 + (\beta_4-\beta_2)\beta_2)$. Notice that $\frac{(\lambda_2-\lambda_1)}{r^2}\frac{2\lambda_2}{\lambda_1-2\delta_{\mathbf{x}_*}} > 0$ and

$$\begin{aligned}(\beta_3-\beta_1)\beta_2\mathbf{v}_2^\top\mathbf{v}_1 + (\beta_4-\beta_2)\beta_2 &= \frac{-\lambda_1}{\lambda_1-2\delta_{\mathbf{x}_*}}\beta_1\beta_2\mathbf{v}_2^\top\mathbf{v}_1 + \frac{-\lambda_2}{\lambda_2-2\delta_{\mathbf{x}_*}}\beta_2^2 \\ &\leq \frac{-\lambda_1}{\lambda_1-2\delta_{\mathbf{x}_*}}(\beta_1\beta_2\mathbf{v}_2^\top\mathbf{v}_1 + \beta_2^2) \leq 0.\end{aligned}$$

Besides, by [120, Proposition 10], $-\alpha'(0)$ is another eigenvalue. Hence, all the eigenvalues of the Jacobian evaluated at $\mathbf{x}_*$ are negative, which means that $\mathbf{x}_*$ is an undesired asymptotically stable equilibrium.

To prove the last claim, let δ_0 denote the only real root of the third-order polynomial $\frac{dF_1(\delta)}{d\delta}$. It follows that $F_1(\delta)$ is monotonically increasing on $(-\infty, \delta_0)$ and monotonically decreasing on $(\delta_0, +\infty)$; this implies that $F_1(\delta) = 0$ only has two solutions. By Lemma 4.4.7, there is only one undesired equilibrium and its indicator satisfies $\delta < \frac{\lambda_1}{2}$. Since $\beta_1^2 + \beta_1\beta_2\mathbf{v}_1^\top\mathbf{v}_2 \geq 0$, there is only one undesired equilibrium and it is a saddle point. □

Remark 4.4.10. (Connection between the eigenvector-eigenvalue structure): Propositions 4.3.11 and 4.3.14 describe the number and stability properties of undesired equilibria based on the specific eigenvector-eigenvalue structure. Proposition 4.3.11 (cf. Table 4.1) consists of the cases where $\mathbf{x}_c$ is an eigenvector of $\tilde{A}$, while Proposition 4.3.14 focuses on the cases where $\mathbf{x}_c$ is not. We clarify

the relationship between them here. Proposition 4.3.14(i) and (ii) correspond to the first row and last row of Table 4.1(a), respectively, but apply to cases where $\mathbf{x}_c$ is not an eigenvector. When the two eigenvalues are "highly distinct", $\lambda_1 \ll \lambda_2$, Proposition 4.3.14(i) aligns with the first row of Table 4.1(a). Specifically, suppose that $\tilde{A}\mathbf{x}_c = \lambda_i \mathbf{x}_c$ and $(\mathbf{v}_i^\top \mathbf{v}_j)^2 < 1 - \frac{(\lambda_i - \lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2}$, then we have $|\beta_1| = 0$ or $|\beta_2| = 0$. However, $|\beta_1| = 0$ cannot hold with $\lambda_1 \ll \lambda_2$, since this implies that $1 - \frac{(\lambda_2 - \lambda_1)^2 r^2}{\lambda_2^2 \|\mathbf{x}_c\|^2} < 0$, contradicting $(\mathbf{v}_1^\top \mathbf{v}_2)^2 < 1 - \frac{(\lambda_2 - \lambda_1)^2 r^2}{\lambda_2^2 \|\mathbf{x}_c\|^2}$. Hence if $\lambda_1 \ll \lambda_2$, the condition of the first row of Table 4.1(a) says that $|\beta_2| = 0$ and $\mathbf{v}_1^\top \mathbf{v}_2$ is small enough. If $|\beta_1/\beta_2| \geq 1$ (i.e., $\mathbf{x}_c$ is "essentially" an eigenvector associated with λ_1), then $\beta_1^2 + \beta_1\beta_2 \mathbf{v}_1^\top \mathbf{v}_2 \geq |\beta_1|(|\beta_1| - |\beta_2||\mathbf{v}_1^\top \mathbf{v}_2|) \geq |\beta_1|(|\beta_1| - |\beta_2|) \geq 0$. Thus the condition $\beta_1^2 + \beta_1\beta_2 \mathbf{v}_1^\top \mathbf{v}_2 \geq 0$ can be viewed as a counterpart to the first row of Table 4.1(a), when $\lambda_1 \ll \lambda_2$.

When the two eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$ are "highly distinct", i.e., $\mathbf{v}_1^\top \mathbf{v}_2$ is small enough, Proposition 4.3.14(ii) corresponds to the last row of Table 4.1(a). Similarly, we have $|\beta_1| = 0$ or $|\beta_2| = 0$ if $\mathbf{x}_c$ is an eigenvector. However, if $|\beta_2| = 0$, one has that $1 - \frac{(\lambda_1 - \lambda_2)^2 r^2}{\lambda_1^2 \|\mathbf{x}_c\|^2} > 0$ together with small enough $\mathbf{v}_1^\top \mathbf{v}_2$ violate the inequality $(\mathbf{v}_1^\top \mathbf{v}_2)^2 > 1 - \frac{(\lambda_1 - \lambda_2)^2 r^2}{\lambda_1^2 \|\mathbf{x}_c\|^2}$. Hence if $\mathbf{v}_1^\top \mathbf{v}_2$ is small enough, $\tilde{A}\mathbf{x}_c = \lambda_i \mathbf{x}_c$ and $(\mathbf{v}_i^\top \mathbf{v}_j)^2 > 1 - \frac{(\lambda_i - \lambda_j)^2 r^2}{\lambda_i^2 \|\mathbf{x}_c\|^2}$ imply that $|\beta_1| = 0$ and $\frac{|\lambda_1|}{|\lambda_2|} > \frac{\|\mathbf{x}_c\|}{r}\sqrt{1 - (\mathbf{v}_1^\top \mathbf{v}_2)^2} + 1$, i.e., $\lambda_1 \ll \lambda_2$. If $|\beta_2/\beta_1| \geq 1$ (i.e., $\mathbf{x}_c$ is "essentially" an eigenvector associated with λ_2), then $\beta_2^2 + \beta_1\beta_2 \mathbf{v}_2^\top \mathbf{v}_1 \geq |\beta_2|(|\beta_2| - |\beta_1||\mathbf{v}_1^\top \mathbf{v}_2|) \geq |\beta_2|(|\beta_2| - |\beta_1|) \geq 0$. Hence, provided that $\mathbf{v}_1^\top \mathbf{v}_2$ is small enough, the condition $\beta_1\beta_2 \mathbf{v}_2^\top \mathbf{v}_1 + \beta_2^2 \geq 0$ can be viewed as a counterpart to the last row of Table 4.1(a). □

Chapter 5

Converse Theorems for Certificates of Safety and Stability

Motivated by the key role of CBFs in assessing safety in assessing safety and and enabling the synthesis of safe controllers in nonlinear control systems, as demonstrated in Chapters 3 and 4, in this chapter we present a suite of converse results on CBFs. Given any safe set, we first identify a set of general sufficient conditions which guarantee the existence of a CBF. Our technical analysis also enables us to define an extended notion of CBF which is always guaranteed to exist if the set is safe. Next, we turn our attention to the problem of simulteanous safety and stability, and give conditions under which the notions of control Lyapunov-barrier function (CLBF) and compatible CLF-CBF pair are guaranteed to exist. Finally, we also identify conditions under which a CLBF and a compatible CLF-CBF pair can be constructed from a non-compatible CLF-CBF pair. Throughout the chapter, we intersperse different examples and counterexamples to motivate our results and position them within the state of the art.

5.1 Problem Statement

We consider a nonlinear control system of the form (2.4) and a safe set $\mathcal{C}$ described by a differentiable function h satisfying (2.6). We are broadly motivated by questions about the existence of functions certifying stability and safety. Specifi-

cally, our goal is to answer the following questions:

(P1) If $\mathcal{C}$ is safe for the system, does it always admit a CBF? This problem corresponds to the converse of Theorem 2.5.3, to which Theorem 2.5.4 provides an answer in case $\mathcal{C}$ is compact. Here we intend to establish a more general result;

(P2) Under what conditions can the existence of a CLBF or a (strictly) compatible CLF-CBF pair be guaranteed? These problems are motivated by the fact that in either case feedback controllers that achieve safe stabilization can be designed under appropriate technical conditions, as described in Chapter 2.

(P3) Does the existence of a (not necessarily compatible) CLF-CBF pair imply the existence of a (strictly) compatible CLF-CBF pair? This question shares its motivation with (P2) and the ease afforded by identifying a CLF and a CBF independently of each other.

We address these problems in the remainder of the chapter, providing sufficient conditions under which each of them can be solved.

5.2 Converse Results for Safety

In this section, we address problem (P1). Note that Theorem 2.5.4 already provides a partial answer for the case when $\mathcal{C}$ is compact. The treatment of this section establishes more general results. We start with an example showing that, given an arbitrary safe set $\mathcal{C}$, not every candidate CBF of $\mathcal{C}$ is a CBF of $\mathcal{C}$.

Example 5.2.1. (Choice of candidate CBF matters for unbounded safe sets): Consider the function $h : \mathbb{R}^2 \to \mathbb{R}$ given by $h(x, y) = x$ and the set $\mathcal{C}$ defined as in (2.6). Consider the system

$$\dot{x} = xy + 1,$$
$$\dot{y} = -y + u.$$

Since $\frac{d}{dt}h(x,y) = 1$ when $x = 0$ for any choice of u, by Nagumo's Theorem [126], $\mathcal{C}$ is safe. However, h is not a CBF. To show this, assume that it is. Therefore, there exists an extended class $\mathcal{K}_\infty$ function α satisfying

$$\nabla h(x,y)^\top \begin{pmatrix} xy \\ -y+u \end{pmatrix} = xy + 1 \geq -\alpha(x).$$

Note that, for any fixed $x > 0$, $\alpha(x)$ is constant, but by taking y sufficiently negative, xy can be arbitrarily negative, and the inequality $xy + 1 \geq -\alpha(x)$ will not be satisfied. Since this argument holds for any extended class $\mathcal{K}_\infty$ function α, h is not a CBF. Similarly, by assuming that α is a minimal function [104, Definition 1] also shows that h is not a *minimal control barrier function* [104, Definition 3].

However, one can show that the function $\tilde{h}(x,y) = e^y x$, which also satisfies (2.6), is in fact a CBF. Indeed, note that

$$\frac{d}{dt}\tilde{h}(x,y) = \nabla \tilde{h}(x,y)^\top \begin{pmatrix} xy+1 \\ -y+u \end{pmatrix} = e^y + e^y xu.$$

Taking $u = 0$ for all $(x,y) \in \mathbb{R}^2$ makes $\tilde{h}$ satisfy (2.7) for any class $\mathcal{K}_\infty$ function α. $\triangle$

The relevance of this example is in showing that the assumption that $\mathcal{C}$ be compact is critical for Theorem 2.5.4 (as well as [104, Corollary 2]) to hold, since this result establishes that any candidate CBF of $\mathcal{C}$ is a CBF of $\mathcal{C}$. The extension of this result to unbounded safe sets therefore requires adjustments in the technical approach. Interestingly, we should point out that some aspects of Lyapunov theory for stability are also not fully understood in the case of unbounded attractors [127].

Remark 5.2.2. (Other counterexamples in the literature): We explain here the relative value and qualitative differences of Example 5.2.1 with respect to other counterexamples in the literature. [1, Remark 8] gives an example of a safe set for which a differentiable function satisfying (2.6) is not a CBF, but does not specify whether there exists another function with the same properties that is. [128, Example 1] provides an example of a safe set with empty interior which does not admit a continuous barrier certificate [22] that is only a function of the state. However, the system considered does not have control inputs and the notion of

barrier certificate is different from the standard notion of CBF considered here (for which, for instance, safe sets have non empty interior). Finally, the counterexample in [128, Example 5] defines a safe set that is not expressible as the superlevel set of a differentiable function. •

5.2.1 Converse Theorem for CBFs

Example 5.2.1 shows that, for an arbitrary safe set $\mathcal{C}$, not every function satisfying (2.6) is a CBF, and in turn also raises the question of whether a CBF might even exist. The following result states conditions under which this is the case.

Theorem 5.2.3. (Converse CBF result for arbitrary sets): *Given a control system* (2.4)*, let* $\mathcal{C}$ *be a set for which there exists a continuously differentiable function* $h : \mathbb{R}^n \to \mathbb{R}$ *satisfying* (2.6)*. Suppose that* $\mathcal{C}$ *is safe and any of the following assumptions hold:*

(1) there exists an extended class $\mathcal{K}_\infty$ *function* α *and a function* $u_* : \mathbb{R}^n \to \mathbb{R}^m$ *such that, for all* $r \geq 0$*,*

$$\inf_{\{\mathbf{x}\in\mathbb{R}^n : h(\mathbf{x})\in[0,r]\}} \nabla h(\mathbf{x})^T f(\mathbf{x}, u_*(\mathbf{x})) \geq -\alpha(r); \tag{5.1}$$

(2) there exists a locally Lipschitz safe controller $u_0 : \mathbb{R}^n \to \mathbb{R}^m$ *and a positive function* $\nu : Int(\mathcal{C}) \to \mathbb{R}_{>0}$ *such that, for any* $\mathbf{x}_0 \in Int(\mathcal{C})$*, the trajectory* $x(\cdot)$ *of* $\dot{\mathbf{x}} = f(\mathbf{x}, u_0(\mathbf{x}))$ *with initial condition at* $\mathbf{x}_0$*, satisfies* $h(x(t)) \geq \nu(x_0) > 0$ *for all* $t \geq 0$*;*

(3) the function f *is continuously differentiable, there exists a continuously differentiable safe controller* $\hat{u} : \mathbb{R}^n \to \mathbb{R}^m$*, positive integers* $M_2 \in \mathbb{Z}_{>0}$*,* $N_2 \in \mathbb{Z}_{>0}$*, and positive constants* $\{b_j\}_{j\in\{1,\cdots,M_2\}}$*, and* $\{c_k\}_{k\in\{1,\cdots,N_2\}}$ *such that*

$$\left\|\nabla(\|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^2)\right\|^2 \leq \sum_{j=0}^{M_2} c_j \|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^j, \tag{5.2a}$$

$$\|\nabla h(\mathbf{x})\|^2 \leq \sum_{k=0}^{N_2} b_k \|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^k, \tag{5.2b}$$

for all $\mathbf{x} \in \mathcal{C}$*;*

(4) the set $\mathcal{C}$ is compact.

Then, there exists a CBF of $\mathcal{C}$.

Proof. Note that 4 is simply Theorem 2.5.4.

To show 1, note that if (5.1) holds, then for any $x \in \mathbb{R}^n$, we have

$$\nabla h(\mathbf{x})^T f(\mathbf{x}, u_*(\mathbf{x})) \geq -\alpha(h(\mathbf{x})),$$

and hence h is a CBF of $\mathcal{C}$.

We now prove 2 and divide the proof in two steps. First, we construct a function that is differentiable almost everywhere, satisfies (2.6) and for which the CBF condition (2.7) holds at all points where it is differentiable. Second, we smoothen this function and obtain an actual CBF.

First step: construction of a *CBF almost everywhere.* For this step, we rely on the techniques in [129], which studies the connection between Hamilton-Jacobi reachability and CBFs. Let us consider the cost function $V : \mathbb{R}^n \times \mathbb{R}_{<0} \to \mathbb{R}$

$$V(\mathbf{x}, t) = \min_{s \in [t,0]} h(x(s)),$$

which captures the minimum value of h along the trajectory $x(\cdot)$ that solves (2.4), with initial condition $\mathbf{x}$, initial time $t < 0$ and control $\mathbf{u}_0$ (note that as opposed to [129], here we omit the maximization over all possible controllers and simply use $\mathbf{u}_0$). As explained in [129, Section II.D], by extending the definition of V for infinite time as $V_{-\infty}(\mathbf{x}) := \lim_{t \to -\infty} V(\mathbf{x}, t)$, we obtain a time-invariant function whose zero-superlevel set is the largest forward invariant set of $\dot{\mathbf{x}} = f(\mathbf{x}, u_0(\mathbf{x}))$ contained in $\mathcal{C}$. In our case, since u_0 is a safe controller, $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : V_{-\infty}(\mathbf{x}) \geq 0\}$. Moreover, since $\mathbf{u}_0$ is such that all trajectories of $\dot{\mathbf{x}} = f(\mathbf{x}, u_0(\mathbf{x}))$ with initial condition $\mathbf{x}_0 \in \mathrm{Int}(\mathcal{C})$ satisfy $h(x(t)) \geq \nu(x_0)$ for all $t \geq 0$, it follows that $V(\mathbf{x}_0, t) \geq \nu(\mathbf{x}_0)$ for all $t < 0$ and therefore $V_{-\infty}(\mathbf{x}_0) \geq \nu(\mathbf{x}_0) > 0$ for all $\mathbf{x}_0 \in \mathrm{Int}(\mathcal{C})$. As also noted in [129, Section II.D], for all points in $\mathcal{C}$ where the gradient of $V_{-\infty}$ exists,

$$\nabla V_{-\infty}(\mathbf{x})^\top f(\mathbf{x}, u_0(\mathbf{x})) \geq -\alpha(V_{-\infty}(\mathbf{x})), \tag{5.3}$$

for any smooth extended class $\mathcal{K}_\infty$ function α. Since $V_{-\infty}$ might not be differentiable at some points, it might not be a valid CBF. However, since f, u_0 and h are

locally Lipschitz, $V_{-\infty}$ is locally Lipschitz (cf. [129, Remark 1]), and therefore by Rademacher's Theorem $V_{-\infty}$ is differentiable almost everywhere [130, Theorem 7.11].

Second step: smoothing. The rest of the proof smoothens $V_{-\infty}$ to obtain a valid CBF. To do so, we follow a procedure closely related to that of [131] for smoothing Lyapunov functions. Let us start by showing that we can smoothen $V_{-\infty}$ at the interior of $\mathcal{C}$ and guarantee (5.3) for all $\mathbf{x} \in \text{Int}(\mathcal{C})$ for the smoothened version of $V_{-\infty}$. Indeed, by [131, Theorem B.I] there exists a smooth $\Psi : \text{Int}(\mathcal{C}) \to \mathbb{R}$ such that for all $\mathbf{x} \in \text{Int}(\mathcal{C})$,

$$|V_{-\infty}(\mathbf{x}) - \Psi(\mathbf{x})| < \min\{\frac{1}{2}V_{-\infty}(\mathbf{x}), 1\},$$
$$\nabla\Psi(\mathbf{x})^T f(\mathbf{x}, u_0(\mathbf{x})) \geq -2\alpha(V_{-\infty}(\mathbf{x})).$$

Since $V_{-\infty}(\mathbf{x}) > 0$ for all $\mathbf{x} \in \text{Int}(\mathcal{C})$, then $\Psi(\mathbf{x}) > V_{-\infty}(\mathbf{x}) - \frac{1}{2}V_{-\infty}(\mathbf{x}) = \frac{1}{2}V_{-\infty}(\mathbf{x}) > 0$ for all $\mathbf{x} \in \text{Int}(\mathcal{C})$. Now extend Ψ at $\partial\mathcal{C}$ so that $\Psi(\mathbf{x}) = 0$ for all $\mathbf{x} \in \partial\mathcal{C}$. It follows that Ψ defined in this way is smooth in $\text{Int}(\mathcal{C})$ and continuous in $\mathcal{C}$. Moreover, since α is increasing, $2\alpha(V_{-\infty}(\mathbf{x})) \leq 2\alpha(2\Psi(\mathbf{x}))$. Hence, by defining $\bar{\alpha}(r) = 2\alpha(2r)$, $\bar{\alpha}$ is smooth, extended class $\mathcal{K}_\infty$ and for all $\mathbf{x} \in \text{Int}(\mathcal{C})$ it holds that $\nabla\Psi(x)^T f(\mathbf{x}, u_0(\mathbf{x})) \geq -\bar{\alpha}(\Psi(\mathbf{x}))$. Now, extend Ψ in $\mathbb{R}^n \backslash \mathcal{C}$ in such a way that Ψ is smooth in $\mathbb{R}^n \backslash \mathcal{C}$ and $\Psi(\mathbf{x}) < 0$ for all $\mathbf{x} \in \mathbb{R}^n \backslash \mathcal{C}$ so that Ψ is continuous in $\mathbb{R}^n$ and smooth in $\mathbb{R}^n \backslash \partial\mathcal{C}$. Let us now use Ψ to construct a function $\Phi : \mathbb{R}^n \to \mathbb{R}$ that is smooth in all of $\mathbb{R}^n$. In order to do so, let us show that there exists an extended class $\mathcal{K}_\infty$ function β such that $\Phi := \beta \circ \Psi$ is smooth in all of $\mathbb{R}^n$. The proof follows that of [131, Lemma 4.3], where the main difference is that in our case Ψ takes positive and negative values. For $i \in \mathbb{Z}_{>0}$, let K_i be compact subsets of $\mathbb{R}^n$ such that $\partial\mathcal{C} \subset \bigcup_{i=1}^{\infty} K_i$. For any $k \in \mathbb{Z}_{>0}$, let:

$$I_k^+ := \left(\frac{1}{k+2}, \frac{1}{k}\right), \quad I_k^- := \left(-\frac{1}{k}, -\frac{1}{k+2}\right).$$

Pick also smooth $\mathcal{C}^\infty(\mathbb{R})$ functions $\gamma_k^+ : \mathbb{R} \to [0, 1]$, $\gamma_k^- : \mathbb{R} \to [-1, 0]$ satisfying

- $\gamma_k^+(t) = 0$ if $t \notin I_k^+$,
- $\gamma_k^+(t) > 0$ if $t \in I_k^+$,

- $\gamma_k^-(t) = 0$ if $t \notin I_k^-$,
- $\gamma_k^-(t) < 0$ if $t \in I_k^-$.

Define also for any $k \in \mathbb{Z}_{>0}$,

$$\mathcal{G}_k := \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \in \bigcup_{i=1}^{k} K_i, \quad \Psi(\mathbf{x}) \in \text{clos}(I_k^+ \cup I_k^-)\}.$$

Observe that $\mathcal{G}_k$ is compact for all $k \in \mathbb{Z}_{>0}$ (because the sets K_i are compact and Ψ is continuous) and hence for each $k \in \mathbb{Z}_{>0}$ there exists $c_k \in \mathbb{R}$ satisfying:

(1) $c_k \geq 1$,

(2) $c_k \geq |(D^\rho \Psi)(\mathbf{x})|$ for any multi-index $|\rho| \leq k$ and $x \in \mathcal{G}_k$,

(3) $c_k \geq |\gamma_k^{(i)}(t)|$ for any $i \leq k$ and any $t \in \mathbb{R}_{>0}$.

Choose the sequence $\{d_k\}_{k \in \mathbb{Z}_{>0}}$ to satisfy

$$0 < d_k < \frac{1}{2^k (k+1)! c_k^k}, \quad k \in \mathbb{Z}_{>0}.$$

Now, define

$$\gamma(t) = \sum_{k=1}^{\infty} d_k (\gamma_k^+(t) + \gamma_k^-(t)) + \delta(t)$$

where $\delta : \mathbb{R} \to \mathbb{R}$ is a $\mathcal{C}^\infty(\mathbb{R})$ function such that $\delta \equiv 0$ on $[-\frac{1}{3}, \frac{1}{3}]$, $\delta \geq 1$ on $[\frac{1}{2}, \infty)$ and $\delta \leq -1$ on $(-\infty, -\frac{1}{2}]$. By following an argument analogous to the one in the proof of [131, Lemma 4.3], we can show that γ is smooth in $\mathbb{R}\backslash\{0\}$ and $\lim_{t \to 0} \gamma^{(i)}(t) = 0$ for all $i \geq 1$. Moreover, $\beta(t) := \int_0^t \gamma(s) ds$ is an extended class $\mathcal{K}_\infty$, smooth in $\mathbb{R}\backslash\{0\}$, and satisfies $\lim_{t \to 0} \beta^{(i)}(t) = 0$ for all $i \geq 1$. Again by following the proof of [131, Lemma 4.3], one can show that $\Phi = \beta \circ \Psi$ is smooth in $\mathbb{R}^n$. This follows by considering sequences converging to points in $\partial\mathcal{C}$ and showing that the derivatives of any order of Φ along these sequences converge to zero.

Finally, now that we know that Φ is smooth and satisfies $\text{Int}(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n : \Phi(\mathbf{x}) > 0\}$, $\partial\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : \Phi(\mathbf{x}) = 0\}$, let us show that Φ is a CBF. Indeed, for all $\mathbf{x} \in \text{Int}(\mathcal{C})$, since $\Phi = \beta \circ \Psi$, it holds that

$$\nabla \Phi(\mathbf{x})^\top f(\mathbf{x}, u_0(\mathbf{x})) \geq -\beta'(\Psi(\mathbf{x})) \bar{\alpha}(\Psi(\mathbf{x}))$$

Note that $\beta'(r)\bar{\alpha}(r) > 0$ for $r > 0$, $\beta'(0)\bar{\alpha}(0) = 0$ and $\beta'(r)\bar{\alpha}(r)$ is smooth for all $r \in \mathbb{R}$. Therefore, $\beta'(r)\bar{\alpha}(r)$ can be upper bounded for $r \geq 0$ by a smooth extended class $\mathcal{K}_\infty$ function $\hat{\alpha}$. Finally, since β is an extended class $\mathcal{K}_\infty$ function, it is invertible and we can define $\breve{\alpha}(r) := \hat{\alpha} \circ \beta^{-1}(r)$, which is also smooth and extended class $\mathcal{K}_\infty$, so that for all $x \in \mathcal{C}$ it holds that

$$\nabla\Phi(\mathbf{x})^\top f(\mathbf{x}, u_0(\mathbf{x})) \geq -\breve{\alpha}(\Phi(\mathbf{x})).$$

Hence Φ is a CBF of $\mathcal{C}$. In fact $u_0(\mathbf{x})$ satisfies the CBF inequality (2.7) for all $\mathbf{x} \in \mathcal{C}$.

Let us now show 3. First, let us show that without loss of generality, we can assume that h is bounded in $\mathcal{C}$. Indeed, if h is not bounded, consider the function $\tilde{h} : \mathbb{R}^n \to \mathbb{R}$ as $\tilde{h}(\mathbf{x}) = h(\mathbf{x})e^{-h(\mathbf{x})}$. Note that $\tilde{h}$ is continuously differentiable (because h is also continuously differentiable), bounded in $\mathcal{C}$ and, since $e^{h(\mathbf{x})} > 0$ for all $\mathbf{x} \in \mathcal{C}$, $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : \tilde{h}(\mathbf{x}) \geq 0\}$, $\partial\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) = 0\}$, $\text{Int}(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) > 0\}$. Furthermore,

$$\nabla\tilde{h}(\mathbf{x}) = \nabla h(\mathbf{x})e^{-h(\mathbf{x})}(1 - h(\mathbf{x})), \tag{5.4}$$

for all $\mathbf{x} \in \mathcal{C}$, and it satisfies an inequality analogous to (5.2b). Indeed, let $\tilde{M} > 0$ be such that $e^{-2h(\mathbf{x})}(1 + h(\mathbf{x}))^2 < \tilde{M}$ for all $\mathbf{x} \in \mathcal{C}$. Then, by defining $\tilde{b}_k := \tilde{M}b_k$ for $k \in \{0, 1, \cdots, N_2\}$, and using (5.4) we have

$$\|\nabla\tilde{h}(\mathbf{x})\|^2 \leq \sum_{k=0}^{N_2} \tilde{b}_k \|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^2,$$

for all $\mathbf{x} \in \mathcal{C}$. Therefore, without loss of generality, we assume that h is bounded in $\mathcal{C}$. Let $M > 0$ be such that $h(\mathbf{x}) \leq M$ for all $\mathbf{x} \in \mathcal{C}$. Now, consider the function $\bar{h}(\mathbf{x}) = e^{-\|f(\mathbf{x},\hat{u}(\mathbf{x}))\|^2}h(\mathbf{x})$. Note that $\bar{h}$ is bounded, continuously differentiable and $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : \bar{h}(\mathbf{x}) \geq 0\}$, $\text{Int}(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n : \bar{h}(\mathbf{x}) > 0\}$ and $\partial\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : \bar{h}(\mathbf{x}) = 0\}$. Moreover,

$$\begin{aligned}\nabla\bar{h}(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x})) = e^{-\|f(\mathbf{x},\hat{u}(\mathbf{x}))\|^2}\nabla h(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x}))\\ -h(\mathbf{x})e^{-\|f(\mathbf{x},\hat{u}(\mathbf{x}))\|^2}\nabla(\|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^2)^\top f(\mathbf{x}, \hat{u}(\mathbf{x})),\end{aligned}$$

and, by using the bounds in (5.2), the fact that h is bounded in $\mathcal{C}$, and the Cauchy-Schwartz inequality, we get that for all $\mathbf{x} \in \mathcal{C}$, the following holds:

$$\nabla \bar{h}(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x})) \geq$$
$$- e^{-\|f(\mathbf{x},\hat{u}(\mathbf{x}))\|^2} \sqrt{\sum_{k=0}^{N_2} b_k \|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^{k+1}} - e^{-\|f(\mathbf{x},\hat{u}(\mathbf{x}))\|^2} M \sqrt{\sum_{j=0}^{M_2} c_j \|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|^{j+1}}.$$

Thus,

$$\alpha(r) = - \inf_{\{\mathbf{x} \mid \bar{h}(\mathbf{x}) \in [0,r]\}} \nabla \bar{h}(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x}))$$

is finite for all $r \geq 0$. This follows from the fact that even if $\|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|$ is unbounded as $\|\mathbf{x}\| \to \infty$, the exponential term in $\|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|$ will dominate the polynomial terms in $\|f(\mathbf{x}, \hat{u}(\mathbf{x}))\|$. Moreover, since $\hat{u}$ is safe, and $\bar{h}$ satisfies conditions (2.6), any trajectory $x(\cdot)$ of $\dot{\mathbf{x}} = f(\mathbf{x}, \hat{u}(\mathbf{x}))$ for which $x(t^*) \in \partial\mathcal{C}$ for some $t^* \in \mathbb{R}$ necessarily satisfies $\nabla \bar{h}(\mathbf{x})^T f(\mathbf{x}, \hat{u}(\mathbf{x})) \geq 0$ by Nagumo's Theorem [126]. This implies that $\alpha(0) \leq 0$, and α can be upper bounded by a class $\mathcal{K}_\infty$ function α_0, from where we have $\nabla \bar{h}(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x})) \geq -\alpha_0(\bar{h}(\mathbf{x}))$ for all $\mathbf{x} \in \mathcal{C}$, and hence $\bar{h}$ is a CBF of $\mathcal{C}$. In fact $\hat{u}(\mathbf{x})$ satisfies the CBF inequality (2.7) for all $\mathbf{x} \in \mathcal{C}$. □

Remark 5.2.4. (Minimal CBFs and smoothness properties): Even though 0 is not a regular value of the CBF Φ constructed in Theorem 5.2.3 2, Φ is a minimal CBF because the extended class $\mathcal{K}_\infty$ function $\breve{\alpha}$ is smooth [104, Corollary 1]. Moreover, if in Theorem 5.2.3 3, we add the assumption that 0 is a regular value of h, then 0 is also a regular value of $\bar{h}$ (the CBF constructed in the proof) and $\bar{h}$ is a minimal CBF [104, Section III]. This implies that the CBFs constructed in Theorem 5.2.3 can be used for control design according to [104, Theorem 4] and [23, Theorem 2]. Moreover, even if the minimal CBFs constructed in Theorem 5.2.3 **??** and **??** are not $\mathcal{C}^\infty(\mathbb{R}^n)$, by applying the smoothing procedure outlined in the proof of Theorem 5.2.3 2 to any differentiable minimal CBF, we can construct another minimal CBF that is $\mathcal{C}^\infty(\mathbb{R}^n)$. •

Remark 5.2.5. (Class of systems and safe sets satisfying (5.2)): As shown in the proof of Theorem 5.2.3 3, condition (5.2) guarantees that $\bar{h}$ (as defined therein) satisfies that the function $\mathbf{x} \to \nabla \bar{h}(\mathbf{x})^T f(\mathbf{x}, \hat{u}(\mathbf{x}))$ is lower bounded in the set

$\{\mathbf{x} \in \mathbb{R}^n : \bar{h}(\mathbf{x}) \in [0, r]\}$, avoiding the issues faced in Example 5.2.1. Condition (5.2) is satisfied by a large class of systems, including polynomial systems for which there exists a polynomial safe feedback and safe sets $\mathcal{C}$ for which there exists a polynomial function h satisfying (2.6). •

Remark 5.2.6. (Comparison with time-varying barrier functions): The result in [128, Theorem 2] guarantees the existence of a time-varying barrier function, cf. [128, Definition 15], under more general assumptions than Theorem 5.2.3. Despite the importance of this result, the construction of such time-varying barrier functions is in general complicated and requires computing an appropriately defined reachable set. Moreover, such functions are in general not differentiable even if the dynamics are smooth [128, Theorem 4]. The added time dependence and the lack of control input and extended class $\mathcal{K}_\infty$ function make the notion of time-varying barrier functions substantially different from the notion of control barrier function considered here, which is the one widely employed in the safety-critical control literature [23, 1, 132]. It is also not apparent from the proof of [128, Theorem 2] when the obtained barrier function is time-independent. We also point out that the proof technique in Theorem 5.2.3 is different from that of [128, Theorem 2], and as pointed out in Remark 5.2.4, can be used to obtain barrier functions which are $\mathcal{C}^\infty(\mathbb{R}^n)$. •

Remark 5.2.7. (Robust safety): Here we comment on the relationship between robust safety, cf. [133, Definition 2], and the assumptions in Theorem 5.2.3 2, motivated by the fact that robust safety is also a sufficient condition for the existence of a certain notion of barrier function (different from the one adopted here because it does not utilize extended class $\mathcal{K}_\infty$ functions) [133, Theorems 1 and 2]. In particular, next we provide an example where the conditions in Theorem 5.2.3 **??** hold but robust safety does not hold. Consider the scalar system $\dot{x} = xu$, safe set $\mathcal{C} = \{x \in \mathbb{R} : x \geq 0\}$, and safe controller $k(x) = 1$ for all $x \in \mathbb{R}$. Any trajectory of the closed-loop system with initial condition in $\mathrm{Int}(\mathcal{C})$ diverges to infinity and therefore the assumptions of Theorem 5.2.3 **??** hold. However, the system is not robustly safe, since for any scalar function $\epsilon : \mathbb{R} \to \mathbb{R}_{>0}$, the trajectory of $\dot{x} = x - \epsilon(x)$ with initial condition at the origin enters the unsafe set (because $\epsilon(0) > 0$). •

Remark 5.2.8. (Strict positivity in the interior of the safe set): Definition 2.5.2 requires h to be strictly positive in $\text{Int}(\mathcal{C})$. However, other definitions available in the literature (e.g., [104, Theorem 1]) only require $\mathcal{C} \coloneqq \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}$. With this definition of CBF it can be shown that any safe set admits a CBF. This follows by adapting the proof of Theorem 5.2.3 2 to the case where there might be points $x \in \text{Int}(\mathcal{C})$ for which $V_{-\infty}(\mathbf{x}) = 0$, i.e., finding a smooth approximation Ψ of $V_{-\infty}(\mathbf{x})$ at $\{\mathbf{x} \in \mathbb{R}^n : V_{-\infty}(\mathbf{x}) \neq 0\}$ and then extending Ψ smoothly at $\{\mathbf{x} \in \mathbb{R}^n : V_{-\infty}(\mathbf{x}) = 0\}$ as done in the proof of Theorem 5.2.3 2. •

Remark 5.2.9. (Asymptotic stability of safe set): As shown in [1, Proposition 2], if $u_{\text{sf}} : \mathbb{R}^n \to \mathbb{R}^m$ is a Lipschitz controller satisfying the CBF condition (2.7) for all $\mathbf{x} \in \mathcal{D}$, where $\mathcal{D}$ is an open set containing $\mathcal{C}$, then the set $\mathcal{C}$ is asymptotically stable. By appropriately strengthening the conditions in Theorem 5.2.3, we can also guarantee the existence of a CBF valid in an open set containing $\mathcal{C}$, and hence certifying asymptotic stability of $\mathcal{C}$. Indeed,

(1) in Theorem 5.2.3 1, if there exists $r_0 < 0$ such that (5.1) is satisfied for all $r \geq r_0$, then h is a CBF and (2.7) is feasible (by using $u = u_*(\mathbf{x})$) for all $\mathbf{x} \in \mathbb{R}^n$ with $h(\mathbf{x}) \geq r_0$;

(2) in Theorem 5.2.3 2, under the additional assumption that there exists an open set $\mathcal{D}$ containing $\mathcal{C}$ for which any trajectory of $\dot{x} = f(\mathbf{x}_0, u_0(\mathbf{x}))$ with initial condition in $\mathcal{D} \backslash \text{Int}(\mathcal{C})$ either converges to $\mathcal{C}$ in finite time or asymptotically, by following the same proof technique we can show that Φ (as obtained in the proof) is a CBF and (2.7) is feasible (by using $\mathbf{u} = u_0(\mathbf{x})$) for all $\mathbf{x} \in \mathcal{D}$;

(3) in Theorem 5.2.3 3, if there exists an open set $\mathcal{D}$ containing $\mathcal{C}$ for which (5.2) holds for all $\mathbf{x} \in \mathcal{D}$, then the same proof technique shows that there exists a CBF of $\mathcal{C}$ and the corresponding inequality (2.7) is also feasible in $\mathcal{D}$;

(4) in Theorem 5.2.3 4, since $\mathcal{C}$ is compact, if it is asymptotically stable, by [131, Theorem 2.9] there exists a Lyapunov function with respect to $\mathcal{C}$. Therefore, h (which is guaranteed to be a CBF by Theorem 2.5.4) can be extended outside of $\mathcal{C}$ using this Lyapunov function (smoothly, using the arguments in [131, Proposition 4.2] and Theorem 5.2.3 2). •

Even though Theorem 5.2.3 extends significantly Theorem 2.5.4 regarding the class of safe sets and systems for which a CBF exists, it is an open problem to determine whether an even more general result holds true. The following example is not covered by any of the cases in Theorem 5.2.3.

Example 5.2.10. (Example not covered by converse CBF theorem): Here we provide an example of a control system and safe set not covered by any of the cases in Theorem 5.2.3. Let $m = n = 1$, $h : \mathbb{R} \to \mathbb{R}$ be defined as $h(x) = e^x \sin(x)$, and let $\mathcal{C}$ be the corresponding safe set as defined in (2.6). Note that h is continuously differentiable. Define the dynamics by letting $f(x, u) = h(x)$ (since systems without control are a special case of systems with control, Theorem 5.2.3 still applies). Note that $\mathcal{C}$ is safe because all points in $\partial\mathcal{C}$ are equilibrium points, and since h is continuously differentiable, trajectories of the dynamical system are unique, which means that no trajectory can leave the safe set. Furthermore, since $\dot{x} > 0$ whenever $x \in \text{Int}(\mathcal{C})$, trajectories of the dynamical system with initial condition in $\text{Int}(\mathcal{C})$ converge to $\partial\mathcal{C}$ and therefore item 2 does not hold. Similarly, since $\mathcal{C}$ is not compact, item 4 does not hold either. Now let us show that item 1 does not hold, which in turn also implies that item 3 can not hold (because item 3 implies item 1, as shown in the proof of Theorem IV.3). For any $k \in \mathbb{Z}_{>0}$, let $\underline{a}_k = (2k+1)\pi - \frac{\pi}{4}$, $\bar{a}_k = (2k+1)\pi$, and note that

$$h(\underline{a}_k) \geq \frac{e^{-\frac{\pi}{4}}\sqrt{2}}{2},\ \cos(\underline{a}_k) = -\frac{\sqrt{2}}{2},\ h(\bar{a}_k) = 0,\ \cos(\bar{a}_k) = -1,$$

and $\cos(a) < 0$ for all $a \in [\underline{a}_k, \bar{a}_k]$. Therefore, by letting $r = e^{-\frac{\pi}{4}}\frac{\sqrt{2}}{2}$, there exists a sequence $(a_k)_{k\in\mathbb{Z}_{>0}}$ (with $a_k \in ((2k+1)\pi - \frac{\pi}{4}, (2k+1)\pi)$ for all $k \in \mathbb{Z}_{>0}$) such that $\frac{r}{2} < h(a_k) < r$, and $\cos(a_k) < 0$ for all $k \in \mathbb{Z}_{>0}$. Now, note that

$$h'(a_k)f(a_k) = h(a_k)^2 + e^{a_k}\cos(a_k)h(a_k).$$

Since $\sin(a_k) < \frac{r}{e^{a_k}} < 1$, it follows that $|\cos(a_k)| = \sqrt{1 - \sin^2(a_k)} > \sqrt{1 - \left(\frac{r}{e^{a_k}}\right)^2}$, and

$$h'(a_k)f(a_k) < r^2 - e^{a_k}\frac{r}{2}\sqrt{1 - \left(\frac{r}{e^{a_k}}\right)^2}.$$

Therefore, since $\lim_{k\to\infty} a_k = \infty$,

$$\lim_{k\to\infty} h'(a_k)f(a_k) = -\infty,$$

which means that 1 does not hold. •

5.2.2 Extended Control Barrier Functions

In this section, we show that Theorem 2.5.4 remains valid when we drop the compactness assumption provided that one employs a slight generalization of the notion of CBF. The latter requires a generalization of the notion of extended class $\mathcal{K}_\infty$.

Definition 5.2.11. (Extended class $\mathcal{KK}$ function): *A continuous function $\alpha : \mathbb{R} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{KK}$ if $\alpha(\cdot, s)$ and $\alpha(r, \cdot)$ are strictly increasing for all $s \geq 0$, $r \in \mathbb{R}$, respectively and $\alpha(0, s) = 0$ for all $s \geq 0$. It is of extended class $\mathcal{K}_\infty\mathcal{K}$ if, additionally, $\lim_{r\to\pm\infty} \alpha(r, s) = \pm\infty$ for all $s \geq 0$.*

We are ready to introduce the notion of *Extended Control Barrier Functions*.

Definition 5.2.12. (Extended Control Barrier Function): *Let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function and let $\mathcal{C}$ be defined as in* (2.6)*. The function h is an extended control barrier function (**eCBF**) of $\mathcal{C}$ if there exists an extended class $\mathcal{K}_\infty\mathcal{K}$ function α such that, for all $\mathbf{x} \in \mathcal{C}$, there exists a control $\mathbf{u} \in \mathbb{R}^m$ satisfying:*

$$\nabla h(\mathbf{x})^T f(\mathbf{x}, \mathbf{u}) \geq -\alpha(h(\mathbf{x}), \|\mathbf{x}\|). \tag{5.5}$$

Note that eCBFs allow for the time derivative of h to become arbitrarily negative as $\|x\|$ approaches infinity, as long as such derivative stays nonnegative at the boundary of $\mathcal{C}$. The following result relates the notions of CBF and eCBF.

Proposition 5.2.13. (Relationship between CBFs and eCBFs): *A CBF of $\mathcal{C}$ is also an eCBF of $\mathcal{C}$. Moreover, if $\mathcal{C}$ is compact, an eCBF of $\mathcal{C}$ is a CBF of $\mathcal{C}$.*

Proof. Let h be a CBF of $\mathcal{C}$, i.e., there exists an extended class $\mathcal{K}_\infty$ function α such that, for all $\mathbf{x} \in \mathcal{C}$, there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (2.7). Define

$$\hat{\alpha}(r, s) := \alpha(r)(s + 1)$$

and note that it is an extended class $\mathcal{K}_\infty\mathcal{K}$ function. Since $\hat{\alpha}(h(\mathbf{x}), \|\mathbf{x}\|) \geq \alpha(h(\mathbf{x}))$ for all $\mathbf{x} \in \mathcal{C}$, it follows that for all $\mathbf{x} \in \mathcal{C}$ there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (5.5). Now, suppose that $\mathcal{C}$ is compact and let h_e be an eCBF of $\mathcal{C}$, i.e., there exists a class $\mathcal{K}_\infty\mathcal{K}$ function α_e such that, for all $x \in \mathcal{C}$, there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (5.5). Define, for $r \geq 0$,

$$\tilde{\alpha}_e(r) := \sup_{\{\mathbf{x} \in \mathbb{R}^n :\ 0 \leq h_e(\mathbf{x}) \leq r\}} \alpha_e(r, \|\mathbf{x}\|).$$

Since $\mathcal{C}$ is compact, $\tilde{\alpha}_e(r)$ is finite for all $r \geq 0$. Furthermore, it is strictly increasing, satisfies $\tilde{\alpha}_e(0) = 0$, and satisfies $\lim_{r \to \infty} \alpha(r) = \infty$, so it can be extended to $\mathbb{R}_{<0}$ so that is of extended class $\mathcal{K}_\infty$. Since for all $\mathbf{x} \in \mathcal{C}$, $\tilde{\alpha}_e(h(\mathbf{x})) \geq \alpha(h(\mathbf{x}), \|\mathbf{x}\|)$, we have that, for all $\mathbf{x} \in \mathcal{C}$, there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (2.7), i.e., h_e is a CBF. □

According to Proposition 5.2.13, eCBFs coincide with CBFs when the safe set is compact. As we show later, the notion of eCBF is a more suitable notion to deal with safe sets that are unbounded. Similarly to Definition 2.5.7, we can also define a notion of compatibility for eCBFs (instead of CBFs) and CLFs.

Definition 5.2.14. *A CLF V and an eCBF h are **compatible** at $\mathbf{x} \in \mathcal{C}$ if there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying* (2.5) *and* (5.5) *simultaneously. We refer to both functions as compatible in $\mathcal{C}$ if they are compatible at every point in $\mathcal{C}$.*

Since eCBFs also enforce the satisfaction of Nagumo's Theorem [126], they can be used to certify safety, as stated in the following result. We omit its proof, which follows an argument analogous to that of [23, Theorem 2].

Proposition 5.2.15. (eCBFs certify safety): *Let $\mathcal{C} \subset \mathbb{R}^n$, h an eCBF of $\mathcal{C}$, and 0 a regular value of h. Any Lipschitz controller $k : \mathbb{R}^n \to \mathbb{R}^m$ that satisfies $k(\mathbf{x}) \in K_{ecbf}(\mathbf{x}) := \{\mathbf{u} \in \mathbb{R}^m : \nabla h(\mathbf{x})^\intercal f(\mathbf{x}, \mathbf{u}) + \alpha(h(\mathbf{x}), \|\mathbf{x}\|) \geq 0\}$ for all $\mathbf{x} \in \mathcal{C}$ renders the set $\mathcal{C}$ forward invariant.*

We also point out that the control designs proposed in [31, 4, 1] can easily be adapted using eCBFs instead of CBFs.

Next we show that the flexibility added by the class $\mathcal{K}_\infty\mathcal{K}$ function allows eCBFs to resolve some of the issues faced by CBFs.

Example 5.2.16 (Examples 5.2.1 and 5.2.10 revisited)**.** We show here that $h(x, y) = x$ is an eCBF for Example 5.2.1. Take $\alpha(r, s) = rs$ as the extended class $\mathcal{K}_\infty\mathcal{K}$ function in (5.5). It is straightforward to check that $\nabla h(x, y)^\top \left(\begin{smallmatrix} xy+1 \\ -y+u \end{smallmatrix}\right) = xy + 1 \geq -x\sqrt{x^2 + y^2} = -\alpha(h(x, y), \|(x, y)\|)$ for $x \geq 0$ and hence (5.5) is satisfied for all points in $\mathcal{C}$. By a similar argument, the function h defined in 5.2.10 is also an eCBF for the dynamics defined therein. △

The following result states that the existence of an eCBF is also necessary for a set to be safe, generalizing Theorem 2.5.4 to safe sets that might be unbounded.

Theorem 5.2.17. (Converse eCBF result for safe sets): *Given a control system* (2.4)*, let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function with $\mathcal{C}$ defined as in* (2.6) *and with* 0 *a regular value of h. If $\mathcal{C}$ is safe, then h is an eCBF.*

Proof. For $r \geq 0$, $c \geq 0$, define the set $S_{r,c} \coloneqq \{\mathbf{x} \in \mathbb{R}^n : 0 \leq h(\mathbf{x}) \leq r, \|\mathbf{x}\| \leq c + c_{\min}\}$, where $c_{\min} \geq 0$ is taken so that $S_{0,0} \neq \varnothing$ (for instance, one can set $c_{\min}$ as the distance from the origin to $\partial\mathcal{C}$). Since $S_{0,0} \subseteq S_{r,c}$ for any $r \geq 0$, $c \geq 0$, this guarantees that $S_{r,c} \neq \varnothing$ for all $r \geq 0, c \geq 0$. Next, define

$$\hat{\alpha}(r, c) \coloneqq -\min_{\mathbf{x} \in S_{r,c}} \nabla h(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x})), \tag{5.6}$$

where $\hat{u} : \mathbb{R}^n \to \mathbb{R}^m$ is a locally Lipschitz controller that renders $\mathcal{C}$ safe (which exists, by assumption). Since $S_{r,c}$ is compact for all $r \geq 0$, $c \geq 0$, $\hat{\alpha}(r, c)$ is finite for all $r \geq 0$, $c \geq 0$. Note that $\hat{\alpha}$ is non-decreasing in both its first and second arguments. Moreover, since $\mathcal{C}$ is forward invariant under $\dot{\mathbf{x}} = f(\mathbf{x}, \hat{u}(\mathbf{x}))$ and 0 is a regular value of h, by Nagumo's theorem [126], $\hat{\alpha}(0, c) \leq 0$ for all $c \geq 0$. Hence, we can find a class $\mathcal{K}_\infty\mathcal{K}$ function α such that $\alpha(r, c) \geq \hat{\alpha}(r, c)$ for all $r \geq 0, c \geq 0$. This ensures that

$$\nabla h(\mathbf{x})^\top f(\mathbf{x}, \hat{u}(\mathbf{x})) \geq -\alpha(h(\mathbf{x}), \|\mathbf{x}\|).$$

for all $\mathbf{x} \in \mathcal{C}$, hence completing the proof. □

Remark 5.2.18. (Comparison with time-varying barrier functions-cont'd): As mentioned in Remark 5.2.6, [128, Theorem 2] provides a necessary and sufficient condition for safety in terms of so-called time-varying barrier functions, which might however be difficult to construct and utilize in practice to design safe controllers. Instead, in the less general setting considered here, Theorem 5.2.17 ensures that if $\mathcal{C}$ is safe, any scalar continuously differentiable function satisfying (2.6) and having 0 as a regular value is an eCBF. This ensures that h is time-invariant and continuously differentiable, and instead of computing a complicated reachable set, only requires finding a scalar continuously differentiable function satisfying (2.6), with 0 being a regular value of it. •

5.3 Converse Theorems for Joint Safety and Stability

In this section we address problems (P2) and (P3) in Section 5.1. We start by studying under what conditions the existence of either (i) a compatible CLF-CBF pair or (ii) a CLBF is guaranteed. Our motivation comes from the fact that in either case locally Lipschitz feedback controllers that achieve safe stabilization can be designed under appropriate technical conditions, cf. Chapter 2. Throughout this section, we assume $\mathbf{0}_n \in \mathrm{Int}(\mathcal{C})$.

Our starting point is the result in [30, Theorem 11], which shows that if the set $\mathbb{R}^n \backslash \mathcal{C}$ is bounded, then a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$ can not exist. In fact the proof of [30, Theorem 11] (as well as [116]) shows that if $\mathbb{R}^n \backslash \mathcal{C}$ is bounded, a locally Lipschitz safe stabilizing controller can not exist. More generally, the same argument shows that if $\mathbb{R}^n \backslash \mathcal{C}$ has a bounded connected component, then a safe stabilizing controller can not exist.

Proposition 5.3.1. (Topological obstruction for existence of compatible CLF-CBF pair): *If the set $\mathbb{R}^n \backslash \mathcal{C}$ has a bounded connected component, then there does not exist a strictly compatible CLF-CBF pair on $\mathcal{C}$.*

Proof. Suppose there exits a strictly compatible CLF-CBF pair on $\mathcal{C}$. Then, by

using the universal formula in [31] (which is constructed by computing the centroid of the set of controls satisfying the CLF and CBF conditions), one can construct a smooth safe stabilizing controller on $\mathcal{C}$. But, since $\mathbb{R}^n \backslash \mathcal{C}$ contains a bounded connected component, by the argument used in [30, Theorem 11], this can not be possible, reaching a contradiction. □

Even though Proposition 5.3.1 only ensures the non-existence of a *strictly* compatible CLF-CBF pair, it also shows that even if a compatible CLF-CBF pair exists, one would not be able to leverage it to design a locally Lipschitz controller that safely stabilizes the system. The above result explains why the recent body of literature [34, 118, 4, 6, 5] on locally Lipschitz controllers that achieve safe stabilization obtain closed-loop systems with undesirable equilibrium points in the boundary of the safe set, when the set of unsafe states has a bounded connected component. We note also that the proof of Proposition 5.3.1 relies on [30, Theorem 11], which shows that if $\mathbb{R}^n \backslash \mathcal{C}$ is bounded, there can not exist a smooth safe stabilizing controller. A similar result (for analytic vector fields) is also available in [17, Proposition 3].

The next result identifies another scenario where a CLBF does not exist.

Proposition 5.3.2. (No CLBF exists for unbounded safe sets): *Suppose $\mathcal{C} \neq \mathbb{R}^n$ is unbounded. Then, there does not exist a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$.*

Proof. If $\mathbb{R}^n \backslash \mathcal{C}$ is bounded, there does not exist a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$ by [117]. If $\mathbb{R}^n \backslash \mathcal{C}$ is unbounded, assume by contradiction that there exists a CLBF $\bar{V}$. As shown in [134, Remark 13], condition (2.12c) requires that $\partial \mathcal{C}$ is the 0-level set of $\bar{V}$. Indeed, if $\mathbf{x} \in \partial \mathcal{C}$ is such that $\bar{V}(\mathbf{x}) > 0$, then there exists a sequence $\{\mathbf{x}_n\}_{n \in \mathbb{Z}_{>0}}$ converging to x such that $\bar{V}(\mathbf{x}_n) > 0$ (and hence $\mathbf{x}_n \notin \mathcal{U}$) and $\mathbf{x}_n \in \mathcal{C}$ for all $n \in \mathbb{Z}_{>0}$. This means that $\mathbf{x} \in \overline{(\mathcal{C} \backslash \mathcal{U})} \cap \overline{(\mathbb{R}^n \backslash \mathcal{C})}$, which is impossible by condition (2.12c). Finally, note that it is not possible for $\partial \mathcal{C}$ to be a 0-level set of $\bar{V}$ because $\bar{V}$ is proper, implying that all of its level sets are compact. □

Next, we turn our attention to identifying conditions under which either a CLBF or a compatible CLF-CBF pair exists provided that the origin is safely stabilizable.

Theorem 5.3.3. (Converse result on safe stabilization): *Given a control system* (2.4)*, let* $\mathcal{C}$ *be a set for which there exists a continuously differentiable function* $h : \mathbb{R}^n \to \mathbb{R}$ *satisfying* (2.6)*. Then,*

(1) if $\mathcal{C}$ *is compact and the origin is safely stabilizable on* $\mathcal{C}$*, then there exists a CLBF of* $\mathbb{R}^n \backslash \mathcal{C}$ *and a strictly compatible CLF-CBF pair in* $\mathcal{C}$*;*

(2) if the origin is safely stabilizable on $\mathcal{C}$ *with* u_{ss} *a safe stabilizing controller, and either the condition in Theorem 5.2.3 1 holds with* $u_\star = u_{ss}$*, the condition in Theorem 5.2.3 2 holds with* $u_0 = u_{ss}$*, the condition in Theorem 5.2.3 3 holds with* $\hat{u} = u_{ss}$*, or the condition in Theorem 5.2.3 4 holds, then there exists a compatible CLF-CBF pair on* $\mathcal{C}$*;*

(3) if the origin is safely stabilizable on $\mathcal{C}$*, there exists a compatible CLF-eCBF pair on* $\mathcal{C}$*.*

Proof. **We first show 1.** Note that if the origin is safely stabilizable on $\mathcal{C}$, say with a controller $u_{\text{ss}} : \mathbb{R}^n \to \mathbb{R}^m$, by [134, Proposition 12] (using the sets $A = \mathbf{0}_n$, $W = \text{Int}(\mathcal{C})$, $U = \text{clos}(\mathbb{R}^n \backslash \mathcal{C})$, and D an open set containing $\mathcal{C}$), there exists a function $B : \mathbb{R}^n \to \mathbb{R}$ such that $\mathcal{C} = \{x \in \mathbb{R}^n : B(x) \geq 0\}$ and $\nabla B(x)^T f(x, u_{\text{ss}}) > 0$ for all $x \in \mathcal{C} \backslash \{\mathbf{0}_n\}$ (although the inequality is not defined strictly in the statement of [134, Proposition 12], the proof of this result shows that it holds strictly in $\mathcal{C} \backslash \{\mathbf{0}_n\}$. Likewise, even though the statement requires W to be compact, the proof can be easily adapted to the case where W is open but bounded by defining the constant $c = \sup_{x \in \text{clos}(W)} V(x)$). Let us now show that $\bar{V}(x) = -B(x)$ is a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$. Indeed, we have that $\bar{V}(x) > 0$ for all $x \in \mathbb{R}^n \backslash \mathcal{C}$, $\mathcal{U} = \{x \in \mathbb{R}^n : \bar{V}(x) \leq 0\} \neq \varnothing$ (since $\bar{V}(\mathbf{0}_n) \leq 0$), $\text{clos}(\mathcal{C} \backslash \mathcal{U}) \cap \text{clos}(\mathbb{R}^n \backslash \mathcal{C}) = \varnothing$, and $\nabla \bar{V}(x)^T f(x, u_{ss}(x)) < 0$ for all $x \in \mathcal{C} \backslash \{\mathbf{0}_n\}$. Furthermore, $\bar{V}$ is lower bounded and, without loss of generality, we can assume it is proper. Indeed, if it is not proper, we can add to $\bar{V}$ a radially unbounded function that is identically 0 at $\mathcal{C}$ (which exists by using partitions of unity [135, Theorem 2.33]). Hence, $\bar{V}$ is a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$.

Next, let us show that there exists a strictly compatible CLF-CBF pair in $\mathcal{C}$. We do so by using the CLBF $\bar{V}$. Since $\bar{V}$ is lower-bounded, it achieves its minimum value at a point $\mathbf{p}$. Note that $\mathbf{p}$ must be the origin, because otherwise,

by (2.12d) $\nabla\bar{V}(\mathbf{p}) \neq 0$, which would mean that $\mathbf{p}$ is not a local minimum. Let $\hat{V}(\mathbf{x}) = \bar{V}(\mathbf{x}) - \bar{V}(\mathbf{0}_n)$. Note that $\hat{V}$ is proper, positive definite and, for each $\mathbf{x} \in \mathcal{C}$, there exists a control $\mathbf{u} \in \mathbb{R}^m$ satisfying (2.5) strictly. Indeed, this follows by considering a controller $\breve{u} : \mathbb{R}^n \to \mathbb{R}^m$ satisfying $\nabla\bar{V}(\mathbf{x})^\top f(\mathbf{x}, \breve{u}(\mathbf{x})) < 0$ for all $\mathbf{x} \in \mathcal{C}\backslash\{\mathbf{0}_n\}$ and taking $W(\mathbf{x}) := -\frac{1}{2}\bar{V}(\mathbf{x})^\top f(\mathbf{x}, \breve{u}(\mathbf{x}))$ for $\mathbf{x} \neq \mathbf{0}_n$ and $W(\mathbf{0}_n) = 0$ in Definition 2.5.1. Therefore, $\hat{V}$ is a CLF. Now, let $\hat{h}(\mathbf{x}) = -\bar{V}(\mathbf{x})$. It is easy to check that $\hat{h}$ is a CBF of $\mathcal{C}$ because it is a candidate CBF of $\mathcal{C}$ and $\mathcal{C}$ is compact (cf. Theorem 2.5.4). Now, (2.5) and (2.7) read as

$$\nabla\bar{V}(\mathbf{x})^\top f(\mathbf{x}, \mathbf{u}) + W(\mathbf{x}) \leq 0, \tag{5.7a}$$

$$-\nabla\bar{V}(\mathbf{x})^\top f(\mathbf{x}, \mathbf{u}) + \alpha(-\bar{V}(\mathbf{x})) \geq 0. \tag{5.7b}$$

Now note that $\breve{u}(\mathbf{x})$ satisfies (5.7) strictly for all $\mathbf{x} \in \mathcal{C}$. Hence, $\hat{V}$ and $\hat{h}$ are a strictly compatible CLF-CBF pair.

To show 2 and 3, we reason as follows. Since u_{ss} is a safe stabilizing controller, $\mathcal{C}$ is forward invariant and the origin is asymptotically stable for the closed-loop system $\dot{\mathbf{x}} = f(\mathbf{x}, u_{\text{ss}}(\mathbf{x}))$ with $\mathcal{C}$ contained in an open set contained in its region of attraction. By [121, Theorem 4.17], there exists a Lyapunov function V for the closed-loop system $\dot{\mathbf{x}} = f(\mathbf{x}, u_{\text{ss}}(\mathbf{x}))$, and u_{ss} satisfies (2.7). Now, if condition 2 in Theorem 5.2.3 holds with $u_0 = u_{\text{ss}}$, there exists a CBF h^* of $\mathcal{C}$. As shown in the proof of Theorem 5.2.32, u_{ss} satisfies the associated CBF condition (2.7) for all $\mathbf{x} \in \mathcal{C}$. Similarly, if condition 3 in Theorem 5.2.3 holds with $\hat{u} = u_{\text{ss}}$, there exists a CBF h^* of $\mathcal{C}$. As shown in the proof of Theorem 5.2.33, u_{ss} satisfies the associated CBF condition (2.7) for all $\mathbf{x} \in \mathcal{C}$. Finally, if condition 4 in Theorem 5.2.3 holds, there exists a CBF h^* of $\mathcal{C}$, and as shown in the proof of [1, Proposition 3], any safe controller (in particular, u_{ss}) satisfies (2.7) for an appropriately defined extended class $\mathcal{K}_\infty$ function α. Hence, for every $\mathbf{x} \in \mathcal{C}$, $u_{\text{ss}}(\mathbf{x})$ satisfies inequalities (2.5) and (2.7), which means that V and h^* are compatible, showing 2.

Moreover, since $\mathcal{C}$ is safe under u_{ss}, Theorem 5.2.17 implies that there exists an eCBF $\hat{h}$ of $\mathcal{C}$. Moreover, as shown in the proof of Theorem 5.2.17, any locally Lipschitz safe controller (in particular, u_{ss}) satisfies (5.5) for all $x \in \mathcal{C}$. Since $u_{\text{ss}}(\mathbf{x})$

satisfies (2.5) and (5.5) simultaneously, V and $\hat{h}$ are a compatible CLF-eCBF pair, showing 3. □

Theorem 5.3.3 1 is consistent with Proposition 5.3.1, because it only ensures the existence of a CLBF if $\mathcal{C}$ is compact.

Remark 5.3.4. (On CLBFs and compatible pairs): It is worth noting how Theorem 5.3.3(i)-(iii) provide existence results under decreasingly restrictive hypotheses. In fact, the conditions in Theorem 5.3.3 under which a CLBF is guaranteed to exist always guarantee the existence of a compatible CLF-CBF pair, but the converse does not hold. To see this, note that from Proposition 5.3.2 and Theorem 5.3.3, that unbounded sets containing a safely stabilizable point do not admit a CLBF, but they can admit a compatible CLF-CBF pair if either of the conditions in Theorem 5.2.32, 3, or 4 hold. Instead, compact safe sets that contain a safely stabilizable point and satisfy the strict inequality condition in Theorem 5.3.3 1 for some controller admit both a CLBF and a compatible CLF-CBF pair (because if the safe set is compact the assumptions of Theorem 5.3.3 2 hold). •

Next we address problem (P3) in Section 5.1.

The following example shows that in general, even if there exists a CBF of $\mathcal{C}$ and a CLF on an open set containing $\mathcal{C}$, there might not exist a strictly compatible CLF-CBF pair in $\mathcal{C}$.

Example 5.3.5. (Safety and stability separately do not imply safe stabilization): Consider the control-affine system:

$$\dot{x} = -xu, \tag{5.8a}$$

$$\dot{y} = -yu. \tag{5.8b}$$

Let $h : \mathbb{R}^2 \to \mathbb{R}$ be a differentiable function and $\mathcal{V}$ a neighborhood of $\mathbf{p} = (0, 5)$ with the following properties:

- $h(x, y) = 1 - (x + 1)^2 - (y - 5)^2$ in $\mathcal{V}$,
- $h(0, 0) > 0$,

- $\{(x, y) \in \mathbb{R}^n : h(x, y) \geq 0\}$ is compact.

Let $\mathcal{C}$ be defined as in (2.6). The controller $u_{\text{sf}} : \mathbb{R}^2 \to \mathbb{R}$ given by $u_{\text{sf}}(x, y) = 0$ for all $(x, y) \in \mathbb{R}^2$ renders the set $\mathcal{C}$ safe. Since $\mathcal{C}$ is compact, by Theorem 5.2.3 **??** it follows that h is a CBF of $\mathcal{C}$. Moreover, the origin is globally asymptotically stabilizable, since the controller $u_{\text{st}} : \mathbb{R}^2 \to \mathbb{R}$ given by $u_{\text{st}}(x, y) = 1$ for all $(x, y) \in \mathbb{R}^2$ makes the origin globally asymptotically stable. Moreover, $V(x, y) = \frac{1}{2}(x^2 + y^2)$ is a CLF in $\mathbb{R}^2$. However, any locally Lipschitz controller $\hat{u} : \mathbb{R}^2 \to \mathbb{R}$ such that $\hat{u}(0, 5) \neq 0$ steers the trajectory starting at the point $(0, 5)$ away from $\mathcal{C}$. Indeed, note that the y axis is forward invariant and hence $x(t) = 0$ for all $t \geq 0$. Moreover, the solution of (5.8) is differentiable and by performing a Taylor expansion of first order, for time $0 < \epsilon \ll 1$, the solution of (5.8) satisfies

$$y(\epsilon) = 5 - 5u(\mathbf{p})\epsilon + O(\epsilon^2).$$

This implies that

$$h(x(\epsilon), y(\epsilon)) = -25u(\mathbf{p})^2\epsilon^2 + O(\epsilon^3),$$

and therefore $h(x(\epsilon), y(\epsilon)) < 0$ for small enough ϵ. Hence, there does not exist a safe stabilizing controller in $\mathcal{C}$. Therefore, even though h is a CBF of $\mathcal{C}$ and V is a CLF in $\mathbb{R}^2$, there does not exist a strictly compatible CLF-CBF pair. Indeed, if that were the case the control design provided in [31] would yield a safe stabilizing controller, which does not exist. Note that this example does not preclude the existence of a compatible CLF-CBF pair. However, even if such a compatible pair exists, one would not be able to use it to obtain a safe stabilizing controller. △

Note that the cause of difficulty in Example 5.3.5 is the point $\mathbf{p} = (0, 5)$, which is such that $\nabla h(x, y)^\top f(x, y, u) = 0$ for any $u \in \mathbb{R}$. Instead, using Theorem 5.3.3 1, we know that if there exists a locally Lipschitz controller $u_{\text{str}} : \mathbb{R}^n \to \mathbb{R}^m$ such that $\nabla h(\mathbf{x})^\top f(\mathbf{x}, u_{\text{str}}(\mathbf{x})) > 0$ for all $x \in \partial\mathcal{C}$, $\mathcal{C}$ is compact and there exists a safe stabilizing controller with region of attraction containing the safe set, then there exists a strictly compatible CLF-CBF pair. Note that the proof of Theorem 5.3.3 1 heavily relies on the compactness of $\mathcal{C}$. Next, we provide a similar result for non-compact $\mathcal{C}$ but restricted to control-affine systems.

Proposition 5.3.6. (Existence of compatible CLF-eCBF pair): *Given an open set* Γ *such that* $\mathcal{C} \subseteq \Gamma$*, let* h *be an eCBF of* $\mathcal{C}$ *with* 0 *as a regular value and* V *be a CLF on* Γ*. Further assume that the dynamics are control-affine, so that* $\dot{\mathbf{x}} = a(\mathbf{x}) + g(\mathbf{x})u$*, with* $a : \mathbb{R}^n \to \mathbb{R}^n$ *and* $g : \mathbb{R}^n \to \mathbb{R}^m$ *locally Lipschitz. Let* $\mathcal{P} := \{\mathbf{x} \in \mathbb{R}^n : L_g V(\mathbf{x}) = \kappa L_g h(\mathbf{x}),\ \kappa > 0\}$*. Assume that* $\mathcal{P} \cap \partial\mathcal{C}$ *is contained in*

$$\{\mathbf{x} \in \partial\mathcal{C} : L_g h(\mathbf{x}) \neq \mathbf{0}_m,\ L_a V(\mathbf{x}) < \frac{L_g V(\mathbf{x})^\top L_g h(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} L_a h(\mathbf{x})\}.$$

Then, there exists a compatible CLF-eCBF pair in $\mathcal{C}$ *with* 0 *a regular value of the eCBF.*

Proof. The proof relies on the characterization of compatibility for a CLF and a CBF, as provided in [4, Lemma 5.2], and which naturally extends to CLFs and eCBFs. This result says that V and h are compatible at $\mathbf{x} \in \mathcal{C}$ if and only if $L_g V(\mathbf{x})$ and $L_g h(\mathbf{x})$ are linearly dependent, $L_g V(\mathbf{x})^\top L_g h(\mathbf{x}) > 0$ and $L_f V(\mathbf{x}) + W(\mathbf{x}) > \frac{L_g V(\mathbf{x})^\top L_g h(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2}(L_f h(\mathbf{x}) + \alpha(h(\mathbf{x})))$. By continuity of $L_g V$ and $L_g h$, there exists a neighborhood $\mathcal{T}$ of $\partial\mathcal{C}$ such that $\mathcal{P} \cap \mathcal{T} \subseteq \{x \in \mathbb{R}^n : L_g h(\mathbf{x}) \neq \mathbf{0}_m,\ L_a V(\mathbf{x}) < \frac{L_g V(\mathbf{x})^\top L_g h(\mathbf{x})}{\|L_g h(\mathbf{x})\|^2} L_a h(\mathbf{x})\}$. By [4, Lemma 5.2], V and h are compatible in $\mathcal{C} \cap \mathcal{T}$. Next, define $\mathcal{S} = \{\mathbf{x} \in \mathcal{C} \backslash (\mathcal{T} \cup \{\mathbf{0}_n\}) : L_g V(\mathbf{x})^\top L_g h(\mathbf{x}) = \mathbf{0}_m\}$. Given $\mathbf{y} \in \mathcal{S}$, if $L_g V(\mathbf{y})$ and $L_g h(\mathbf{y})$ are linearly independent, V and h are compatible at $\mathbf{y}$ (cf. [4, Lemma 5.2]). If instead $L_g V(\mathbf{y})$ and $L_g h(\mathbf{y})$ are linearly dependent, $L_g V(\mathbf{y}) = L_g h(\mathbf{y}) = \mathbf{0}_m$ and V and h are compatible at $\mathbf{y}$ because V is a CLF and h an eCBF. Moreover, there exists a neighborhood $\bar{\mathcal{S}}$ of $\mathcal{S}$ such that V and h are compatible in $\bar{\mathcal{S}}$. This is because for any $y \in \mathcal{S}$, if $L_g V(\mathbf{y})$ and $L_g h(\mathbf{y})$ are linearly independent, there exists a neighborhood $\mathcal{V}(\mathbf{y})$ of $\mathbf{y}$ where $L_g V(\mathbf{z})$ and $L_g h(\mathbf{z})$ are linearly independent for all $\mathbf{z} \in \mathcal{V}(\mathbf{y})$, and hence by [4, Lemma 5.2], V and h are compatible at $\mathbf{z}$. If instead $L_g V(\mathbf{y})$ and $L_g h(\mathbf{y})$ are linearly dependent, we can assume without loss of generality that $L_a h(\mathbf{y}) + \alpha(h(\mathbf{y})) > 0$ and $L_a V(\mathbf{y}) + W(\mathbf{y}) < 0$ (otherwise, define $\tilde{\alpha}(s) := \frac{1}{2}\alpha(s)$ and $\tilde{W(\mathbf{x})} = \frac{1}{2}W(\mathbf{x})$), hence making V and h compatible in a neighborhood of $\mathbf{y}$. Now, we only need to show that V and h are compatible at $\mathcal{C} \backslash (\mathcal{T} \cup \bar{\mathcal{S}})$. Define $S_{r,c} := \{\mathbf{x} \in \mathbb{R}^n : 0 \leq h(\mathbf{x}) \leq r,\ \|\mathbf{x}\| \leq c + c_{\min}\}$, where $c_{\min}$ is taken

so that $S_{0,0} \neq \varnothing$, and define α as follows:

$$\alpha(r,c) := \sup_{\mathbf{x} \in S_{r,c} \backslash (\mathcal{T} \cup \bar{\mathcal{S}})} \Big\{ (L_a V(\mathbf{x}) + W(\mathbf{x})) \frac{\|L_g h(\mathbf{x})\|^2}{L_g V(\mathbf{x})^\top L_g h(\mathbf{x})} - L_a h(\mathbf{x}) \Big\}.$$

Since $S_{r,c} \backslash (\mathcal{T} \cup \bar{\mathcal{S}})$ is bounded for all $r \geq 0$, $c \geq 0$, and there exists a positive constant $\iota_{r,c} > 0$ such that $L_g V(\mathbf{x})^\top L_g h(\mathbf{x}) > \iota_{r,c}$ for all $\mathbf{x} \in S_{r,c}$, $\alpha(r,c)$ is finite for all $r \geq 0$, $c \geq 0$. Hence, there exists a class $\mathcal{K}_\infty\mathcal{K}$ function $\hat{\alpha}$ such that $\hat{\alpha}(h(\mathbf{x}), \|\mathbf{x}\|) \geq \alpha(h(\mathbf{x}), \|\mathbf{x}\|)$ for all $\mathbf{x} \in \mathcal{C} \backslash (\mathcal{T} \cup \bar{\mathcal{S}})$. Hence, by [4, Lemma 5.2], for all $\mathbf{x} \in \mathcal{C} \backslash (\mathcal{T} \cup \bar{\mathcal{S}})$ there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying

$$\begin{aligned} L_a V(\mathbf{x}) + L_g V(\mathbf{x}) \mathbf{u} + W(\mathbf{x}) &\leq 0, \\ L_a h(\mathbf{x}) + L_g h(\mathbf{x}) \mathbf{u} + \hat{\alpha}(h(\mathbf{x}), \|\mathbf{x}\|) &\geq 0, \end{aligned}$$

and hence V and h are compatible in all of $\mathcal{C}$. □

The conditions in Proposition 5.3.6 are only sufficient. In other words, there could exist weaker conditions ensuring the existence of a compatible CLF-eCBF pair.

Remark 5.3.7. (Origin at the boundary of safe set): The treatment above relies on the assumption that the origin belongs to $\mathrm{Int}(\mathcal{C})$. The extension of our results to the case when the origin is instead at $\partial\mathcal{C}$ remains an open problem. In fact, establishing whether in such case there exists a CLBF of $\mathbb{R}^n \backslash \mathcal{C}$, or a (strictly) compatible CLF-CBF pair in $\mathcal{C}$ requires facing additional technical challenges. For example, the construction of the CLBF in the proof of Theorem 5.3.3 relies on the fact that $\mathbf{0}_n$ does not belong to the set $\mathcal{T}$ and belongs to the set Π. Otherwise, the CLBF $\bar{V}$ (as defined therein) does not satisfy condition (2.12d) at the origin. •

Chapter 6

Regularity Properties of Optimization-based Controllers

In this chapter we study the regularity properties of optimization-based controllers, which are obtained by solving optimization problems where the parameter is the system state and the optimization variable is the input to the system. Under a wide range of assumptions on the optimization problem data, we provide an exhaustive collection of results about their regularity, and examine their implications on the existence and uniqueness of solutions and the forward invariance guarantees for the resulting closed-loop systems. We discuss the broad relevance of the results in different areas of systems and controls.

6.1 Motivation

Optimization-based controllers are ubiquitous in numerous areas of systems and control including safety-critical control [23], model predictive control [136, 19], and online feedback optimization [137, 138]. Optimization-based controllers are a particular class of parametric optimization problems. The theory of parametric optimization [139, 99, 140] considers optimization problems that depend on a parameter and studies the regularity properties of the minimizers with respect to it. In optimization-based control, the parameter is the state and the optimization variable is the input.

Given a dynamical system (either in discrete or continuous time) with state $\mathbf{x} \in \mathbb{R}^n$ and input $\mathbf{u} \in \mathbb{R}^m$, an optimization-based controller is a feedback law obtained by solving a problem of the form

$$\underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \; f(\mathbf{x}, \mathbf{u}) \tag{6.1a}$$

$$\text{s.t. } g(\mathbf{x}, \mathbf{u}) \leq 0 \tag{6.1b}$$

with $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ and $g : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^p$. Note that the system state $\mathbf{x}$ acts as a parameter in (6.1). Assuming that the optimizer of (6.1) is unique for every $\mathbf{x} \in \mathbb{R}^n$, this defines a function $u^\star : \mathbb{R}^n \to \mathbb{R}^m$, mapping each state to the optimizer of (6.1). This approach allows to encode desirable goals for controller synthesis both in the cost function f and in the constraints g. For instance, desirable performance objectives such as minimum control effort or maximizing convergence rate can be captured by the cost function, whereas the constraint functions can capture operational limitations on control effort and prescriptions to ensure properties such as closed-loop stability or safety. The flexibility of this synthesis approach makes it particularly attractive, but we should note the caveat that, in general, the controller $u^\star$ is not available in closed form. Instead, additional work needs to be performed in order to find the input by solving the resulting optimization problem (6.1). Independently of the computational aspects, one needs to ensure that the resulting controller behaves properly when employed to close the loop on the dynamical system, hence the importance of the study of the regularity properties of optimization-based controllers. Next we present different examples from the systems and controls literature where such controllers arise and motivate the importance of studying the regularity properties of $u^\star$.

Example 6.1.1. (Control barrier and Lyapunov function-based control): In safety-critical applications, safe controllers are often designed through control barrier functions (CBF) [23]. Let $\dot{\mathbf{x}} = F(\mathbf{x}, \mathbf{u})$ be a control system with $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ locally Lipschitz. Assume that the set of safe states is given by the 0-superlevel set of a continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$, and suppose that h is a CBF. Given a nominal controller $k : \mathbb{R}^n \to \mathbb{R}^m$, designed with desirable properties such as asymptotic stability of an equilibrium point or minimizing a certain infinite-

horizon optimal control cost, *safety filters*, as introduced in Chapter 4, seek to find the controller closest to k that satisfies the CBF constraint. Such controller can be found at every state $\mathbf{x} \in \mathbb{R}^n$ by solving the following optimization problem:

$$u_{\text{sf}}^\star(\mathbf{x}) = \underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \ \frac{1}{2}\left\|\mathbf{u} - k(\mathbf{x})\right\|^2, \tag{6.2a}$$

$$\text{s.t. } \nabla h(\mathbf{x})^\top F(\mathbf{x},\mathbf{u}) + \alpha(h(\mathbf{x})) \geq 0, \tag{6.2b}$$

where $\alpha : \mathbb{R} \to \mathbb{R}$ is an extended class $\mathcal{K}$ function. Note that (6.2) is a special case of (6.1). Often, one also seeks to endow safety filters with stability guarantees by employing CLFs. Given a CLF $V : \mathbb{R}^n \to \mathbb{R}$, one can seek to endow u_{sf} with stability guarantees by solving the following optimization problem at every $x \in \mathbb{R}^n$:

$$u_{\text{cc}}^\star(\mathbf{x}) = \underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \ \frac{1}{2}\left\|\mathbf{u} - k(\mathbf{x})\right\|^2, \tag{6.3a}$$

$$\text{s.t. } \nabla h(\mathbf{x})^T F(\mathbf{x},\mathbf{u}) + \alpha(h(\mathbf{x})) \geq 0, \tag{6.3b}$$

$$\nabla V(\mathbf{x})^T F(\mathbf{x},\mathbf{u}) + W(\mathbf{x}) \leq 0, \tag{6.3c}$$

Note that (6.3) is a special case of (6.1). Other similar optimization-based control designs of the form (6.1) leveraging CLFs and CBFs have been proposed in [1, 4, 119, 38, 141, 43, 142, 9], among many others. If the system is control-affine, as it is often the case in practice, then (**??**) and (6.3) are quadratic programs (QPs). Importantly, $u_{\text{sf}}^\star$ (resp. $u_{\text{cc}}^\star$) is only guaranteed to be safe (resp. safe and stable) if it is locally Lipschitz. Hence, studying the regularity properties of (**??**) and (6.3) is critical to ensure that the closed-loop system has the desired safety and/or stability properties. Moreover, if $u^\star$ is locally Lipschitz, then the right-hand side of $\dot{\mathbf{x}} = F(\mathbf{x}, u^\star(\mathbf{x}))$ is locally Lipschitz too, and then the Picard-Lindelöf theorem [143, Theorem 2.2] guarantees existence and uniqueness of solutions for small enough times. Similar regularity properties are also relevant in the study of the contraction properties of optimization-based controllers of the form (**??**) and (6.3), as shown in [144]. •

Example 6.1.2. (Online feedback optimization): Here we describe the problem of optimally regulating the steady-state output of a plant, a task often referred

to as *online feedback optimization* [137, 138]. This problem arises in a variety of application areas including power systems [145, 146], network congestion control [147], and traffic networks [148]. In a typical set-up, the plant is modeled with the dynamics

$$\begin{aligned} \dot{\mathbf{x}} &= F(\mathbf{x}, \mathbf{u}) \\ \mathbf{y} &= G(\mathbf{x}, \mathbf{u}) \end{aligned} \tag{6.4}$$

where $G : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^k$ and $\mathbf{y} \in \mathbb{R}^k$ denote the output. We assume that there exists a map $h : \mathbb{R}^m \to \mathbb{R}^k$, called the *steady-state map*, such that for each constant input $\mathbf{u} \in \mathbb{R}^m$ and initial condition $\mathbf{x}_0 \in \mathbb{R}^n$, the corresponding output of (6.4) satisfies $y(t) \to h(\mathbf{u})$ as $t \to \infty$. Consider the problem of driving the output to an optimal steady-state, formalized by the optimization

$$\min_{\mathbf{u} \in \mathbb{R}^m, \mathbf{y} \in \mathbb{R}^k} \quad \Phi(\mathbf{u}, \mathbf{y}) \tag{6.5a}$$

$$\text{s.t.} \quad (\mathbf{u}, \mathbf{y}) \in \mathcal{U} \times \mathcal{Y} \tag{6.5b}$$

$$\mathbf{y} = h(\mathbf{u}), \tag{6.5c}$$

where $\mathcal{Y} \subset \mathbb{R}^k$ denotes the set of valid outputs, $\mathcal{U} \subset \mathbb{R}^m$ denotes the set of valid inputs, and $\Phi : \mathbb{R}^m \times \mathbb{R}^k \to \mathbb{R}$ denotes the cost of the corresponding input-output pair. The problem can equivalently be viewed as an optimization over a set of inputs alone by eliminating the variable y from (6.5):

$$\min_{\mathbf{u} \in \mathbb{R}^m} \quad \Phi(\mathbf{u}, h(\mathbf{u})) \tag{6.6a}$$

$$\text{s.t.} \quad (\mathbf{u}, h(\mathbf{u})) \in \mathcal{U} \times \mathcal{Y}. \tag{6.6b}$$

Note that (6.5) and (6.6) are "static" problems, i.e., the state of the plant does not appear in the cost function or the constraints as a parameter. In practice, however, the steady-state map and the plant dynamics are only partially known, and subject to external disturbances or model uncertainties. This precludes one from directly solving either problem offline and simply applying the resulting input to (6.4) (this strategy is called *feedforward optimization*). Instead, one turns the "static" formulation into a "dynamic" one by solving the problem online and using real-time measurements of the output of the plant in place of a closed-form expression

of the steady-state output. Formally, this amounts to replacing the expression $\mathbf{y}$ in (6.5), or $h(\mathbf{u})$ in (6.6), with $G(\mathbf{x}, \mathbf{u})$:

$$u^*_{\text{ofo}}(\mathbf{x}) = \underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \quad f(\mathbf{x}, \mathbf{u}) := \Phi(\mathbf{u}, G(\mathbf{x}, \mathbf{u})) \tag{6.7a}$$

$$\text{s.t.} \qquad \mathbf{u} \in \mathcal{U} \tag{6.7b}$$

$$G(\mathbf{x}, \mathbf{u}) \in \mathcal{Y}. \tag{6.7c}$$

The idea is that at each time instant, the output measurement is obtained online and fed back into (6.7), hence this strategy is called *online feedback optimization*. We note that (6.7) is of the form (6.1), by rewriting the input and output set inclusions as inequalities as in (6.1). In this setting, understanding the regularity properties of the closed-loop dynamics $\dot{\mathbf{x}} = F(\mathbf{x}, u^*_{\text{ofo}}(\mathbf{x}))$ becomes necessary to ensure good performance of implementing (6.7) on a physical plant. Letting u_{ss} denote the solution to (6.6), one would be interested, for instance, in showing that $u^*_{\text{ofo}}(x(t)) \to \mathbf{u}_{\text{ss}}$ and $y(t) \to h(\mathbf{u}_{\text{ss}})$ as $t \to \infty$. also note that if the cost function in (6.5) is time-varying, the resulting "dynamic" formulation (6.7) is also time-varying. However, the added time-dependence can be treated as an extra parameter in the optimization problem (6.7), and therefore the results outlined in this paper can also be applied in such time-dependent settings. •

Example 6.1.3. (Optimization algorithms as dynamical systems): Optimization algorithms can be viewed from the lens of dynamical systems [149, 150, 151]. In some cases, such dynamical systems are designed using ideas from optimization-based control. Here we discuss the *safe gradient flow* [98]. Consider a constrained optimization problem of the form

$$\min_{\mathbf{x}\in\mathbb{R}^n} \quad \bar{f}(\mathbf{x}), \tag{6.8a}$$

$$\text{s.t.} \qquad \bar{g}(\mathbf{x}) \leq 0 \tag{6.8b}$$

where $\bar{f} : \mathbb{R}^n \to \mathbb{R}$ and $\bar{g} : \mathbb{R}^n \to \mathbb{R}^m$ are continuously differentiable functions with Lipschitz continuous gradients, and $\frac{\partial \bar{g}}{\partial \mathbf{x}}$ has full rank for all $\mathbf{x} \in \mathbb{R}^n$. We consider the problem of designing a continuous-time dynamical system such that the feasible set $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n \mid \bar{g}(\mathbf{x}) \leq \mathbf{0}_m\}$ is forward invariant and trajectories converge to

solutions to (6.8). To solve this problem, we consider the integrator system,

$$\dot{\mathbf{x}} = F(\mathbf{x}, \boldsymbol{\xi}) = \boldsymbol{\xi}, \tag{6.9}$$

along with the feedback controller

$$\xi_\alpha^*(\mathbf{x}) = \underset{\boldsymbol{\xi}\in\mathbb{R}^n}{\operatorname{argmin}} \ \frac{1}{2}\left\|\boldsymbol{\xi} + \nabla \bar{f}(\mathbf{x})\right\|^2 \tag{6.10a}$$

$$\text{s.t} \quad \frac{\partial \bar{g}(\mathbf{x})}{\partial \mathbf{x}}\boldsymbol{\xi} \leq -\alpha \bar{g}(\mathbf{x}), \tag{6.10b}$$

where $\alpha > 0$ is a design parameter. The closed-loop dynamics are referred to as the *safe gradient flow* (cf. [98, Section IV.A] for an alternative derivation of the safe gradient flow using techniques from the theory of control barrier functions). We note again that (6.10) is of the form (6.1). Establishing regularity properties of ξ_α^* such as continuity or local Lipschitzness is critical for the solutions of (6.10) to exist and be unique. These properties are then leveraged to study the convergence of the solutions of (6.10) to the optimizers of (6.8) while ensuring that the feasible set is forward invariant. •

Example 6.1.4. (Projected Dynamical Systems): Projected dynamical systems are a class of systems whose evolution is constrained to remain inside a subset $\mathcal{C} \subset \mathbb{R}^n$. They are are widely used for analyzing and solving nonlinear programs and variational inequalities [152] and have wide-ranging applications including network economics (e.g., for analyzing supply chain networks or financial markets) [153], power networks [145, 154], anti-windup controllers for feedback optimization [155], and traffic flows [156], to name a few. While projected dynamical systems have been considered in quite general settings, such as on Riemmanian manifolds [157], or with respect to oblique projections [158], here we restrict ourselves to the Euclidean case. In this case, projected dynamical systems typically take the form

$$\dot{\mathbf{x}} = \Pi_{\mathcal{C}}[\mathbf{x}, H(\mathbf{x})] \tag{6.11}$$

where $H : \mathbb{R}^n \to \mathbb{R}^n$ is a vector field, and $\mathbf{v} \mapsto \Pi_{\mathcal{C}}[\mathbf{x}, \mathbf{v}]$ is the projection onto the tangent cone of $\mathcal{C}$:

$$\Pi_{\mathcal{C}}[\mathbf{x}, \mathbf{v}] = \operatorname{proj}_{T_{\mathcal{C}}(\mathbf{x})}(\mathbf{v}).$$

Recently, projected dynamical systems have been reinterpreted from the viewpoint of control theory, to design anytime flows solving variational inequalities [159], and for understanding their relationship to controllers obtained using techniques from the theory of control barrier functions [160]. For example, (6.11) can be interpreted as the closed-loop dynamics corresponding to the system,

$$\dot{\mathbf{x}} = H(\mathbf{x}) + \mathbf{u} \tag{6.12}$$

with the feedback controller

$$u^*_{\text{proj}}(\mathbf{x}) = \underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \|\mathbf{u}\|^2 \tag{6.13a}$$

$$\text{s.t.} \quad H(\mathbf{x}) + \mathbf{u} \in T_{\mathcal{C}}(\mathbf{x}). \tag{6.13b}$$

Even though feedback controllers of the form (6.13) are discontinuous, the resulting closed-loop system may still be well behaved. In the case where $\mathcal{C}$ is convex, one can show existence and uniqueness [152, Theorem 2.5] of Carathéodory solutions (cf. [161] for notions of solutions to discontinuous systems), and forward invariance of the set $\mathcal{C}$ [162, Corollary 4.8]. With the additional assumption of strong monotonicity of H, asymptotic stability of the unique equilibrium (6.11) follows as well. The control-theoretic interpretation of projected dynamical systems highlights the complex relationship between the regularity properties of optimization-based feedback controllers and the dynamical properties of the resulting closed-loop system. In particular, it shows that from the perspective of control design, a feedback controller may achieve its intended objective (e.g., ensuring invariance of a safe set or stabilization to a desired equilibrium point) with relatively weak regularity properties. •

Example 6.1.5. (Model predictive control): Here we explain how (6.1) is also applicable to model predictive controllers. Consider a discrete-time dynamical system

$$\mathbf{x}^+ = F(\mathbf{x}, \mathbf{u}), \tag{6.14}$$

where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{u} \in \mathbb{R}^m$. We consider the problem of optimally controlling (6.14) to minimize a running cost $\ell(\mathbf{x}, \mathbf{u})$ while ensuring the state and input satisfy constraints $\mathbf{x} \in \mathcal{X} \subset \mathbb{R}^n$ and $\mathbf{u} \in \mathcal{U} \subset \mathbb{R}^m$. Model predictive control is a method for

solving this problem by solving a finite-horizon optimal control problem and implementing its solution over (6.14) in a receding horizon fashion. Here we show that model predictive control schemes can be interpreted as a discrete-time analog of optimization-based feedback control discussed in previous examples. Let $N > 0$ be a time horizon, and $\mathbf{x} = (\hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1, \dots, \hat{\mathbf{x}}_N) \in \mathbb{R}^{n(N+1)}$ and $\mathbf{u} = (\hat{\mathbf{u}}_0, \hat{\mathbf{u}}_1, \dots, \hat{\mathbf{u}}_{N-1}) \in \mathbb{R}^{mN}$ denote the state and input prediction sequences over the time horizon. Consider the following optimization problem

$$\mathbf{u}^*_{\text{mpc}}(\mathbf{x}) = \underset{\mathbf{u},\mathbf{x}}{\text{argmin}} \quad V_N(\hat{\mathbf{x}}_N) + \sum_{k=0}^{N-1} \ell(\hat{\mathbf{x}}_k, \hat{\mathbf{u}}_k) \tag{6.15a}$$

$$\text{s.t.} \qquad \hat{\mathbf{x}}_{k+1} = F(\hat{\mathbf{x}}_k, \hat{\mathbf{u}}_k) \tag{6.15b}$$

$$\hat{\mathbf{x}}_k \in \mathcal{X}, \ \hat{\mathbf{u}}_k \in \mathcal{U} \tag{6.15c}$$

$$\hat{\mathbf{x}}_N \in \mathcal{X}_f \tag{6.15d}$$

$$\hat{\mathbf{x}}_0 = \mathbf{x} \tag{6.15e}$$

$$k \in \{0, \cdots, N-1\}, \tag{6.15f}$$

where $V_N : \mathbb{R}^n \to \mathbb{R}$ and $\mathcal{X}_f \subset \mathbb{R}^n$ denote the terminal cost and terminal constraint respectively (we refer the reader to [19] for conditions on these ingredients to ensure closed-loop stability.) Next, consider the augmented system

$$\mathbf{x}^+ = \bar{F}(\mathbf{x}, \mathbf{u}) = F(\mathbf{x}, \hat{\mathbf{u}}_0), \tag{6.16a}$$

which simply corresponds to implementing the first input in the sequence $\mathbf{u}$ to (6.14). Note that (6.15) is a parametric optimization problem, where the parameter corresponds to the current state $\mathbf{x}$. Model predictive control studies the closed-loop system obtained by the dynamics (6.16) and the controller (6.15). As shown in [163], establishing the continuity properties of (6.15) is critical in proving stability and robustness properties of MPC-based controllers. •

As motivated by the examples provided above, studying the regularity properties of $u^\star$ is critical in order to establish different properties of interest for the closed-loop system, such as

(1) existence and uniqueness of solutions (for different notions of solution, such as classical, Carathéodory, and Filippov);

(2) dynamical properties such as forward invariance of safe sets or stabilization to an equilibrium point;

(3) convergence of optimization algorithms such as the safe gradient flow;

(4) good performance of online feedback optimization-based controllers;

(5) stability and robustness properties of MPC based controllers.

Additionally, from a practical point of view, guaranteeing regularity properties for $u^\star$ such as continuity or local Lipschitzness is useful to ease the implementation of such controllers on digital platforms and avoid chattering behavior.

We should point out that the importance of characterizing the regularity properties of (6.1) has already been noticed in the literature, and there are a variety of works in the literature [32, 164, 12, 13] and [19, Theorem 2.7] that use the theory of parametric optimization to guarantee local Lipschitz continuity or other regularity properties of optimization-based controllers. For example, the results in [32] give different conditions that ensure continuity and continuous differentiability of optimization-based controllers. However, they either require the rather strong assumption of *strict complementary slackness*, which is not satisfied in many cases of interest, or are limited to quadratic programs that satisfy a set of technical conditions. The paper [32] also revisits Robinson's counterexample, first introduced in [165], in the context of optimization-based control, which shows that even for optimization problems defined by well-behaved data (e.g., second-order continuously differentiable objective function and constraints, strongly convex objective function, and feasible set with non-empty interior, which are widely employed in the design of safe and stabilizing controllers, cf. Example 6.1.1), the resulting controller might not be locally Lipschitz. The result in [164, Theorem 3] is more general but only ensures continuity under *Slater's condition* and other regularity properties on the optimization problem. The regularity results in our previous work [12, 13] establish different Lipschitz continuity results for second-order convex programs, but are limited to this specific type of optimization problems. Finally, [19, Theorem 2.7] only guarantees continuity of optimization-based controllers derived from MPC. We also note that in some cases, $u^\star$ can be computed

in closed-form, in which case the regularity properties of $u^\star$ can be evaluated directly without having to resort to the theory of parametric optimization. Examples of such explicitly computable optimization-based controllers are provided in [118, 4, 119, 166] and [19, Chapter 7]. We would also like to point out that even though this work is mostly focused on control laws obtained as the solution of optimization problems of the form (6.1), the regularity properties of other control designs has also been studied in the literature. For example, the celebrated Sontag's Universal Formula [167] provides a smooth control law for stabilization of control-affine systems. More recently, similar designs have been given in the context of safety-critical control [168, 12, 169, 31].

Our main goal in writing this chapter is to provide an integrative presentation of insights and results about the regularity of optimization-based controllers. We present in Table 6.1 a comprehensive collection of results that offers the reader interested in using optimization-based controllers a one-stop destination to assess the regularity properties of their control design. We present here several results from the literature, but restated here for completeness from the perspective of optimization-based control. The chapter also contains many novel results that help fill gaps in the state of the art.

In what follows, we assume that the control system operates in continuous time and is given by

$$\dot{\mathbf{x}} = F(\mathbf{x}, \mathbf{u}), \tag{6.17}$$

where $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is locally Lipschitz. Hence, the closed-loop system takes the form

$$\dot{\mathbf{x}} = F(\mathbf{x}, u^\star(\mathbf{x})). \tag{6.18}$$

6.2 Regularity of Parametric Optimizers

In this section we discuss how the assumptions on the functions f and g defining (6.1) affect the regularity properties of the resulting controller $u^\star$. Throughout this section, we assume that f and g belong to $\mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$, $f(\mathbf{x}, \cdot)$ is strictly

convex for all $\mathbf{x} \in \mathbb{R}^n$ (for some specific results, we further assume that $f(\mathbf{x}, \cdot)$ is strongly convex for all $\mathbf{x} \in \mathbb{R}^n$, but we make it explicit if this is the case) and $g(\mathbf{x}, \cdot)$ is convex for all $\mathbf{x} \in \mathbb{R}^n$. We further assume that, for each $\mathbf{x} \in \mathbb{R}^n$, (6.1) has at least one minimizer (note that if $f(\mathbf{x}, \cdot)$ is strongly convex for all $\mathbf{x} \in \mathbb{R}^n$, this holds if (6.1) is feasible for all $\mathbf{x} \in \mathbb{R}^n$). By the convexity assumptions described above, this implies that $u^*(\mathbf{x})$ is a singleton for every $\mathbf{x} \in \mathbb{R}^n$. Furthermore, the assumptions on convexity also ensure that for each $\mathbf{x} \in \mathbb{R}^n$, *interior-point algorithms* [174] can be used to solve (6.1), which run in polynomial time when the optimization problem is a linear program, a quadratic program, a second-order convex program, or a semidefinite program.

This type of assumptions are very common, for instance, in CBF-based QPs, (cf. Example 6.1.1), or in model predictive controllers for linear systems (cf. Example 6.1.5), for which there also exist specific algorithms that solve them efficiently [175].

First, we gather a few existing results from the literature:

Continuity: Under the assumption that MFCQ holds at $(\mathbf{x}, u^*(\mathbf{x}))$, the parametric solution u^* is continuous [173, Theorem 5.3].

Local Lipschitzness: Under the assumption that both MFCQ and CR hold at $(\mathbf{x}, u^*(\mathbf{x}))$, the parametric solution u^* is locally Lipschitz [172, Theorem 3.6]. The same conclusion can be obtained if LICQ holds [171, Theorem 4.1] at $(\mathbf{x}, u^*(\mathbf{x}))$. We note also that since the satisfaction of LICQ implies the satisfaction of MFCQ and CR (cf. [172, Proposition 3.1]), [172, Theorem 3.6] is stronger than [171, Theorem 4.1].

Continuous Differentiability: Under the assumptions of LICQ and SCS, the parametric solution u^* is continuously differentiable [170, Theorem 2.1]. This last point was already noted in the optimization-based control literature in [32, Theorem 1]. In fact, if f and g belong to $\mathcal{C}^p(\mathbb{R}^n \times \mathbb{R}^m)$, with $p \in \mathbb{Z}_{>0}, p \geq 2$, the proof of [170, Theorem 2.1] can be adapted using the Implicit Function Theorem for higher degree of differentiability [176, Proposition 1B.5], to show that the parametric optimizer belongs to $\mathcal{C}^{p-1}(\mathbb{R}^n)$.

Analyticity: Similarly, if f and g are analytic in $\mathbb{R}^n$, then the proof of [170, Theorem 2.1] can be adapted using the Analytic Function Theorem [177, Theorem 3.3.2], to show that the parametric optimizer is analytic in $\mathbb{R}^n$.

If the constraint qualifications given above for the case of local Lipschitzness do not hold, the parametric optimizer can fail to be locally Lipschitz. To illustrate this, we revisit next an example due to Robinson [165].

Example 6.2.1. (Robinson's Counterexample): In [165], Robinson introduces the following parametric optimization problem: for $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$, consider

$$\min_{\mathbf{u}\in\mathbb{R}^4} \quad \frac{1}{2}\mathbf{u}^\top\mathbf{u} \tag{6.19a}$$

$$\text{s.t.} \quad A(\mathbf{x})\mathbf{u} \geq b(\mathbf{x}) \tag{6.19b}$$

where

$$A(\mathbf{x}) = \begin{bmatrix} 0 & -1 & 1 & 0, \\ 0 & 1 & 1 & 0, \\ -1 & 0 & 1 & 0, \\ 1 & 0 & 1 & x_1 \end{bmatrix}, \quad b(\mathbf{x}) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 + x_2 \end{bmatrix}.$$

Problem (6.19) is a quadratic program with strongly convex objective function, smooth objective function and constraints, and for which Slater's condition holds for every value of the parameter (this can be shown by noting that $\hat{u} = (0, 0, 2 + |x_2|, 0)$ satisfies all constraints strictly). Despite these nice properties, the parametric solution of (6.19) is not locally Lipschitz at $(x_1, x_2) = (0, 0)$. Indeed, let $u^\star : \mathbb{R}^2 \to \mathbb{R}^4$ denote the parametric solution of (6.19), and $u_4^\star : \mathbb{R}^2 \to \mathbb{R}$ its fourth component, which is given by

$$u_4^*(x_1, x_2) = \begin{cases} 0 & \text{if } x_2 \leq 0, \\ \frac{x_2}{x_1} & \text{if } x_2 \geq 0,\ x_1 \neq 0, \frac{x_1^2}{2} \geq x_2, \\ \frac{x_1(x_2+1)}{x_1^2+2} & \text{otherwise.} \end{cases}$$

We plot $u_4^\star$ in Figure 6.1. For $s \geq 0$, let $p(s) = (s, s^2/2)$ and $q(s) = (s, 0)$. Then, observe that $p(s)$ and $q(s)$ approach the origin as $s \to 0^+$, however,

$$\frac{\|u_4^*(p(s)) - u_4^*(q(s))\|}{\|p(s) - q(s)\|} = \frac{1}{s}.$$

Since the right hand side of the previous expression can be made arbitrarily large by choose s sufficiently small, it follows that u^* is not locally Lipschitz at the origin. We also note that [172, Example 3.11] gives a similar example for a parametric quadratic program with a two-dimensional optimization variable, three-dimensional parameter, strongly convex objective function, smooth objective function and constraints, and for which Slater's condition holds for every value of the parameter and the corresponding parametric optimizer also fails to be locally Lipschitz. •

Even though Example 6.2.1 shows that the parametric optimizer of (6.19) is not locally Lipschitz, it actually satisfies a set of weaker regularity properties. The following result characterizes them, in the general setting of optimization problems satisfying the same conditions as (6.19).

Proposition 6.2.2. (Regularity Properties of Parametric Optimizer): *Suppose that f and g belong to $\mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$. Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $g(\mathbf{x}, \cdot)$ is convex. Suppose that SC holds at $\mathbf{x}_0 \in \mathbb{R}^n$. Then,*

(1) if $f(\mathbf{x}, \cdot)$ is strongly convex for all $\mathbf{x} \in \mathbb{R}^n$, there exists a neighborhood $\mathcal{V}_{\mathbf{x}_0}$ of $\mathbf{x}_0$ such that u^* is point-Lipschitz at $\mathbf{y}$ for all $\mathbf{y} \in \tilde{\mathcal{V}}_{\mathbf{x}_0}$;

(2) if $f(\mathbf{x}, \cdot)$ is strongly convex for all $\mathbf{x} \in \mathbb{R}^n$, u^* has the Hölder property at $\mathbf{x}_0$;

(3) if $f(\mathbf{x}, \cdot)$ is strictly convex for all $\mathbf{x} \in \mathbb{R}^n$ and (6.1) has at least one minimizer for all $\mathbf{x} \in \mathbb{R}^n$, u^* is directionally differentiable at $\mathbf{x}_0$.

Proof. First we note that since in 1 and 2, $f(\mathbf{x}_0, \cdot)$ is strongly convex, and in 3 $f(\mathbf{x}_0, \cdot)$ is strictly convex and (6.1) has at least one minimizer at $\mathbf{x}_0$, it follows that in all of 1, 2, 3, $u^*(\mathbf{x}_0)$ is unique and well-defined for all $\mathbf{x}_0 \in \mathbb{R}^n$.

To prove 1 we use [99, Theorem 6.4]. Since SC holds at $\mathbf{x}_0$, by [178, Prop. 5.39], since $g(\mathbf{x}_0, \cdot)$ is convex, MFCQ holds at $(\mathbf{x}_0, u^*(\mathbf{x}_0))$. Furthermore, since $f(\mathbf{x}_0, \cdot)$ is strongly convex and $g(\mathbf{x}_0, \cdot)$ is convex, the second-order condition SOC2 [99, Definition 6.1] holds (note that SOC2 is not guaranteed to hold if $f(\mathbf{x}_0, \cdot)$ is only strictly convex). All of this, together with the twice continuous differentiability of f and g imply, by [99, Theorem 6.4], that u^* is point-Lipschitz at $\mathbf{x}_0$. Now, since

g is continuous, there exists a neighborhood $\mathcal{V}_{\mathbf{x}_0}$ of $\mathbf{x}_0$ such that SC holds for all $\mathbf{y} \in \mathcal{V}_{\mathbf{x}_0}$. By repeating the same argument, u^* is point-Lipschitz at $\mathbf{y}$ for all $\mathbf{y} \in \mathcal{V}_{\mathbf{x}_0}$.

Now let us prove 2. We use [179, Theorem 2.1], which gives a sufficient condition for the solution of a variational inequality to have the Hölder property. Recall that given a map $F : \mathbb{R}^m \to \mathbb{R}^m$, and a constraint set $\bar{\mathcal{C}} \subset \mathbb{R}^m$, a variational inequality refers to the problem of finding $\mathbf{u}^* \in \bar{\mathcal{C}}$ such that $(\mathbf{u} - \mathbf{u}^*)^T F(\mathbf{u}^*) \geq 0$ for all $\mathbf{u} \in \bar{\mathcal{C}}$. For every fixed $\mathbf{x} \in \mathbb{R}^n$, by taking the map F to be the gradient of f with respect to $\mathbf{u}$ at $\mathbf{x}$, and by taking $\bar{\mathcal{C}}$ to be the constraint set of (6.1) at $\mathbf{x}$, a constrained optimization problem of the form (6.1) can be posed as a variational inequality, cf. [180]. Since f is twice continuously differentiable and $f(\mathbf{x}_0, \cdot)$ is strongly convex, conditions (2.1) and (2.2) in [179, Theorem 2.1] hold. Note that condition (2.2) in [179, Theorem 2.1] is not guaranteed to hold if $f(\mathbf{x}_0, \cdot)$ is only strictly convex. Moreover, since MFCQ holds at $(\mathbf{x}_0, u^*(\mathbf{x}_0))$ (because SC holds), by [181, Remark 3.6] the constraint set is pseudo-Lipschitzian [179, Definition 1.1]. All of this implies by [179, Theorem 2.1] that u^* has the Hölder property at $\mathbf{x}_0$.

Finally, 3 follows from the fact that SC implies MFCQ and [182, Theorem 1]. Note that in this case, the assumptions of [182, Theorem 1] are satisfied by only requiring that $f(\mathbf{x}, \cdot)$ is strictly convex for all $\mathbf{x} \in \mathbb{R}^n$, instead of strongly convex for all $\mathbf{x} \in \mathbb{R}^n$. □

In Proposition 6.2.2, note that neither 1 implies 2 nor the converse. Even though the parametric optimizer in Robinson's counterexample is not locally Lipschitz, Proposition 6.2.2 shows that it enjoys other, slightly weaker, regularity properties. In particular, this result implies that $u_4^\star$, the fourth component of the parametric optimizer of Robinson's counterexample, is continuous, cf. Figure 6.1.

Proposition 6.2.2 also clarifies a confusion that has arisen in the literature due to the loose use of terminology. Indeed, according to [99, Theorem 6.4], a parametric optimization problem whose data satisfies the properties of Robinson's counterexample has a Lipschitz minimizer! This apparent contradiction is rooted in different notions of Lipschitzness. Indeed, the notion of Lipschitzness used in [99, Theorem 6.4] corresponds to point-Lipschitzness.

Next we show that in the special case of parametric quadratic programs that

satisfy the assumptions of Proposition 6.2.2 with a scalar optimization variable, the parametric optimizer is locally Lipschitz.

Proposition 6.2.3. (Scalar parametric quadratic programs have locally Lipschitz optimizers): *Suppose that* $f \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^1)$ *and and for* $i \in [p]$, *let* $g_i^0 : \mathbb{R}^n \to \mathbb{R}$, $g_i^1 : \mathbb{R}^n \to \mathbb{R}$ *belong to* $\mathcal{C}^2(\mathbb{R}^n)$ *and*

$$g(\mathbf{x}, \mathbf{u}) = \begin{pmatrix} g_1^0(\mathbf{x})\mathbf{u} + g_1^1(\mathbf{x}) \\ \vdots \\ g_i^0(\mathbf{x})\mathbf{u} + g_i^1(\mathbf{x}) \\ \vdots \\ g_p^0(\mathbf{x})\mathbf{u} + g_p^1(\mathbf{x}) \end{pmatrix}.$$

Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $f(\mathbf{x}, \cdot)$ *is strictly convex and* (6.1) *has at least one minimizer. Suppose that SC holds at* $\mathbf{x}_0 \in \mathbb{R}^n$. *Then,* u^* *is locally Lipschitz at* $\mathbf{x}_0$.

Proof. First, since (6.1) has at least one minimizer for all $\mathbf{x} \in \mathbb{R}^n$, the convexity assumptions of f and g imply that u^* is a singleton for all $\mathbf{x} \in \mathbb{R}^n$. Note that for all $i \in \mathcal{I}(\mathbf{x}_0, u^*(\mathbf{x}_0))$, $g_i^0(\mathbf{x}_0) \neq 0$. Indeed, if $g_i^0(\mathbf{x}_0) = 0$ and $i \in \mathcal{I}(\mathbf{x}_0, u^*(\mathbf{x}_0))$, it follows that $g_i^1(\mathbf{x}_0) = 0$, which implies that Slater's condition at $\mathbf{x}_0$ is violated. Hence, $g_i^0(\mathbf{x}_0) \neq 0$ for all $i \in \mathcal{I}(\mathbf{x}_0, u^*(\mathbf{x}_0))$ and the CR holds at $(\mathbf{x}_0, u^*(\mathbf{x}_0))$. Moreover, since Slater's condition holds at $\mathbf{x}_0$, by [178, Prop. 5.39], since $g(\mathbf{x}_0, \cdot)$ is convex, MFCQ holds at $(\mathbf{x}_0, u^*(\mathbf{x}_0))$. By [172, Theorem 3.6], this implies that u^* is locally Lipschitz at $\mathbf{x}_0$. □

Note that Robinson's counterexample or [172, Example 3.11] do not contradict Proposition 6.2.3, since in those two examples the optimization variable of the quadratic program has dimensions four and two, respectively.

Proposition 6.2.3 shows that optimization-based controllers for single-input systems with affine constraints (e.g., obtained from CBF or CLF based conditions for control-affine systems) that satisfy Slater's conditions are locally Lipschitz.

The following examples show that the results from Proposition 6.2.2 do not hold if the assumptions are weakened, even slightly.

Example 6.2.4. (Not point-Lipschitz optimizer without differentiability of problem data with respect to the parameter): If f and g are not differentiable with respect to the parameter $\mathbf{x}$ but the rest of the assumptions of Proposition 6.2.2 hold (even with $f(\mathbf{x},\cdot)$ strongly convex for all $\mathbf{x} \in \mathbb{R}^n$), the following example, inspired by Robinson's counterexample, shows that the parametric optimizer is not necessarily point-Lipschitz. Let $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ and consider (6.19) with

$$A(\mathbf{x}) = \begin{bmatrix} 0 & -1 & 1 & 0, \\ 0 & 1 & 1 & 0, \\ -1 & 0 & 1 & 0, \\ 1 & 0 & 1 & \sqrt{|x_1|} \end{bmatrix}, \quad b(\mathbf{x}) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 + x_2 \end{bmatrix}.$$

Let $\tilde{u}^\star : \mathbb{R}^2 \to \mathbb{R}^4$ be its parametric solution and let $\tilde{u}_4^\star : \mathbb{R}^2 \to \mathbb{R}$ denote its fourth component, which is given by

$$\tilde{u}_4^\star(\mathbf{x}) = \begin{cases} 0 & \text{if } x_2 \leq 0, \\ \frac{x_2}{\sqrt{|x_1|}} & \text{if } x_2 \geq 0,\ x_1 \neq 0, \frac{|x_1|}{2} \geq x_2, \\ \frac{\sqrt{|x_1|}(x_2+1)}{|x_1|+2} & \text{otherwise.} \end{cases}$$

Let $x_1 > 0$ and define $\mathbf{p}_{x_1} = (x_1, \frac{|x_1|}{2})$. Note that

$$\frac{\|\tilde{u}_4^\star(\mathbf{p}_{x_1}) - \tilde{u}_4^\star(0)\|}{\|\mathbf{p}_{x_1} - 0\|} = \frac{1}{\sqrt{5|x_1|}}.$$

Since x_1 can be taken to be arbitrarily small, $\tilde{u}^\star$ is not point-Lipschitz at the origin. However, because f and g, as well as their first and second derivatives with respect to $\mathbf{u}$, are continuous in $\mathbf{u}$ and $\mathbf{x}$, and the rest of assumptions of Proposition 6.2.2 hold (with $f(\mathbf{x},\cdot)$ strongly convex for all $\mathbf{x} \in \mathbb{R}^n$), then by [173, Theorem 5.3], the corresponding parametric optimizer, and hence $\tilde{u}_4^\star$, is continuous. •

Example 6.2.5. (Discontinuous optimizer without Slater's condition): The following example, taken from [32, Section VI], shows that if Slater's condition does not hold, then continuity of the parametric optimizer is not guaranteed even if the rest of assumptions from Proposition 6.2.2 (even with $f(\mathbf{x},\cdot)$ strongly convex for

all $\mathbf{x} \in \mathbb{R}^n$) do hold:

$$\hat{u}^\star(x) = \operatorname*{argmin}_{u \in \mathbb{R}} \frac{1}{2}u^2 - 2u, \tag{6.20a}$$

$$\text{s.t.} \quad xu \leq 0. \tag{6.20b}$$

Indeed, the objective function and constraint of (6.20) are twice continuously differentiable, the objective function is strongly convex and the constraint is convex for any $x \in \mathbb{R}$. However, Slater's condition does not hold at $x = 0$. In fact,

$$\hat{u}^\star(x) = \begin{cases} 2 & \text{if} \quad x \leq 0, \\ 0 & \text{else}, \end{cases}$$

is discontinuous at $x = 0$. However, note that $\hat{u}^\star$ is bounded. •

Example 6.2.6. (Unbounded optimizer without Slater's condition): The following example, adapted from [103, Example III.5], shows that if Slater's condition fails, not only can the parametric optimizer fail to be continuous, as shown in Example 6.2.5, but it can even fail to be locally bounded. Let $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$, $a(\mathbf{x}) = 2x_1x_2 + x_2^2(1 - x_1^2 - x_2^2)$, and consider:

$$\breve{u}^\star(\mathbf{x}) = \operatorname*{argmin}_{u \in \mathbb{R}} \frac{1}{2}u^2, \tag{6.21a}$$

$$\text{s.t.} \quad a(\mathbf{x}) + 2x_2^3 u \leq 0. \tag{6.21b}$$

Note that Slater's condition does not hold at the point $\mathbf{x} = (1, 0)$. Moreover, $\breve{u}^\star$ is given by:

$$\breve{u}^\star(\mathbf{x}) = \begin{cases} 0 & \text{if} \quad a(\mathbf{x}) \leq 0, \\ -\frac{a(\mathbf{x})}{2x_2^3} & \text{else}. \end{cases}$$

Note that $a(1, 0) = 0$ and $a(1, \epsilon) = 2\epsilon - \epsilon^4$. Moreover, since any neighborhood of $(1, 0)$ contains points of the form $(1, \epsilon)$ for sufficiently small $\epsilon > 0$, for any neighborhood $\mathcal{N}$ of $(1, 0)$ there exists $\epsilon_{\mathcal{N}} > 0$ sufficiently small such that $a(1, \epsilon_{\mathcal{N}}) > 0$. Now, since

$$\lim_{\epsilon \to 0} \frac{a(1, \epsilon)}{2\epsilon^3} = \infty,$$

and $\breve{u}^\star(\mathbf{x}) = -\frac{a(\mathbf{x})}{2x_2^3}$ if $a(\mathbf{x}) > 0$, it follows that $\breve{u}^\star$ is not locally bounded. •

Discontinuous controllers are relevant, and even necessary, in multiple applications, cf. [161]. When dealing with discontinuous systems, one needs to ensure basic properties such as local boundedness and measurability. In the following, we provide conditions that guarantee these properties for optimization-based controllers.

The following result gives a condition which ensures that parametric optimizers are locally bounded, hence precluding the behavior exhibited in Example 6.2.6.

Proposition 6.2.7. (Conditions for local boundedness): *Suppose that f and g belong to $\mathcal{C}^0(\mathbb{R}^n \times \mathbb{R}^m)$. Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $f(\mathbf{x}, \cdot)$ is strictly convex, $g(\mathbf{x}, \cdot)$ is convex, and* (6.1) *has at least one minimizer. Then, given $\mathbf{x}_0 \in \mathbb{R}^n$, u^* is locally bounded at $\mathbf{x}_0$ if and only if LCF holds at $\mathbf{x}_0$.*

Proof. Note that since (6.1) has at least one minimizer for all $x \in \mathbb{R}^n$, the convexity assumptions on f and g imply that u^* is a singleton for all $\mathbf{x} \in \mathbb{R}^n$. First suppose that LCF holds at $\mathbf{x}_0$. Therefore, there exists a compact set $K \subset \mathbb{R}^m$ and $\delta > 0$ such that for all $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}\| < \delta$, there exists $\mathbf{u} \in K$ such that $g(\mathbf{y}, \mathbf{u}) \leq 0$. Since f is continuous and K is compact, there exists $B_f > 0$ such that $|f(\mathbf{y}, \mathbf{u})| < B_f$ for all $\mathbf{u} \in K$ and $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}_0\| < \delta$. Since for all $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}_0\| < \delta$, there exists a feasible $\mathbf{u} \in K$, it follows that $|f(\mathbf{y}, u^*(\mathbf{y}))| < B_f$ for all $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}_0\| < \delta$. This implies that u^* is locally bounded at $\mathbf{x}_0$. Now suppose that u^* is locally bounded at $\mathbf{x}_0$ and suppose, by contradiction, that LFC does not hold at $\mathbf{x}_0$. Then, for any $\delta > 0$ and compact set K, there exists $\mathbf{y} \in \mathbb{R}^n$ with $\|\mathbf{y} - \mathbf{x}\| \leq \delta$ and such that all $\mathbf{u} \in \mathbb{R}^m$ with $g(\mathbf{y}, \mathbf{u}) \leq 0$ satisfy $\mathbf{u} \notin K$. This means that there exists a sequence $\{\mathbf{y}_n\}_{n \in \mathbb{Z}_{>0}}$ such that $\|\mathbf{y}_n - \mathbf{x}\| \leq 1/n$ and $\|u^*(\mathbf{y}_n)\| \geq n$ for all $n \in \mathbb{Z}_{>0}$, which implies that u^* is not locally bounded, hence reaching a contradiction. □

Verifying the local compact feasibility property can be challenging in general. However, for the particular case of CBF-based quadratic programs, [103, Theorem V.1] gives an alternative sufficient condition for local boundedness of u^* that only requires solving a specific linear equation.

Next, we turn our attention to the measurability properties of u^*.

Proposition 6.2.8. (Sufficient conditions for measurability): *Suppose that f and g belong to $\mathcal{C}^0(\mathbb{R}^n \times \mathbb{R}^m)$. Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $f(\mathbf{x}, \cdot)$ is strictly convex, $g(\mathbf{x}, \cdot)$ is convex, and* (6.1) *has at least one minimizer. Further assume that for every $\mathbf{x} \in \mathbb{R}^n$, LCF holds at $\mathbf{x}$. Then, u^* is measurable.*

Proof. Note that since (6.1) has at least one minimizer for all $\mathbf{x} \in \mathbb{R}^n$, the convexity assumptions on f and g imply that u^* is a singleton for all $\mathbf{x} \in \mathbb{R}^n$. We use the Measurable Maximum Theorem [183, Theorem 18.19]. We assume that $\mathbb{R}^n$ and $\mathbb{R}^m$ are equipped with the usual Borel σ-algebras. Since f is continuous, it is a Carathéodory function (cf. [183, Definition 4.50]). Therefore, we only need to ensure that the set-valued map $\phi : \mathbf{x} \to \{\mathbf{u} \in \mathbb{R}^m : g(\mathbf{x}, \mathbf{u}) \leq 0\}$ is a weakly measurable correspondence (cf. [183, Definition 18.1]) with nonempty compact values. The fact that ϕ takes nonempty values follows from the fact that the feasible set $\{u \in \mathbb{R}^m : g(\mathbf{x}, \mathbf{u}) \leq 0\}$ is nonempty. Moreover, since Proposition 6.2.7 ensures that u^* is locally bounded at every $\mathbf{x} \in \mathbb{R}^n$, without loss of generality we can assume that ϕ takes compact values (otherwise, we can define extra constraints that ensure that the feasible set is bounded for every $\mathbf{x} \in \mathbb{R}^n$ without changing the optimizer u^*). Now, to show that ϕ is a weakly measurable correspondence, we follow an argument similar to the proof of [183, Corollary 18.8]. For every $n \in \mathbb{Z}_{>0}$, define the set-valued map $\phi_n : \mathbf{x} \to \{\mathbf{u} \in \mathbb{R}^m : g(\mathbf{x}, \mathbf{u}) \leq 1/n\}$. By Lemma [183, Corollary 18.8], ϕ_n is measurable. Moreover, for every $\mathbf{x} \in \mathbb{R}^n$ and $n \in \mathbb{Z}_{>0}$, $\phi(\mathbf{x}) \subset \partial(\phi_n(\mathbf{x}))$ (where $\partial(\phi_n(\mathbf{x}))$ denotes the boundary of $\phi_n(\mathbf{x})$), and $\phi(\mathbf{x}) = \cap_{n=1}^{\infty} \partial(\phi_n(\mathbf{x}))$. Furthermore, again without loss of generality, $\partial(\phi_n)$ has compact values for every $n \in \mathbb{Z}_{>0}$ (again, if that is not the case we can define extra constraints that ensure that this holds without changing the optimizer u^*), and by [183, Theorem 18.4(3)], the intersection $\phi : \mathbf{x} \to \cap_{n=1}^{\infty} \partial(\phi_n(\mathbf{x}))$ is measurable. □

The second column in Table 6.1 summarizes the different results discussed in this section.

Remark 6.2.9. (Verifying constraint qualifications and conditions in practice without knowledge of the optimizer): To show that u^* is locally Lipschitz at a point $\mathbf{x} \in \mathbb{R}^n$ using [172, Theorem 3.6], we need to verify that both MFCQ and

CR hold at $(\mathbf{x}, u^*(\mathbf{x}))$. Similarly, [171, Theorem 4.1] (resp. [170, Theorem 2.1]) require the verification of LICQ (resp. LICQ and SCS) at $(\mathbf{x}, u^*(\mathbf{x}))$. These results require knowledge of $u^*(\mathbf{x})$ to verify the corresponding property holds at $\mathbf{x}$. However, in several applications it can be useful to know the regions where the controller u^* is discontinuous (for instance, to design safety-critical controllers that avoid such regions). Slater's condition is useful for this purpose because Proposition 6.2.2 guarantees different regularity properties of u^* at $\mathbf{x}$ without requiring knowledge of $u^*(\mathbf{x})$ (assuming that the extra conditions on differentiability and convexity of the objective function and constraints in Proposition 6.2.2 also hold). Moreover, in the special case where the constraints in (6.1) are affine, i.e.,

$$g(\mathbf{x}, \mathbf{u}) = \begin{pmatrix} g_1^0(\mathbf{x})^\top \mathbf{u} + g_1^1(\mathbf{x}) \\ \vdots \\ g_i^0(\mathbf{x})^\top \mathbf{u} + g_i^1(\mathbf{x}) \\ \vdots \\ g_p^0(\mathbf{x})^\top \mathbf{u} + g_p^1(\mathbf{x}) \end{pmatrix},$$

for $i \in [p]$ and $g_i^0 : \mathbb{R}^n \to \mathbb{R}^m$ and $g_i^1 : \mathbb{R}^n \to \mathbb{R}$ in $\mathcal{C}^2(\mathbb{R}^n)$, then [184] shows that by letting $c_{\mathbf{x}}^*$ be the optimal value of the linear program

$$\max_{u \in \mathbb{R}^m} \sum_{i=1}^m |u_i| \tag{6.22a}$$

$$\text{s.t.} \quad u_i \geq 0, \ i \in \{1, \cdots, m\}, \tag{6.22b}$$

$$\sum_{i=1}^m u_i g_i^0(\mathbf{x}) = 0, \tag{6.22c}$$

$$\sum_{i=1}^m u_i g_i^1(\mathbf{x}) = 0. \tag{6.22d}$$

then Slater's condition holds at $\mathbf{x}$ if and only if $c_{\mathbf{x}}^* = 0$. Hence, (6.22) can be solved before solving (6.1) to verify that u^* satisfies the regularity properties in Proposition 6.2.2. •

6.3 Existence and Uniqueness of Solutions under Optimization-Based Controllers

In this section, we leverage the regularity properties established in Section 6.2 to study existence and uniqueness of solutions for the closed-loop system (6.18) under the optimization-based controller u^*.

First, we note that by the Picard-Lindelöf theorem [143, Theorem 2.2], any of the assumptions described in Section 6.2 that guarantee that u^* is locally Lipschitz at a point $\mathbf{x}_0$ also guarantee that the closed-loop system (6.18) has a unique solution with initial condition at $\mathbf{x}_0$ for sufficiently small times.

The following result establishes existence of solutions under weaker assumptions.

Proposition 6.3.1. (Existence of classical solutions for the closed-loop system): *Suppose that f and g belong to $\mathcal{C}^{0,2}(\mathbb{R}^n \times \mathbb{R}^m)$. Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $f(\mathbf{x}, \cdot)$ is strictly convex, $g(\mathbf{x}, \cdot)$ is convex, and* (6.1) *has at least one minimizer. Further assume that SC holds at $\mathbf{x}_0 \in \mathbb{R}^n$. Let $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ be locally Lipschitz. Then, there exists $\delta_0 > 0$ such that the differential equation* (6.18) *has at least one solution $x : (-\delta_0, \delta_0) \to \mathbb{R}^n$ with initial condition $x(0) = \mathbf{x}_0$.*

Proof. Note that since (6.1) has at least one minimizer for all $\mathbf{x} \in \mathbb{R}^n$, the convexity assumptions on f and g imply that u^* is a singleton for all $\mathbf{x} \in \mathbb{R}^n$. Since SC holds at $\mathbf{x}_0$, by [178, Prop. 5.39], since $g(\mathbf{x}_0, \cdot)$ is convex, MFCQ holds at $(\mathbf{x}_0, u^*(\mathbf{x}_0))$. By [173, Theorem 5.3], this implies that u^* is continuous at $\mathbf{x}_0$. Since g is continuous, there exists a neighborhood $\mathcal{V}_{\mathbf{x}_0}$ of $\mathbf{x}_0$ such that SC holds for all $\mathbf{y} \in \mathcal{V}_{\mathbf{x}_0}$. By the same argument, this implies that u^* is continuous in $\mathcal{V}_{\mathbf{x}_0}$. The result now follows by Peano's existence theorem [185, Theorem 2.1]. □

Proposition 6.3.1 implies in particular that, under the assumptions of Proposition 6.2.2, the closed-loop system (6.18) has at least one solution in a neighborhood of $\mathbf{x}_0$.

Next, we study uniqueness of solutions under the assumptions of Proposition 6.2.2. We first note that the Hölder property does not imply uniqueness,

even in simple one-dimensional examples. For example, the differential equation $\dot{x} = x^{1/3}$ has the Hölder property at 0 but infinitely many solutions starting from the origin. The next example shows that, in general, point-Lipschitz continuity does not imply uniqueness of solutions either.

Example 6.3.2. (Point-Lipschitz differential equation with non-unique solutions): Let $u^\star : \mathbb{R}^2 \to \mathbb{R}^4$ be the parametric optimizer of Robinson's counterexample. Consider the dynamical system

$$\dot{x}_1 = \frac{1}{2}, \tag{6.23a}$$

$$\dot{x}_2 = u_4^*(x_1, x_2), \tag{6.23b}$$

with initial condition $(x_1(0), x_2(0)) = (0, 0)$. By Proposition 6.2.2, the vector field in (6.23) is point-Lipschitz at the origin. However, (6.23) admits the following two distinct solutions starting from the origin: $y_1(t) := (\frac{1}{2}t, 0)$ and $y_2(t) := (\frac{1}{2}t, \frac{1}{8}t^2)$, cf. Figure 6.2. •

Hence, in general the assumptions of Proposition 6.2.2 are not sufficient to ensure uniqueness of solutions of the closed-loop system. Interestingly, the next result shows that point-Lipschitz continuity guarantees uniqueness of solutions starting from equilibria.

Proposition 6.3.3. (Point-Lipschitz continuity and uniqueness): *Let $\tilde{F} : \mathbb{R}^n \to \mathbb{R}^n$ be point-Lipschitz at $\mathbf{x}_0 \in \mathbb{R}^n$ and $\tilde{F}(\mathbf{x}_0) = 0$. Then the function $x(t) = \mathbf{x}_0$ for all $t \geq 0$ is the unique solution to the differential equation $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$ with initial condition $x(0) = \mathbf{x}_0$.*

Proof. Let $\delta > 0$ and L be the point-Lipschitz continuity constant of $\tilde{F}$ and take $\delta < \frac{1}{L}$. Suppose that there exists another solution $y : [0, \delta) \to \mathbb{R}^n$ starting from $\mathbf{x}_0$. Then, $\sup_{t\in[0,\delta)} \|y(t) - \mathbf{x}_0\| > 0$. Moreover,

$$\sup_{t\in[0,\delta)} \|y(t) - \mathbf{x}_0\| = \sup_{t\in[0,\delta)} \left\| \int_0^t \tilde{F}(y(s))ds \right\| = \sup_{t\in[0,\delta)} \left\| \int_0^t \Big(\tilde{F}(y(s)) - \tilde{F}(\mathbf{x}_0) \Big) ds \right\|$$

$$\leq \sup_{t\in[0,\delta)} \int_0^t L \|y(s) - \mathbf{x}_0\| \, ds \leq L\delta \sup_{t\in[0,\delta]} \|y(t) - \mathbf{x}_0\| < \sup_{t\in[0,\delta]} \|y(t) - \mathbf{x}_0\| .$$

where in the last inequality we have used the fact that $\sup_{t\in[0,\delta)} \|y(t) - \mathbf{x}_0\| > 0$. We hence reach a contradiction, which means that the constant solution is the only solution for $t \in [0, \delta)$. By repeating the same argument at time δ, we can extend this constant solution for all positive times. □

This result implies that in one dimension, point-Lipschitz ODEs have unique solutions.

Corollary 6.3.4. (Point-Lipschitz continuity implies uniqueness in one dimension): *Let $\tilde{F} : \mathbb{R} \to \mathbb{R}$ be continuous in a neighborhood of $\mathbf{x}_0$ and point-Lipschitz at $\mathbf{x}_0$. Then, the differential equation $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$ with initial condition $x(0) = \mathbf{x}_0$ has a unique solution.*

Proof. If $\tilde{F}(\mathbf{x}_0) \neq \mathbf{0}_n$, by [186, Theorem 1.2.7], the differential equation has only one solution. If $\tilde{F}(\mathbf{x}_0) = \mathbf{0}_n$, the result follows from Proposition 6.3.3. □

If Slater's condition does not hold but the rest of assumptions of Proposition 6.2.2 hold (even with $f(\mathbf{x}, \cdot)$ strongly convex for all $\mathbf{x} \in \mathbb{R}^n$), Example 6.2.5 shows that u^* can be discontinuous, in which case neither existence nor uniqueness of solutions is guaranteed. In the case where f and g are not differentiable with respect to the parameter, but the rest of assumptions of Proposition 6.2.2 hold (even with $f(\mathbf{x}, \cdot)$ strongly convex for all $\mathbf{x} \in \mathbb{R}^n$), Example 6.2.4 shows that u^* is continuous but not necessarily point-Lipschitz. Therefore, in this case existence is guaranteed but uniqueness is not.

Note that so far, we have only considered existence and uniqueness for classical solutions. For discontinuous dynamical systems, other notions of solution, such as Carathéodory or Filippov solutions, can be defined, cf. [161]. The following result gives conditions on (6.1) that ensure the existence of Filippov solutions for (6.18).

Proposition 6.3.5. (Existence of Filippov solutions for the closed-loop system): *Suppose that f and g belong to $\mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$. Further assume that for any $\mathbf{x} \in \mathbb{R}^n$, $f(\mathbf{x}, \cdot)$ is strictly convex, $g(\mathbf{x}, \cdot)$ is convex and (6.1) has at least one minimizer. Finally suppose that for every $\mathbf{x} \in \mathbb{R}^n$, LCF holds at $\mathbf{x}$ and $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is locally Lipschitz. Then for any $\mathbf{x} \in \mathbb{R}^n$, there exists $\delta_{\mathbf{x}} > 0$ such that (6.18) has at least one Filippov solution $y : (-\delta_{\mathbf{x}}, \delta_{\mathbf{x}}) \to \mathbb{R}^n$ with initial condition $y(0) = \mathbf{x}$.*

Proof. Note that since (6.1) has at least one minimizer for all $\mathbf{x} \in \mathbb{R}^n$, the convexity assumptions on f and g imply that u^* is a singleton for all $\mathbf{x} \in \mathbb{R}^n$. By Propositions 6.2.7 and 6.2.8, the assumptions ensure that u^* is measurable and locally bounded. The result follows from [187, Theorem 7]. □

A weaker condition to ensure that Filippov solutions are unique is that the closed-loop system (6.18) is *essentially one-sided Lipschitz* [161]. Although it is known how to verify this property for projected dynamical systems (see e.g., [152, proof of Theorem 2.7] for the Euclidean case, and [157, Proposition 6.12] for the Non-Euclidean case), to the best of our knowledge there exist no results in the parametric optimization literature that guarantee that the parametric optimizer u^*, or the closed-loop dynamics, satisfies this property.

Finally, we note that if f is not strictly convex or g is not convex, the optimizer u^* is not guaranteed to be single-valued, which means that the usual notions of regularity of the controller and of solutions of the closed-loop system are not well defined. The third and fourth columns of Table 6.1 summarize the results presented in this section.

6.4 Forward Invariance Properties of Optimization-Based Controllers

In this section we study conditions that guarantee the forward invariance of a set for the closed-loop system under an optimization-based controller. The basic result concerning forward invariance is the following:

Theorem 6.4.1. (Nagumo's Theorem [126, 188]): *Let $\tilde{F} : \mathbb{R}^n \to \mathbb{R}^n$ and consider the system $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$. Assume that, for each initial condition in a set $\mathcal{D} \subset \mathbb{R}^n$, it admits a unique forward complete solution (i.e., a unique solution defined for all positive times). Let $\mathcal{C} \subset \mathcal{D} \subset \mathbb{R}^n$ be a closed set. Then the set $\mathcal{C}$ is forward invariant for the system if and only if $\tilde{F}(\mathbf{x}) \in T_{\mathcal{C}}(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{C}$.*

The condition that $\tilde{F}(\mathbf{x}) \in T_{\mathcal{C}}(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{C}$ is called the *sub-tangentiality condition*, and can be enforced using the constraints of an optimization-based

feedback controller of the form (6.1). We show how in the following. Suppose that $\mathcal{C}$ is parameterized as $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n \mid h_j(\mathbf{x}) \geq 0,\ 1 \leq j \leq p\}$, where $h_j : \mathbb{R}^n \to \mathbb{R}$ are continuously differentiable for $j = 1, \ldots, p$, and the dynamics take the form

$$\dot{\mathbf{x}} = F(\mathbf{x}, \mathbf{u}) = F_0(\mathbf{x}) + \sum_{i=1}^{m} u_i F_i(\mathbf{x}), \tag{6.24}$$

for smooth functions $F_i : \mathbb{R}^n \to \mathbb{R}^n$ for $i \in \{0\} \cup [m]$. Next, define $A(\mathbf{x}) \in \mathbb{R}^{p \times m}$ and $b(\mathbf{x}) \in \mathbb{R}^p$ as

$$A(\mathbf{x}) = \begin{bmatrix} L_{F_1} h_1(x) & \ldots & L_{F_m} h_1(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ L_{F_1} h_p(\mathbf{x}) & \ldots & L_{F_m} h_p(\mathbf{x}) \end{bmatrix}, \quad b(\mathbf{x}) = \begin{bmatrix} -\alpha(h_1(\mathbf{x})) - L_{F_0} h_1(\mathbf{x}) \\ \vdots \\ -\alpha(h_m(\mathbf{x})) - L_{F_0} h_m(\mathbf{x}) \end{bmatrix},$$

where α is an extended class-$\mathcal{K}_\infty$ function. Let $A_j(\mathbf{x})$ denote the jth row of $A(\mathbf{x})$, and for $J \subset [p]$, let $A_J(\mathbf{x})$ denote the matrix consisting of the rows of $A(\mathbf{x})$ corresponding to $j \in J$.

In the literature on optimization-based control design [1], the feasibility of the system $A_j(\mathbf{x})\mathbf{u} \geq b_j(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$ such that $h_j(\mathbf{x}) \geq 0$ is equivalent to h_j being a *control barrier function* for the set $\{\mathbf{x} \in \mathbb{R}^n \mid h_j(\mathbf{x}) \geq 0\}$. Since we are considering the case where $\mathcal{C}$ is possibly parameterized by multiple inequalities, here we make the stronger assumption that the system $A(\mathbf{x})\mathbf{u} \geq b(\mathbf{x})$ (where the inequality holds component-wise) is feasible for all $\mathbf{x} \in \mathcal{C}$. In this case, if $\mathcal{C}$ satisfies an appropriate constraint qualification condition (e.g., MFCQ or LICQ) and $u^* : \mathbb{R}^n \to \mathbb{R}^m$ is a feedback controller such that $A(\mathbf{x})u^*(\mathbf{x}) \geq b(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{C}$, then the closed-loop dynamics satisfies the sub-tangentiality condition $F(\mathbf{x}, u^*(\mathbf{x})) \in T_{\mathcal{C}}(\mathbf{x})$. Such a controller can be obtained from the solution of a parametric optimization problem of the form (6.1) where $g(\mathbf{x}, \mathbf{u}) = b(\mathbf{x}) - A(\mathbf{x})\mathbf{u}$.

To show invariance invoking Theorem 6.4.1, one needs to additionally ensure that the closed-loop dynamics has unique solutions. The conditions discussed in Section 6.3 and summarized in Table 6.1 can be translated into easily checkable conditions on the objective function, the matrix $A(\mathbf{x})$, and the vector $b(\mathbf{x})$. The following result uses [172, Theorem 3.6] to ensure uniqueness, and therefore forward invariance.

Theorem 6.4.2. (Sufficient conditions for forward invariance with respect to closed-loop dynamics): *Consider the dynamics* (6.24) *and the optimization problem* (6.1) *where* $f \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ *is strictly convex, and* $g(\mathbf{x}, \mathbf{u}) = b(\mathbf{x}) - A(\mathbf{x})\mathbf{u}$. *Assume*

- *For all* $\mathbf{x} \in \mathcal{C}$, *there exists* $\mathbf{u} \in \mathbb{R}^m$ *such that* $A(\mathbf{x})\mathbf{u} > b(\mathbf{x})$, *and* (6.1) *has at least one minimizer.*
- *For all* $\mathbf{x} \in \mathcal{C}$, *there is an open set* $U_{\mathbf{x}} \subset \mathbb{R}^n$ *containing* $\mathbf{x}$ *such that, for any subset* J *in* $[p]$, *the matrix* $A_J(\mathbf{y})$ *has constant rank for all* $\mathbf{y} \in U_{\mathbf{x}}$.

Then the closed-loop system under the optimization-based controller (6.1) *has unique solutions, and* $\mathcal{C}$ *is forward invariant.*

In the case where the closed-loop dynamics are point-Lipschitz, solutions are not necessarily unique and therefore forward invariance of $\mathcal{C}$ cannot be guaranteed by Theorem 6.4.1. In fact, the following is an example of a system where the sub-tangentiality condition holds but there exist solutions starting in $\mathcal{C}$ that eventually leave.

Example 6.4.3. (Point-Lipschitz differential equation violating forward invariance): Let $\mathcal{C} = \{(x_1, x_2) \in \mathbb{R}^2 : x_2 \leq 0\}$ and consider the system with the feedback controller defined in Example 6.3.2. Because $\mathcal{C}$ satisfies LICQ, the tangent cone can be computed as $T_{\mathcal{C}}(x_1, x_2) = \mathbb{R}^2$ if $x_2 < 0$, and $T_{\mathcal{C}}(x_1, 0) = \{(\xi_1, \xi_2) : \xi_2 \leq 0\}$. The closed-loop system satisfies $F(\mathbf{x}, u^*(\mathbf{x})) = (\frac{1}{2}, u_4^*(x_1, x_2)) \in T_{\mathcal{C}}(x_1, x_2)$ for all $(x_1, x_2) \in \mathcal{C}$. However, the solution $y_2(t) = (\frac{1}{2}t, \frac{1}{8}t^2)$ satisfies $y_2(0) \in \mathcal{C}$ and $y_2(t) \notin \mathcal{C}$ for all $t > 0$. •

Example 6.4.3 is problematic because it shows that even if the *sub-tangentiality* condition for a safe set $\mathcal{C}$ is included as one of the constraints of the optimization-based controller, if the solutions of the closed-loop system are not unique, some of the solutions might leave the safe set $\mathcal{C}$.

However, using the notion of minimal barrier functions [104], the following result gives a condition for forward invariance that can be applied to systems with non-unique solutions.

Theorem 6.4.4. (Minimal Barrier Functions, [104, Theorem 1]): *Let $\tilde{F} : \mathbb{R}^n \to \mathbb{R}^n$ be continuous and consider the system $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$. Let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function and let $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}$ be a nonempty set. If h is a minimal barrier function, cf. [104, Definition 2], then any solution of $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$ with initial condition in $\mathcal{C}$ remains in $\mathcal{C}$ for all positive times.*

A simple scenario in which h is a minimal barrier function is if there exists a strictly increasing function $\alpha : \mathbb{R} \to \mathbb{R}$ with $\alpha(0) = 0$ and an open set $\mathcal{D}$ with $\mathcal{C} \subset \mathcal{D}$ such that $\nabla h(\mathbf{x})^\intercal \tilde{F}(\mathbf{x}) \geq -\alpha(h(\mathbf{x}))$ for all $\mathbf{x} \in \mathcal{D}$. Such a set $\mathcal{D}$ and class $\mathcal{K}$ function α do not exist in Example 6.4.3. Since Theorem 6.4.4 only requires $\tilde{F}$ to be continuous, the system $\dot{\mathbf{x}} = \tilde{F}(\mathbf{x})$ might have multiple solutions starting from the same initial condition. However, the result ensures that if the initial condition is in $\mathcal{C}$, then all solutions remain in $\mathcal{C}$ for all positive times. Moreover, since point-Lipschitz functions are continuous, Theorem 6.4.4 can be applied to differential equations defined by point-Lipschitz functions. Therefore, if one of the constraints in (6.1) corresponds to the minimal control barrier function condition of a function h, and if the resulting controller is point-Lipschitz (e.g., by satisfying the hypothesis of Proposition 6.2.2), then all solutions of the closed-loop system that start in $\mathcal{C} := \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}$ remain in $\mathcal{C}$ for all positive times.

Finally, we also note that if u^* is discontinuous, the closed-loop system might not have unique solutions and hence the assumptions of Theorem 6.4.1 will not hold. Therefore, this result cannot be used to guarantee forward invariance of sets. However, the following result gives a sufficient condition for forward invariance of sets under Filippov solutions. It follows as an adaptation of [189, Theorem 1], which gives a sufficient condition for forward invariance of sets under hybrid systems.

Theorem 6.4.5. (Forward invariance under Filippov solutions of closed-loop dynamics): *Let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function and $\mathcal{C} := \{x \in \mathbb{R}^n : h(x) \geq 0\}$. Further let $\mathcal{D} \subset \mathbb{R}^n$ be a set containing $\mathcal{C}$ such that, for each initial condition $\mathbf{x}_0$ in $\mathcal{D}$, there exists a forward complete Filippov solution of* (6.18) *with initial condition at $\mathbf{x}_0$. Let $\mathcal{F} : \mathbb{R}^n \to \mathcal{P}(\mathbb{R}^n)$ be the Filippov set-valued map*

of (6.18)*, i.e.,*

$$\mathcal{F}(\mathbf{x}) \coloneqq \bigcap_{\delta>0} \bigcap_{\mu(S)=0} \overline{co}\left\{ \bigcup_{\mathbf{y}\mid\|\mathbf{y}-\mathbf{x}\|\leq\delta} F(\mathbf{y}, u^*(\mathbf{y}))\backslash S \right\},$$

where we recall that μ *denotes the Lebesgue measure. Further assume that there exists a neighborhood* $\mathcal{U}_f$ *of* $\partial\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) = 0\}$ *such that*

$$\nabla h(\mathbf{x})^T \boldsymbol{\eta} \geq 0, \ \forall \mathbf{x} \in \mathcal{U}_f \backslash \mathcal{C} \ \textit{and} \ \ \forall \boldsymbol{\eta} \in \mathcal{F}(\mathbf{x}). \tag{6.25}$$

Then, all Filippov solutions of (6.18) *with initial condition at* $\mathcal{C}$ *remain in* $\mathcal{C}$ *for all positive times.*

In particular, Theorem 6.4.5 ensures that under the assumptions of Proposition 6.3.5, and if Filippov solutions are defined for all positive times, then the *sub-tangentiality*-like condition (6.25) guarantees forward invariance of Filippov solutions. We note also that Theorem 6.4.5 is possibly conservative, and tighter conditions that guarantee forward invariance for Filippov solutions could be developed using an adapted notion of minimal barrier functions for discontinuous systems.

Assumptions	Regularity of $u^\star$	Existence	Uniqueness
f, g analytic $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, LICQ and SCS	analytic cf. [170]	✓	✓
$f, g \in \mathcal{C}^p(\mathbb{R}^n \times \mathbb{R}^m)$ $p \in \mathbb{Z}_{>0}, p \geq 2$ $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, LICQ and SCS	$\mathcal{C}^{p-1}$ cf. [170]	✓	✓
$f, g \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, LICQ	Locally Lipschitz cf. [171]	✓	✓
$f, g \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, CR and MFCQ	Locally Lipschitz cf. [172]	✓	✓
$f, g \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strongly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ of minimizer, SC	Point-Lipschitz and Hölder, cf. Prop. 6.2.2, and locally Lipschitz for scalar QPs, cf. Proposition 6.2.3	✓	Only in special cases cf. Prop. 6.3.3 Cor. 6.3.4, Ex. 6.3.2
$f, g \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, SC	Directionally differentiable, cf. Prop. 6.2.2, locally Lipschitz for scalar QPs, cf. Prop. 6.2.3, and continuous, cf. [173, Thm 5.3], might not be point-Lipschitz, cf. Ex. 6.2.4	✓	✗ cf. Ex. 6.3.2
$f, g \in \mathcal{C}^0(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strictly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer, LCF $\forall \mathbf{x} \in \mathbb{R}^n$	Locally bounded cf. Prop. 3.7, and measurable cf. Prop. 3.8	✗ (classical) ✓ (Filippov)	✗ (classical) ✗ (Filippov)
$f, g \in \mathcal{C}^2(\mathbb{R}^n \times \mathbb{R}^m)$ $f(\mathbf{x}, \cdot)$ strongly convex $\forall \mathbf{x} \in \mathbb{R}^n$ $g(\mathbf{x}, \cdot)$ convex $\forall \mathbf{x} \in \mathbb{R}^n$ $\exists$ minimizer	Might be discontinuous and even unbounded cf. Examples 6.2.5, 6.2.6	✗ (classical) ✗ (Filippov)	✗ (classical) ✗ (Filippov)

Table 6.1: Summary of results on regularity properties of optimization-based controllers. The first column describes the different assumptions. The second column describes the regularity properties of $u^\star$. The third (resp. fourth) column describes whether existence (resp. uniqueness) of classical solutions of the closed-loop system (6.18) is guaranteed (provided that $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is locally Lipschitz). In the last two columns, properties are stated by default for classical solutions. If results are available for both classical and Filippov solutions, the property for each type of solution is denoted separately. The terminology for regularity and constraint qualification is given in Chapter 2.

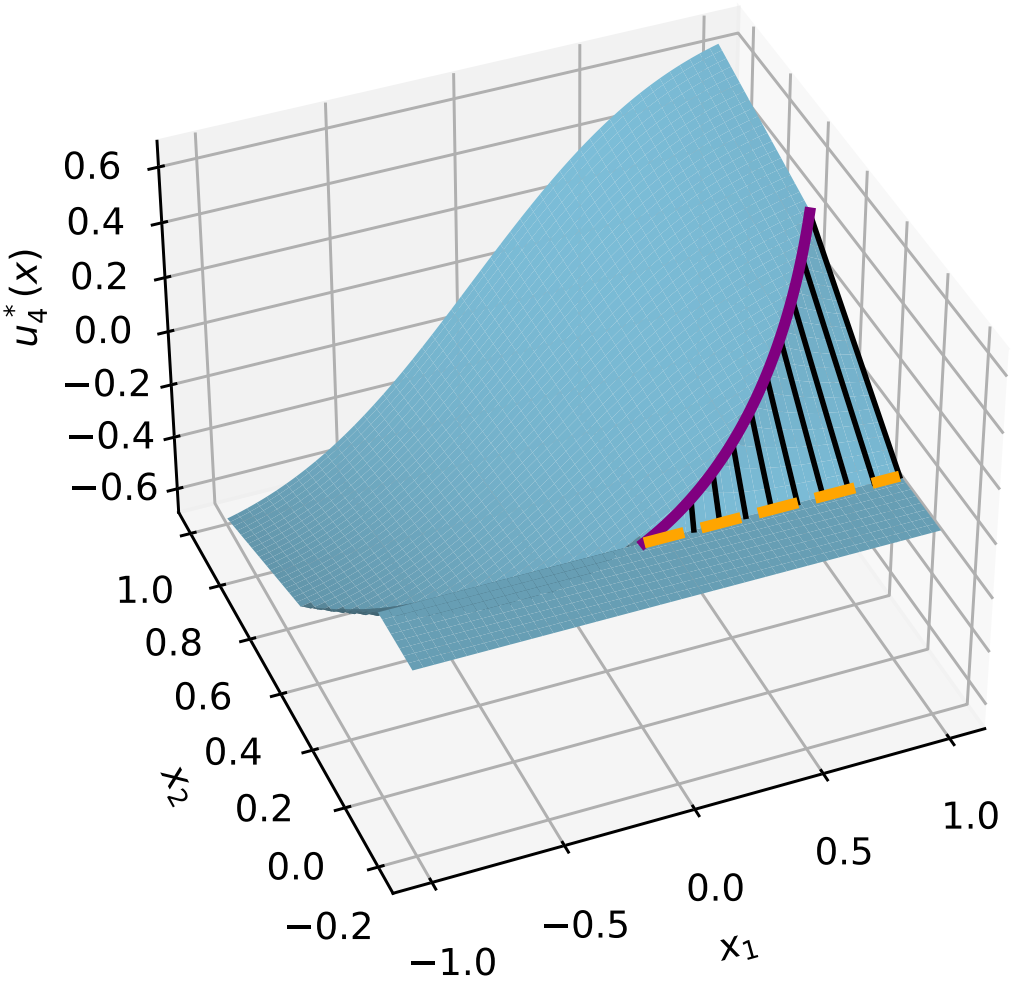


Figure 6.1: Surface plot of u_4, which is the fourth component of the parametric optimizer of Robinson's counterexample, cf. (6.19). The purple solid and orange dashed lines correspond to the plot of $u_4(p(s))$ and $u_4(q(s))$ (defined in Example 6.2.1) respectively, for $s \geq 0$. The solid black lines connect points corresponding to $p(s)$ and $q(s)$. The plot shows that u_4 is continuous at the origin, in agreement with Proposition 6.2.2. However, since the slope of the line connecting $u_4(p(s))$ and $u_4(q(s))$ becomes arbitrarily large as p and q approach the origin, u_4 is not locally Lipschitz at the origin.

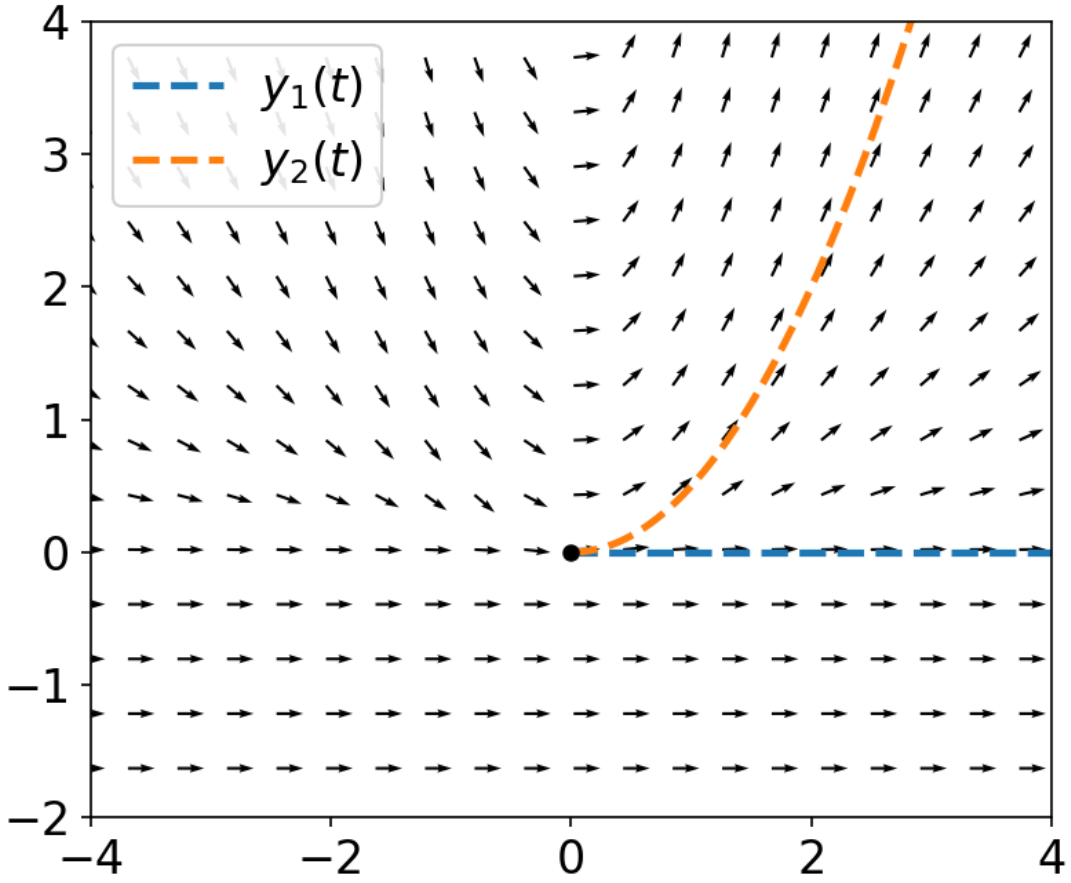


Figure 6.2: The arrows depict the vector field (6.23). The dashed blue and orange curves depict the two solutions y_1 and y_2 starting from the origin, where the vector field is point-Lipschitz but not locally Lipschitz.

Part II

Motion Planning using Safe and Stable Controllers

Chapter 7

Distributed Safe Navigation of Multi-Agent Systems using Control Barrier Function-Based Optimal Controllers

In this chapter we propose a distributed controller synthesis framework for safe navigation of multi-agent systems. The navigation task requires a team of robots to visit a sequence of waypoints of interest while maintaining a predefined formation as close as possible, as well as avoiding obstacles and collisions between agents. We leverage CBFs to formulate collision avoidance with obstacles and teammates as constraints on the control input for a state-dependent network optimization problem that also encodes team formation and the navigation task. The algorithmic solution we present here is valid under general assumptions for nonlinear dynamics and state-dependent network optimization problems with convex constraints and strongly convex objectives. The resulting controller is distributed, satisfies the safety constraints at all times, and asymptotically converges to the solution of the state-dependent network optimization problem. We illustrate its performance on a team of differential-drive robots in a variety of complex environments, both in simulation and in hardware.

7.1 Problem Statement

We are interested in designing distributed controllers that allow a team of differential-drive robots to safely navigate an environment while maintaining a desired formation and visiting a sequence of waypoints of interest. The robots have identities in the set $[N]$ and follow unicycle dynamics

$$\dot{x}_i = v_i \cos\theta_i, \tag{7.1a}$$

$$\dot{y}_i = v_i \sin\theta_i, \tag{7.1b}$$

$$\dot{\theta}_i = \omega_i, \tag{7.1c}$$

where $\mathbf{s}_i = [x_i, y_i] \in \mathbb{R}^2$ is the position of agent i, $\theta_i \in [0, 2\pi)$ its heading and $v_i \in \mathbb{R}$ and $w_i \in \mathbb{R}$ are its linear and angular velocity control inputs, respectively.

We next leverage CBFs to encode the different safety specifications, giving rise to affine constraints in the control inputs. We note that, under the dynamics (7.1), direct application of (2.7) on functions that only depend on position results in limited design flexibility because ω_i does not appear in the time derivative of s_i. Instead, we follow [190, Section IV] and define, for all $i \in [N]$,

$$R(\theta_i) = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix}, \quad \mathbf{p}_i = \mathbf{s}_i + lR(\theta_i)\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 0 \\ 0 & 1/l \end{bmatrix},$$

where $l > 0$ is a design parameter. This defines $\mathbf{p}_i$ as a point orthogonal to the wheel axis of the robot. It follows that $\dot{\mathbf{p}}_i = R(\theta_i)L^{-1}\mathbf{u}_i$, where $\mathbf{u}_i = [v_i, w_i]^\top$. Hence, by choosing $\mathbf{p}_i$ as our position variable, both control inputs appear in the time derivative of the position, which allows for more flexibility in our control design.

Avoiding obstacles

We consider an environment with M obstacles $\{\mathcal{O}_k\}_{k\in[M]}$, each expressable as the sublevel set of a differentiable function h_k, i.e., $\mathcal{O}_k = \{(x, y) \in \mathbb{R}^2 : h_k(x, y) < 0\}$. To guarantee that the robot does not collide with the obstacles, we want to ensure that

$$h_k(\mathbf{p}_i) \geq \eta_k > 0, \quad \forall k \in [M]. \tag{7.2}$$

The parameter $\eta_k \in \mathbb{R}$ should be taken large enough to guarantee that the whole physical robot (instead of just $\mathbf{p}_i$) does not collide with the obstacle $\mathcal{O}_k$. For instance, if r_i is the radius of robot i and $\mathcal{O}_k$ is a circular obstacle with center at $\mathbf{m}_k \in \mathbb{R}^2$ and radius R_k so that $h_k(\mathbf{p}_i) = \|\mathbf{p}_i - \mathbf{m}_k\|^2 - R_k^2$, then η_k can be taken as $(r_i+l)^2+2R_k(r_i+l)$. The CBF condition associated with (7.2) with linear extended class $\mathcal{K}_\infty$ function with slope $\alpha_k > 0$ reads

$$\nabla h_k(\mathbf{p}_i)^\top R(\theta_i)L^{-1}\mathbf{u}_i \geq -\alpha_k(h_k(\mathbf{p}_i) - \eta_k). \tag{7.3}$$

Avoiding inter-agent collisions

We also want to enforce that agents do not collide with other team members. To achieve this, we assume it is enough for each robot i to avoid colliding with a subset of the agents $N_i \subset [N]\backslash\{i\}$. This is motivated by the fact that our control design will make the team maintain a formation at all times. Hence, each agent only needs to avoid colliding with agents closest to it in the formation. For this reason, we assume that if $j \in N_i$, then $i \in N_j$, and agent i can communicate with all agents in N_i to obtain their state variables. We assume that the resulting communication graph is connected. For any $i \in [N]$ and $j \in N_i$, we want to ensure

$$d(\mathbf{p}_i, \mathbf{p}_j) := \|\mathbf{p}_i - \mathbf{p}_j\|^2 - d_{\min}^2 \geq 0, \tag{7.4}$$

with $d_{\min} \geq r_i + r_j + 2l$. The CBF condition for (7.4) with a linear extended class $\mathcal{K}_\infty$ function with slope $\alpha_c^{ij} > 0$ reads

$$2(\mathbf{p}_i-\mathbf{p}_j)^\top(R(\theta_i)L^{-1}\mathbf{u}_i-R(\theta_j)L^{-1}\mathbf{u}_j) \geq -\alpha_c^{ij}d(\mathbf{p}_i, \mathbf{p}_j). \tag{7.5}$$

Team formation

Finally, we are interested in making the team reach a goal while maintaining a certain formation. To do so, we define a *leader* for the team (without loss of generality, agent 1). The rest of the agents $\{2, \cdots, N\}$ are referred to as *followers*. The leader is in charge of steering the team towards a given waypoint $\mathbf{q}_1 \in \mathbb{R}^2$. To achieve it, we define a nominal controller $u_{\text{nom},1} : \mathbb{R}^2 \to \mathbb{R}^2$ that steers it towards

$\mathbf{q}_1$. We use the stabilizing controller for the unicycle dynamics in [191]. To define it, let $e_1 : \mathbb{R}^2 \to \mathbb{R}$ and $\beta_1 : \mathbb{R}^2 \to \mathbb{R}$ defined as

$$e_1(\mathbf{p}_1) = \|\mathbf{p}_1 - \mathbf{q}_1\|, \quad \beta_1(\mathbf{p}_1) = \arctan\Big(\frac{p_{1,y} - q_{1,y}}{p_{1,x} - q_{1,x}}\Big).$$

The control law is $u_{\text{nom},1}(\mathbf{p}_1) = [v_1(\mathbf{p}_1), w_1(\mathbf{p}_1)]$, where

$$v_1(\mathbf{p}_1) = k_r e(\mathbf{p}_1)\cos(\beta_1(\mathbf{p}_1)) - \theta_1), \tag{7.6a}$$

$$\omega_1(\mathbf{p}_1) = k_a\beta_1(\mathbf{p}_1) + \frac{k_r}{2}\sin(2\beta_1(\mathbf{p}_1))\frac{\beta_1(\mathbf{p}_1)+h\theta_1}{\beta_1(\mathbf{p}_1)}, \tag{7.6b}$$

and $k_r > 0, k_a > 0$ and $h > 0$ are design parameters. We can also specify a sequence of waypoints for the leader: once the leader is within a given tolerance of the current waypoint, $u_{\text{nom},1}$ can be updated to steer it towards the next waypoint.

As the leader moves towards the desired waypoint, the followers follow it while maintaining a certain formation of interest. We define the desired formation positions for the followers as follows. First, recall that $N_1 := \{i \in [N]\backslash\{1\} : i \text{ and } 1 \text{ can communicate their respective state variables}\}$ and, for $k \in \mathbb{Z}_{>0}$, $k > 1$, define the k-neighborhood of the leader as $N_1^k := \{i \in [N] : \exists\ j \in N_1^{k-1} \text{ s.t. } i \in N_j\}$ (here, $N_1^1 = N_1$). Since the communication graph is connected, there exists $K \in \mathbb{Z}_{>0}$ such that, for all $i \in [N]\backslash\{1\}$, there is $k \in [K]$ such that $i \in N_1^k$. For every $i \in [N]\backslash\{1\}$, we let k_i be the smallest positive integer k such that $i \in N_1^k$. For every $i \in [N]\backslash\{1\}$, we consider functions $q_i : \mathbb{R}^{2|N_1^{k_i-1}\cap N_i|} \to \mathbb{R}^2$ such that $q_i(\{\mathbf{p}_j\}_{j\in N_1^{k_i-1}\cap N_i})$ defines the desired formation position for agent i. Agent i aims to remain as close as possible to $q_i(\{\mathbf{p}_j\}_{j\in N_1^{k_i-1}\cap N_i})$ while maintaining the safety constraints. To achieve this, we define a nominal controller $u_{\text{nom},i} : \mathbb{R}^2 \to \mathbb{R}^2$ for each agent $i \in \{2, \cdots, N\}$ analogous to (7.6) that steers it towards $q_i(\{\mathbf{p}_j\}_{j\in N_1^{k_i-1}\cap N_i})$. Note that q_i can be computed in a distributed fashion because it only depends on the positions of agents in $N_1^{k_i-1} \cap N_i \subseteq N_i$.

Agents collectively try to design controllers $\{\mathbf{u}_i\}_{i=1}^N$ that satisfy the obstacle avoidance and inter-agent collision avoidance constraints while remaining as close as possible to their nominal controller (i.e., they execute a safety filter). By employing weighting matrix-valued functions $\Gamma_i : \mathbb{R}^n \to \mathbb{R}^{m\times m}$ for each $i \in [N]$ that can be designed to penalize the linear and angular velocity inputs differently, and

leveraging the CBF conditions (7.3), (7.5), we obtain the following network-wide optimization problem:

$$\begin{aligned} \min_{\{\mathbf{u}_i \in \mathbb{R}^2\}_{i=1}^N} \quad & \sum_{i=1}^{N} \frac{1}{2} \left\| \Gamma_i(\mathbf{p}_i)(\mathbf{u}_i - u_{\text{nom},i}(\mathbf{p}_i)) \right\|^2 \\ \text{s.t. } & (\mathbf{p}_i - \mathbf{p}_j)^\top (R(\theta_i)L^{-1}\mathbf{u}_i - R(\theta_j)L^{-1}\mathbf{u}_j) \geq -\alpha_c^{ij} d(\mathbf{p}_i, \mathbf{p}_j), \\ & \nabla h_k(\mathbf{p}_i)^\top R(\theta_i)L^{-1}\mathbf{u}_i \geq -\alpha_k(h_k(\mathbf{p}_i) - \eta_k), \ i \in [N], j \in N_i, \ k \in [M]. \end{aligned} \tag{7.7}$$

The presence of the controls $\mathbf{u}_i$ and $\mathbf{u}_j$ in the inter-agent collision avoidance constraints (7.5) means that the satisfaction of such constraints requires coordination between agents involved in the constraint. This, together with the state-dependency of the objective function and constraints, poses challenges in the implementation of a distributed algorithm that solves (7.7). Our goal is to design a distributed controller that satisfies the constraints at all times and with the same optimality properties as the solution obtained directly from solving (7.7).

7.2 An Anytime Algorithm for Distributed Optimization

Motivated by the problem outlined in Section 7.1, in this chapter we consider the problem of designing an algorithm to solve constrained optimization problems in a distributed way and in an anytime fashion (i.e., such that the feasible set is forward invariant). This algorithm will prove crucial to solve the problem in Section 7.1.

We consider a network composed by agents indexed by $[N]$ whose communication topology is described by a connected undirected graph $\mathcal{G}$. An edge (i, j) represents the fact that agent i can receive information from agent j and vice versa. We refer to an algorithm run by the network as *distributed* if each agent can execute it with the information available to it and its neighbors.

For each $i \in [N]$, $k \in [p]$, $l \in [q]$ let $f_i : \mathbb{R}^n \to \mathbb{R}$ be a strongly convex and continuously differentiable function with locally Lipschitz derivatives, $g_i^k : \mathbb{R}^n \to \mathbb{R}$ be a convex and continuously differentiable function with locally Lipschitz derivatives

and $h_i^l : \mathbb{R}^n \to \mathbb{R}$ be an affine function. We let $\mathbf{x} = [\mathbf{x}_1, \ldots, \mathbf{x}_N] \in \mathbb{R}^{nN}$. Consider the following optimization problem with separable objective function and constraints:

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^{nN}} \sum_{i=1}^{N} f_i(\mathbf{x}_i), \\ &\text{s.t.} \quad \sum_{i=1}^{N} g_i^k(\mathbf{x}_i) \leq 0, \quad k \in [p], \\ &\qquad \sum_{i=1}^{N} h_i^l(\mathbf{x}_i) = 0, \quad l \in [q]. \end{aligned} \tag{7.8}$$

Since the objective function is strongly convex and the feasible set is convex, this program has a unique optimizer $\mathbf{x}^*$. Note that, even though the objective function is separable, the structure of the constraints couples the decision variables of the agents. This makes the design of distributed algorithmic solutions of (7.21) challenging.

Remark 7.2.1. (Separability structure): *Problems of the form* (7.21) *arise in multiple applications, including communications [192], economic dispatch of power systems [193], optimal power flow [194], resource allocation [195], and safe swarm behavior using control barrier functions [46]. Also, given convex sets X_i, $i \in [N]$, a common problem considered in the distributed optimization literature [196] is*

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^n} \sum_{i=1}^{N} f_i(\mathbf{x}), \\ &s.t. \quad \mathbf{x} \in \cap_{i=1}^{N} X_i. \end{aligned}$$

When $X_i = \{\mathbf{x} \in \mathbb{R}^n : \bar{g}_i(\mathbf{x}) \leq 0\} \subseteq \mathbb{R}^n$ for a continuously differentiable convex function with locally Lipschitz derivatives $\bar{g}_i : \mathbb{R}^n \to \mathbb{R}^{m_i}$, for $i \in [N]$, the optimization can be reformulated as

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^{nN}} \sum_{i=1}^{N} f_i(\mathbf{x}_i), \\ &s.t. \quad \bar{g}_i(\mathbf{x}_i) \leq 0, \ i \in [N], \\ &\qquad (L \otimes \mathbf{I}_n)\mathbf{x} = \mathbf{0}_{Nn}, \end{aligned}$$

which is of the form (7.21). •

Throughout this section, we denote $f(\mathbf{x}) = \sum_{i=1}^{N} f_i(\mathbf{x}_i)$, $g^k(\mathbf{x}) = \sum_{i=1}^{N} g_i^k(\mathbf{x}_i)$ for $k \in \{1, \dots, p\}$ and $h^l(\mathbf{x}) = \sum_{i=1}^{N} g_i^l(\mathbf{x}_i)$ for $l \in [q]$, and write the feasible set of (7.21) as

$$\mathcal{F} = \{\mathbf{x} \in \mathbb{R}^{nN} : g^k(\mathbf{x}) \leq 0,\ \forall k \in [p],\ h^l(\mathbf{x}) \leq 0,\ \forall l \in [q]\}.$$

We also make the following assumption.

Assumption 3. (Linear independence constraint qualification for separable constraints): *For all* $\mathbf{x} \in \mathbb{R}^{nN}$, *the vectors* $\{\nabla g^k(\mathbf{x})\}_{k \in I_{g^1,\dots,g^p}(\mathbf{x})} \cup \{\nabla h^l(\mathbf{x})\}_{1 \leq l \leq q}$ *are linearly independent.*

Assumption 3 is common and guarantees that the KKT conditions are necessary and sufficient for the optimality of (7.21).

Our goal is to design an algorithm, in the form of a locally Lipschitz dynamical system, such that

(1) is *distributed*, i.e., each agent can execute it with locally available information;

(2) is *anytime*, i.e., the feasible set $\mathcal{F}$ is forward invariant;

(3) *solves* (7.21), i.e., all trajectories starting in $\mathcal{F}$ converge to its optimizer.

Even though algorithmic solutions exist in the literature that enjoy some of these properties (e.g., the projected saddle-point dynamics [197] enjoys (i) and (iii) for certain classes of optimization problems), the design of an algorithm that enjoys all three is challenging.

7.2.1 Design of Algorithmic Solution

Here we propose an algorithmic solution to the constrained program (7.21) to meet the desired requirements. Our exposition proceeds by first reformulating the optimization problem and then building on the projected saddle-point dynamics (cf. [197]) and the safe gradient flow (cf. [98] to synthesize a coordination algorithm with the desired properties.

Reformulation using constraint mismatch variables

Here we provide an equivalent formulation of (7.21) that addresses the coupling among the agents' decision variables arising from the structure of the constraints. The basic idea to "decouple" them is to introduce, following [107], *constraint-mismatch variables* which help agents keep track of local constraints while collectively satisfying the original constraints. Formally, to the state of each agent, we add one variable per constraint: y_i^k for agent i and the kth inequality constraint and z_j^l for agent j and the lth equality constraint. For convenience, we use the notation $\mathbf{x} = [\mathbf{x}_1, \dots, \mathbf{x}_N]$, $\mathbf{y}_i = [y_i^1, \dots, y_i^p]$, $\mathbf{z}_i = [z_i^1, \dots, z_i^p]$, $\mathbf{y} = [\mathbf{y}_1, \dots, \mathbf{y}_N]$, $\mathbf{z} = [\mathbf{z}_1, \dots, \mathbf{z}_N]$. Consider then the following problem

$$\begin{aligned} \min_{\mathbf{x}\in\mathbb{R}^{nN}, \mathbf{y}\in\mathbb{R}^{Np}, \mathbf{z}\in\mathbb{R}^{Nq}} & \sum_{i=1}^{N} f_i(\mathbf{x}_i), \\ \text{s.t.} \quad & g_i^k(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (y_i^k - y_j^k) \leq 0, \\ & h_i^l(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (z_i^k - z_j^k) = 0, \\ & i \in [N],\ k \in [p],\ l \in [q]. \end{aligned} \tag{7.9}$$

Note that, in this formulation, constraints are now locally expressible, meaning that agent $i \in [N]$ can evaluate the ones corresponding to g_i^k and h_i^l with information from its neighbors. Let $\boldsymbol{\mu}_i = [\mu_i^1, \dots, \mu_i^p]$, $\boldsymbol{\lambda}_i = [\lambda_i^1, \dots, \lambda_i^p]$, $\boldsymbol{\lambda} = [\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_N]$ and $\boldsymbol{\mu} = [\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_N]$ be the Lagrange multipliers for the constraints in (7.9).

We next show that the optimizer in $\mathbf{x}$ of (7.9) is $\mathbf{x}^*$, the optimizer of (7.21).

Proposition 7.2.2. (Equivalence between the two formulations): *Let $\mathcal{F}_r^*$ be the solution set of* (7.9)*. Then,* $\mathbf{x}^* = \Pi_{\mathbf{x}}(\mathcal{F}_r^*)$.

Proof. Note that (7.21) is equivalent to

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^{nN},\mathbf{s}\in\mathbb{R}^{p}} \sum_{i=1}^{N} f_i(\mathbf{x}_i), \\ &\text{s.t.} \quad \sum_{i=1}^{N} g_i^k(\mathbf{x}_i) + s^k = 0,\ s^k \geq 0, \\ &\qquad \sum_{i=1}^{N} h_i^l(\mathbf{x}_i) = 0, \\ &\qquad k \in [p],\ l \in [q]. \end{aligned} \tag{7.10}$$

and (7.9) is equivalent to

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^{Nn},\mathbf{y}\in\mathbb{R}^{Np},\mathbf{s}\in\mathbb{R}^{Np},\mathbf{z}\in\mathbb{R}^{Nq}} \sum_{i=1}^{N} f_i(\mathbf{x}_i), \\ &\text{s.t.} \quad g_i^k(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (y_i^k - y_j^k) + s_i^k = 0,\ s_i^k \geq 0, \\ &\qquad h_i^l(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (z_i^l - z_j^l) = 0, \\ &\qquad i \in [N],\ k \in [p],\ l \in [q]. \end{aligned} \tag{7.11}$$

Now the proof follows a similar reasoning as the proof from [107, Proposition 4.2]. We only need to show that the feasible sets of (7.10) and (7.11) are the same, because their objective functions coincide. First, if $(\hat{\mathbf{x}}, \hat{\mathbf{y}}, \hat{\mathbf{s}}, \hat{\mathbf{z}}) \in \mathbb{R}^{Nn}\times\mathbb{R}^{Np}\times\mathbb{R}^{Np}\times\mathbb{R}^{Nq}$ is a feasible point for (7.11), then by adding up all constraints for $i \in [N]$ and letting $\bar{s}^k = \sum_{i=1}^{N} \hat{s}_i^k$, $\bar{\mathbf{s}} = [\bar{s}^1, \ldots, \bar{s}^p]$ it follows that $(\hat{\mathbf{x}}, \bar{\mathbf{s}})$ is a feasible point for (7.10). Now, let $(\tilde{\mathbf{x}}, \tilde{\mathbf{s}})$ be a feasible point for (7.10). Let $\mathbf{v} = [g_1^1(\tilde{\mathbf{x}}_1), \ldots, g_i^k(\tilde{\mathbf{x}}_i), \ldots; g_N^p(\tilde{\mathbf{x}}_N)] \in \mathbb{R}^{Np}$ and $\breve{\mathbf{s}} = [\frac{\tilde{s}^1}{N}, \ldots, \frac{\tilde{s}^1}{N}, \ldots, \frac{\tilde{s}^p}{N}, \ldots, \frac{\tilde{s}^p}{N}] \in \mathbb{R}^{Np}$. Note that $\mathbf{1}_{Np}^{\top}(\mathbf{v} + \breve{\mathbf{s}}) = 0$. This implies that $\mathbf{v} + \breve{\mathbf{s}}$ belongs to the range space of the Laplacian L of the communication graph and hence there exists $\tilde{\mathbf{y}}$ such that $-L\tilde{\mathbf{y}} = \mathbf{v} + \breve{\mathbf{s}}$. By a similar argument, by letting $\mathbf{w} = [h_1^1(\tilde{\mathbf{x}}_1), \ldots, h_i^l(\tilde{\mathbf{x}}_N), \ldots; h_N^p(\tilde{\mathbf{x}}_N)]$ there exists $\tilde{\mathbf{z}}$ such that $-L\tilde{\mathbf{z}} = \mathbf{w}$. Now it follows that $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}, \breve{\mathbf{s}}, \tilde{\mathbf{z}})$ is feasible for (7.10), hence proving that the feasible sets of (7.10) and (7.11) are the same. □

Proposition 7.2.2 implies that (7.9) has a unique optimizer in the variables $\mathbf{x}$. However, since the objective function in (7.9) is not strongly convex in $\mathbf{y}$ and $\mathbf{z}$, the optimizer in the variables $\mathbf{y}$ and $\mathbf{z}$ might not be unique. Hence, for the

results that follow, we take $\epsilon > 0$ and define $f_i^\epsilon(\mathbf{x}_i, \mathbf{y}_i, \mathbf{z}_i) = f_i(\mathbf{x}_i) + \frac{\epsilon}{2}\|\mathbf{y}_i\|^2 + \frac{\epsilon}{2}\|\mathbf{z}_i\|^2$, $f^\epsilon(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{i=1}^N f_i^\epsilon(\mathbf{x}_i, \mathbf{y}_i, \mathbf{z}_i)$. Consider the following regularized version of (7.9),

$$\begin{aligned} \min_{\mathbf{x}\in\mathbb{R}^{Nn}, \mathbf{y}\in\mathbb{R}^{Np}, \mathbf{z}\in\mathbb{R}^{Nq}} & \sum_{i=1}^N f_i^\epsilon(\mathbf{x}_i, \mathbf{y}_i, \mathbf{z}_i), \\ \text{s.t.} \quad & g_i^k(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (y_i^k - y_j^k) \le 0, \\ & h_i^l(\mathbf{x}_i) + \sum_{j\in\mathcal{N}_i} (z_i^k - z_j^k) = 0, \\ & i \in [N],\ k \in [p],\ l \in [q]. \end{aligned} \tag{7.12}$$

Let $(\mathbf{x}^{*,\epsilon}, \mathbf{y}^{*,\epsilon}, \mathbf{z}^{*,\epsilon}) \in \mathbb{R}^{Nn}\times\mathbb{R}^{Np}\times\mathbb{R}^{Nq}$ be the optimizer of (7.12), which is unique because the objective function is strongly convex and the feasible set is convex. Next we establish a sensitivity result for the regularized optimization problem (7.12).

Lemma 7.2.3. (Sensitivity of regularized problem): *Given $\delta > 0$, there exists $\bar{\epsilon} > 0$ so that if $\epsilon < \bar{\epsilon}$, then $\|\mathbf{x}^{*,\epsilon} - \mathbf{x}^*\| < \delta$.*

Proof. Let $(\mathbf{x}^*, \mathbf{y}^*, \mathbf{z}^*)$ be an optimizer of (7.9) with $m = f(\mathbf{x}^*, \mathbf{y}^*, \mathbf{z}^*)$. Since $\mathbf{x}^*$ is unique, there exists $\beta > 0$ such that $f(\mathbf{x}) = f^0(\mathbf{x}, \mathbf{y}, \mathbf{z}) \ge m + \beta$, for all $\mathbf{x} \in \mathcal{F}$, $\mathbf{y} \in \mathbb{R}^{Np}$, $\mathbf{z} \in \mathbb{R}^{Nq}$ whenever $\|\mathbf{x} - \mathbf{x}^*\| = \delta$. Hence, for any $\epsilon > 0$ it follows that

$$f^\epsilon(\mathbf{x}, \mathbf{y}, \mathbf{z}) \ge f^0(\mathbf{x}, \mathbf{y}, \mathbf{z}) \ge m + \beta,$$

for all $\mathbf{x} \in \mathcal{F}$, $\mathbf{y} \in \mathbb{R}^{Np}$, $\mathbf{z} \in \mathbb{R}^{Nq}$ whenever $\|\mathbf{x} - \mathbf{x}^*\| = \delta$. On the other hand, since f is continuous with respect to ϵ, for any $\delta > 0$ we can find $\bar{\epsilon}$ such that

$$f^\epsilon(\mathbf{x}^*, \mathbf{y}^*, \mathbf{z}^*) \le m + \frac{\beta}{2} \quad \forall \epsilon < \bar{\epsilon}.$$

Hence, by taking $\epsilon < \bar{\epsilon}$ we can ensure that the set

$$\{(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathcal{F} \times \mathbb{R}^{Np} \times \mathbb{R}^{Nq} : \|\mathbf{x} - \mathbf{x}^*\| \le \delta\}$$

contains the local minimizer of f^ϵ for any $\epsilon < \bar{\epsilon}$. Thus, $\|\mathbf{x}^{*,\epsilon} - \mathbf{x}^*\| \le \delta$ for all $\epsilon < \bar{\epsilon}$, as stated. □

Given Lemma 7.2.3, in what follows we focus on solving (7.12) and assume that ϵ is taken sufficiently small to guarantee a desired maximum distance between $\mathbf{x}^{*,\epsilon}$ and $\mathbf{x}^*$.

Cascade of saddle-point dynamics and safe gradient flow

Here, we build on the reformulation presented above to design our proposed algorithmic solution. Note that, if we had knowledge of the optimizers $\mathbf{y}^{*,\epsilon}, \mathbf{z}^{*,\epsilon}$ of Problem (7.12), we could break the optimization into N, one per agent $i \in [N]$, decoupled optimization problems as follows,

$$\begin{aligned} &\min_{\mathbf{x}_i \in \mathbb{R}^n} f_i^\epsilon(\mathbf{x}_i), \\ &\text{s.t.} \quad g_i^k(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} ((y_i^k)^{*,\epsilon} - (y_j^k)^{*,\epsilon}) \leq 0, \\ &\qquad h_i^l(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} ((z_i^k)^{*,\epsilon} - (z_j^k)^{*,\epsilon}) = 0, \\ &\qquad k \in [p],\ l \in [q]. \end{aligned} \tag{7.13}$$

In turn, each of these problems could be solved in an anytime fashion by having each agent execute the corresponding safe gradient flow (cf. [98]). However, since $\mathbf{y}^{*,\epsilon}$ and $\mathbf{z}^{*,\epsilon}$ are not readily available, agents need to interact with their neighbors to compute them. Since this would require an iterative algorithm, this means agents will face evolving $\mathbf{y}$ and $\mathbf{z}$ in the corresponding formulation of (7.13), which raises the additional challenge of ensuring the anytime nature of the safe gradient flow is preserved. We tackle these challenges next.

To generate the update law for $\mathbf{y}$ and $\mathbf{z}$, we propose to use the projected saddle-point dynamics of (7.12). By [197, Theorem 5.1], these are guaranteed to converge to its optimizers. Simultaneously, we implement the safe gradient flow of (7.13) with the current values of $\mathbf{y}$ and $\mathbf{z}$, i.e., (with the notation $\mathbf{y}_{\mathcal{N}_i} = \mathbf{y}_i \cup \{\mathbf{y}_j\}_{j \in \mathcal{N}_i}$, $\mathbf{z}_{\mathcal{N}_i} = \mathbf{z}_i \cup \{\mathbf{z}_j\}_{j \in \mathcal{N}_i}$):

$$\begin{aligned} S_\alpha^i(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}) = &\arg\min_{\boldsymbol{\xi}_i \in \mathbb{R}^n} \frac{1}{2} \left\| \boldsymbol{\xi}_i + \nabla f_i(\mathbf{x}_i) \right\|^2, \\ &\text{s.t. } \nabla g_i^k(\mathbf{x}_i) \boldsymbol{\xi}_i \leq -\alpha(g_i^k(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} (y_i^k - y_j^k)), \\ &\nabla h_i^l(\mathbf{x}_i) \boldsymbol{\xi}_i = -\alpha(h_i^l(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} (z_i^l - z_j^l)), \\ &k \in [p],\ l \in [q], \end{aligned} \tag{7.14}$$

for all $i \in [N]$. We denote $S_\alpha(\mathbf{x}, \mathbf{y}, \mathbf{z}) = [S_\alpha^1(\mathbf{x}_1, \mathbf{y}_{\mathcal{N}_1}, \mathbf{z}_{\mathcal{N}_1}), \ldots, S_\alpha^N(\mathbf{x}_N, \mathbf{y}_{\mathcal{N}_N}, \mathbf{z}_{\mathcal{N}_N})]$. To add more flexibility to our design, we add a timescale separation parameter

$\tau > 0$ that allows the projected saddle-point dynamics to be run at a faster rate relative to the safe gradient flow. This leads to the cascaded dynamical system:

$$\tau \dot{\mathbf{v}}_i = -\nabla f_i(\mathbf{v}_i) - \sum_{k=1}^{p} \lambda_i^k \nabla g_i^k(\mathbf{v}_i), \tag{7.15a}$$

$$\tau \dot{y}_i^k = -\epsilon y_i^k - \sum_{j \in \mathcal{N}_i} (\lambda_i^k - \lambda_j^k), \tag{7.15b}$$

$$\tau \dot{z}_i^l = -\epsilon z_i^l - \sum_{j \in \mathcal{N}_i} (\mu_i^l - \mu_j^l), \tag{7.15c}$$

$$\tau \dot{\lambda}_i^k = [g_i^k(\mathbf{v}_i) + \sum_{j \in \mathcal{N}_i} (y_i^k - y_j^k)]_{\lambda_i^k}^+, \tag{7.15d}$$

$$\tau \dot{\mu}_i^l = h_i^l(\mathbf{v}_i) + \sum_{j \in \mathcal{N}_i} (z_i^k - z_j^k), \tag{7.15e}$$

$$\dot{\mathbf{x}}_i = S_\alpha^i(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}), \tag{7.15f}$$

for $i \in [N]$, $k \in [p]$ and $l \in [q]$, where $\mathbf{v}_i$ are *virtual* variables that play the role of $\mathbf{x}_i$ in the projected saddle-point dynamics. Since (7.15) results from the cascaded interconnection of saddle-point dynamics and the safe gradient flow, we refer to it as SP-SGF.

Remark 7.2.4. (Scalability and distributed character of SP-SGF): In algorithm (7.15), each agent has a state variable of dimension $2n + 2p + 2q$. To compute the evolution of these state variables, each agent only requires information provided by its neighbors in $\mathcal{G}$. Therefore, the algorithm is distributed. In addition, since the memory needed by each agent to run (7.15) remains constant as the network size N increases, the algorithm is also scalable. •

Remark 7.2.5. (Algorithm implementation): *Note that the execution of SP-SGF requires solving the optimization problem* (7.14)*, for each $i \in [N]$, which is a quadratic program and hence can be solved efficiently. In fact, if the number of constraints is low, closed-form expressions for its solution [35, Theorem 1] are available.* •

In what follows, we assume that for all $i \in [N]$, the set of initial conditions for $\mathbf{v}_i$, $\mathbf{y}_i$, $\mathbf{z}_i$, λ_i and μ_i in (7.15) lie in compact sets $\mathcal{V}_i$, $\mathcal{Y}_i$, $\mathcal{Z}_i$, Λ_i and M_i respectively. This means that the initial conditions $\mathbf{v}, \mathbf{y}, \mathbf{z}, \boldsymbol{\lambda}, \boldsymbol{\mu}$ lie in compact sets $\mathcal{V} := \times_{i=1}^N \mathcal{V}_i$,

$\mathcal{Y} \coloneqq \bigtimes_{i=1}^{N} \mathcal{Y}_i$, $\mathcal{Z} \coloneqq \bigtimes_{i=1}^{N} \mathcal{Z}_i$, $\Lambda = \bigtimes_{i=1}^{N} \Lambda_i$, $M = \bigtimes_{i=1}^{N} M_i$. Since the projected saddle-point dynamics (7.15a)-(7.15e) are convergent by [197, Theorem 5.1], there exist compact sets $\bar{\mathcal{V}}$, $\bar{\mathcal{Y}}$, $\bar{\mathcal{Z}}$, $\bar{\Lambda}$, $\bar{M}$ such that the trajectories of $\mathbf{v}, \mathbf{y}, \mathbf{z}, \boldsymbol{\lambda}, \boldsymbol{\mu}$ under (7.15) stay in $\bar{\mathcal{V}}$, $\bar{\mathcal{Y}}$, $\bar{\mathcal{Z}}$, $\bar{\Lambda}$ and $\bar{M}$ respectively for all positive times. In what follows, we make the following assumption regarding the feasibility of (7.14).

Assumption 4. (Feasibility of S_α): *For all $i \in [N]$, (7.14) is feasible for all $(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}) \in \Pi_{\mathbf{x}_i} \mathcal{F} \times \Pi_{\mathbf{y}_{\mathcal{N}_i}} \bar{\mathcal{Y}} \times \Pi_{\mathbf{z}_{\mathcal{N}_i}} \bar{\mathcal{Z}}$.*

The following result gives a sufficient condition under which Assumption 4 holds.

Lemma 7.2.6. (Sufficient condition for feasibility of S_α): *Suppose that the vectors $\{\nabla g_i^k(\mathbf{x}_i)\}_{k=1}^{p} \cup \{\nabla h_i^l(\mathbf{x}_i)\}_{l=1}^{q}$ are linearly independent for all $\mathbf{x}_i \in \Pi_{\mathbf{x}_i} \mathcal{F}$. Then, for all $i \in [N]$, (7.14) is feasible for all $(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}) \in \Pi_{\mathbf{x}_i} \mathcal{F} \times \Pi_{\mathbf{y}_{\mathcal{N}_i}} \bar{\mathcal{Y}} \times \Pi_{\mathbf{z}_{\mathcal{N}_i}} \bar{\mathcal{Z}}$.*

Proof. By considering the inequality constraints in (7.14) as equality constraints, and since $p + q \leq n$ necessarily, (7.14) consists of a linear system of equations with at least as many unknowns as equations. If the number of equations is strictly less than the number of unknowns (i.e., $p + q < n$), (7.14) is feasible. If the number of equations is equal to the number of unknowns, (i.e., $p + q = n$), (7.14) is feasible because $\{\nabla g_i^k(\mathbf{x}_i)\}_{k=1}^{p} \cup \{\nabla h_i^l(\mathbf{x}_i)\}_{l=1}^{q}$ are linearly independent for all $\mathbf{x}_i \in \Pi_{\mathbf{x}_i} \mathcal{F}$. □

The next result establishes some feasibility and regularity properties of S_α. Its proof follows an argument analogous to the proof of [98, Proposition 5.3].

Proposition 7.2.7. (Well-posedness and regularity of SP-SGF): *Under Assumption 4, the following statements hold:*

- *There exists an open neighborhood U containing $\bar{\mathcal{V}} \times \bar{\mathcal{Y}} \times \bar{\mathcal{Z}} \times \bar{\Lambda} \times \bar{M} \times \mathcal{F}$ such that (7.15) is well-defined on U;*
- *The dynamical system (7.15) is locally Lipschitz on U;*
- *The Lagrange multipliers of (7.14) are unique and locally Lipschitz as a function of $\mathbf{x}, \mathbf{y}$ and $\mathbf{z}$ on U.*

7.2.2 Invariance and Convergence Analysis

Having established the distributed character of the algorithm (7.15), here we show the forward invariance of the feasible set and the asymptotic convergence to the optimizer.

We start by introducing some useful notation. For $i \in [N]$, $k \in [p]$ and $l \in [q]$, we let $\psi_{y_i^k}(t;\mathbf{p}_0), \psi_{z_j^l}(t;\mathbf{p}_0), \psi_{\mathbf{x}_i}(t;\mathbf{p}_0)$ be the solution of (7.15b), (7.15c), (7.15f) respectively for initial conditions $\mathbf{p}_0 = (\mathbf{v}_0, \mathbf{y}_0, \mathbf{z}_0, \boldsymbol{\lambda}_0, \boldsymbol{\mu}_0, \mathbf{x}_0) \in \mathcal{P} := \mathcal{V}\times\mathcal{Y}\times\mathcal{Z}\times\Lambda\times M\times\mathcal{F}$. We also let $\psi_{\mathbf{y}}(t;\mathbf{p}_0) = [\psi_{y_1^1}(t;\mathbf{p}_0), \ldots, \psi_{y_1^p}(t;\mathbf{p}_0), \ldots, \psi_{y_N^1}(t;\mathbf{p}_0), \ldots, \psi_{y_N^p}(t;\mathbf{p}_0)]$, and define $\psi_{\mathbf{z}}(t;\mathbf{p}_0)$ and $\psi_{\mathbf{x}}(t;\mathbf{p}_0)$ analogously. The next result establishes the *anytime* nature of SP-SGF.

Lemma 7.2.8. (Anytime property): *Suppose that $\mathbf{x}_0 \in \mathcal{F}$ and Assumption 4 holds. Then, the trajectories of* (7.15) *satisfy $\psi_{\mathbf{x}}(t;\mathbf{p}_0) \in \mathcal{F}$ for all $t \geq 0$.*

Proof. Since Assumption 4 holds, the dynamics (7.15) are well-defined on a neighborhood U, cf. Proposition 7.2.7. If, at some $\bar{t}$, $\sum_{i=1}^N g_i^k(\psi_{\mathbf{x}_i}(\bar{t};\mathbf{p}_0)) = 0$ for $k \in [p]$, then because of the constraints in (7.14),

$$\begin{aligned}
&\frac{d}{dt}\sum_{i=1}^N g_i^k(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0))|_{t=\bar{t}} \\
&= \sum_{i=1}^N \nabla g_i^k(\psi_{\mathbf{x}_i}(\bar{t};\mathbf{p}_0)) S_\alpha^i(\psi_{x_i}(\bar{t};\mathbf{p}_0), \psi_{y_{\mathcal{N}_i}}(\bar{t};\mathbf{p}_0), \psi_{z_{\mathcal{N}_i}}(\bar{t};\mathbf{p}_0)) \\
&\leq -\alpha \sum_{i=1}^N \Big(g_i^k(\psi_{\mathbf{x}_i}(\bar{t};\mathbf{p}_0)) + \sum_{j\in\mathcal{N}_i} (\psi_{y_i^k}(\bar{t};\mathbf{p}_0) - \psi_{y_j^k}(\bar{t};\mathbf{p}_0)) \Big) = 0.
\end{aligned}$$

Hence by Brezis' Theorem [198], it follows that $\sum_{i=1}^N g_i^k(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0)) \leq 0$ for all $t \geq 0$, $\mathbf{p}_0 \in \mathcal{P}$ and $k \in [p]$. By a similar argument, $\frac{d}{dt}\sum_{i=1}^N h_i^l(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0))|_{t=\bar{t}} = 0$. Hence, it follows that $\sum_{i=1}^N h_i^l(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0)) = 0$ for all $t \geq 0$, $\mathbf{p}_0 \in \mathcal{P}$ and $l \in \{1,\ldots,q\}$. □

Next, we turn to the study of the convergence properties of (7.15). The next result establishes a connection between the equilibrium points of S_α and the optimizers of (7.12).

Proposition 7.2.9. (Relationship between equilibria and optimizers): *Let $\mathbf{x} \in \mathcal{F}$. Then, $S_\alpha(\mathbf{x}, \mathbf{y}^{*,\epsilon}, \mathbf{z}^{*,\epsilon}) = 0$ if and only if $\mathbf{x} = \mathbf{x}^{*,\epsilon}$.*

Proof. Note that $S^i_\alpha(\mathbf{x}_i, \mathbf{y}^{*,\epsilon}_{\mathcal{N}_i}, \mathbf{z}^{*,\epsilon}_{\mathcal{N}_i})$ is the safe gradient flow associated to the optimization problem (7.13), which by Proposition 7.2.2 has $\mathbf{x}_i^{*,\epsilon}$ as the unique optimizer. The result then follows from [98, Proposition 5.1]. □

Next we show that the trajectories of $\mathbf{x}$ in (7.15) converge to the optimizer of (7.12).

Theorem 7.2.10. (Convergence to optimizer): *Suppose Assumption 4 holds. For any $\delta > 0$ and compact set Ω containing $\{\mathbf{x} \in \mathcal{F} : \|\mathbf{x} - \mathbf{x}^{*,\epsilon}\| \leq \delta\}$, there exists $\tau_{\delta,\Omega} > 0$ and $T_{\delta,\Omega}$ such that if $\tau < \tau_{\delta,\Omega}$, then under the dynamics* (7.15)*:*

$$\|\psi_{\mathbf{x}}(t; \mathbf{p}_0) - \mathbf{x}^{*,\epsilon}\| < \delta,$$

for all $t \geq T_{\delta,\Omega}$ and $\mathbf{p}_0 = (\mathbf{v}_0, \mathbf{y}_0, \mathbf{z}_0, \boldsymbol{\lambda}_0, \boldsymbol{\mu}_0, \mathbf{x}_0) \in \mathcal{P}$. Moreover, if $\mathcal{F}$ is bounded, then for any $\tau > 0$,

$$\lim_{t\to\infty} \|\psi_{\mathbf{x}}(t; \mathbf{p}_0) - \mathbf{x}^{*,\epsilon}\| = 0.$$

for all $\mathbf{p}_0 \in \mathcal{P}$.

Proof. Since the dynamics in (7.15) are not differentiable, the standard version of Tikhonov's theorem for singular perturbations [199, Theorem 11.2] is not applicable. Instead we use [200, Corollary 3.4], which gives a Tikhonov-type singular perturbation statement for differential inclusions. In the case of non-smooth ODEs for which the fast dynamics do not depend on the slow variable, like (7.15), we need to check the following assumptions. First, that the dynamics (7.15) are Lipschitz. Note that local Lipschitzness of (7.15) follows from Proposition 7.2.7, the Lipschitzness of the gradients of f and g and the Lipschitzness of the max operator. Moreover, since $\bar{\mathcal{V}}$, $\bar{\mathcal{Y}}$, $\bar{\mathcal{Z}}$, $\bar{\Lambda}$, $\bar{M}$ and Ω are compact, we can redefine the dynamics (7.15) outside of $\bar{\mathcal{V}} \times \bar{\mathcal{Y}} \times \bar{\mathcal{Z}} \times \bar{\Lambda} \times \bar{M} \times \Omega$ so that they are globally Lipschitz while still keeping the same dynamics for initial conditions in $\mathcal{V} \times \mathcal{Y} \times \mathcal{Z} \times \Lambda \times M \times \Omega$. Second, existence and uniqueness of the equilibrium of the fast dynamics. This follows from the fact that (7.12) has a strongly convex objective function and convex constraints, which implies that it has a unique KKT point. Third, Lipschitzness and asymptotic stability of the reduced-order model

$$\dot{\bar{\mathbf{x}}} = S_\alpha(\bar{\mathbf{x}}, \mathbf{y}^{*,\epsilon}, \mathbf{z}^{*,\epsilon}) \tag{7.16}$$

Lipschitzness follows from Proposition 7.2.7 and asymptotic stability follows from [98, Theorem 5.6] and the fact that Ω is compact. Fourth, asymptotic stability of the fast dynamics. This follows from [197, Theorem 5.1]. Finally, note that $\mathbf{x}^{*,\epsilon}$ is the only equilibrium point of (7.27) and hence the result follows from [200, Corollary 3.4].

Now suppose that $\mathcal{F}$ is compact. Pick an arbitrary $\theta > 0$. Since f is continuous and $\mathbf{x}^{*,\epsilon}$ is the unique minimizer of (7.12), there exist constants $a_\theta > 0$, $b_\theta > 0$ such that the sets

$$A_\theta = \{\mathbf{x} \in \mathcal{F} : f(\mathbf{x}) - f(\mathbf{x}^{*,\epsilon}) \leq a_\theta\}$$
$$B_\theta = \{\mathbf{x} \in \mathcal{F} : \|\mathbf{x} - \mathbf{x}^{*,\epsilon}\| \leq b_\theta\}$$
$$C_\theta = \{\mathbf{x} \in \mathcal{F} : \|\mathbf{x} - \mathbf{x}^{*,\epsilon}\| \leq \theta\}$$

satisfy $B_\theta \subseteq A_\theta \subseteq C_\theta$. Next, we show that there exists $T_\theta > 0$ such that $\psi_{\mathbf{x}}(t; \mathbf{p}_0) \in C_\theta$ for $t \geq T_\theta$ and all $\mathbf{p}_0 \in \mathcal{P}$ (i.e., C_θ is asymptotically stable relative to $\mathcal{F}$). Since θ is arbitrary, this completes the proof. Let $(\{\phi_i^k(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i})\}_{k=1}^p, \{\chi_i^l(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i})\}_{l=1}^q)$ be the Lagrange multipliers associated to the optimization problem defining the function $S_\alpha^i(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i})$, which are unique and locally Lipschitz by Proposition 7.2.7. Then, by following an argument analogous to the one in the proof of [98, Lemma 5.8]:

$$\frac{d}{dt}(f(x) - f(x^{*,\epsilon})) \leq -\|S_\alpha(\mathbf{x}, \mathbf{y}, \mathbf{z})\|^2 + \sum_{i=1}^N \sum_{k=1}^p \phi_i^k(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}) \alpha(g_i^k(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} (y_i^k - y_j^k))$$
$$+ \sum_{i=1}^N \sum_{l=1}^q \chi_i^l(\mathbf{x}_i, \mathbf{y}_{\mathcal{N}_i}, \mathbf{z}_{\mathcal{N}_i}) \alpha(h_i^l(\mathbf{x}_i) + \sum_{j \in \mathcal{N}_i} (z_i^k - z_j^k)). \tag{7.17}$$

Since (7.15a)-(7.15e) are the projected saddle-point dynamics of (7.12) and the objective function of (7.12) is strongly convex, by [197, Theorem 5.1], the variables $\mathbf{v}, \mathbf{y}, \mathbf{z}, \boldsymbol{\lambda}, \boldsymbol{\mu}$ converge to the KKT point of (7.12) for all $\tau > 0$. Moreover, since $S_\alpha(\mathbf{x}, \mathbf{y}^{*,\epsilon}, \mathbf{z}^{*,\epsilon}) = 0$ if and only if $\mathbf{x} = \mathbf{x}^{*,\epsilon}$ by Proposition 7.2.9, S_α is continuous by Proposition 7.2.7 and $\mathcal{P}$ is compact, for any fixed $\tau > 0$, there exist $\sigma_{\theta,\tau}$ and $T_{1,\theta,\tau}$ such that for all $t \geq T_{1,\theta,\tau}$ and $\mathbf{p}_0 \in \mathcal{P}$, $\|\psi_{\mathbf{x}}(t; \mathbf{p}_0) - \mathbf{x}^{*,\epsilon}\| > b_\theta$ implies $\|S_\alpha(\psi_{\mathbf{x}}(t; \mathbf{p}_0), \psi_{\mathbf{y}}(t; \mathbf{p}_0), \psi_{\mathbf{z}}(t; \mathbf{p}_0))\| > \sigma_{\theta,\tau}$.

Now, define

$$\hat{g}_i^k(t,\mathbf{p}_0) = g_i^k(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0)) + \sum_{j\in\mathcal{N}_i}(\psi_{y_i^k}(t;\mathbf{p}_0) - \psi_{y_j^k}(t;\mathbf{p}_0)),$$
$$\hat{h}_i^l(t,\mathbf{p}_0) = h_i^l(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0)) + \sum_{j\in\mathcal{N}_i}(\psi_{z_i^l}(t;\mathbf{p}_0) - \psi_{z_j^l}(t;\mathbf{p}_0)),$$
$$\hat{\phi}_i^k(t,\mathbf{p}_0) = \phi_i^k(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0), \psi_{\mathbf{y}_{\mathcal{N}_i}}(t;\mathbf{p}_0), \psi_{\mathbf{z}_{\mathcal{N}_i}}(t;\mathbf{p}_0)),$$
$$\hat{\chi}_i^l(t,\mathbf{p}_0) = \chi_i^l(\psi_{\mathbf{x}_i}(t;\mathbf{p}_0), \psi_{\mathbf{y}_{\mathcal{N}_i}}(t;\mathbf{p}_0), \psi_{\mathbf{z}_{\mathcal{N}_i}}(t;\mathbf{p}_0)),$$

and let us show that there exists a time $T_{2,\theta,\tau} > 0$ such that

$$\alpha\sum_{i=1}^{N}\sum_{k=1}^{p}\hat{\phi}_i^k(t,\mathbf{p}_0)\hat{g}_i^k(t,\mathbf{p}_0) + \alpha\sum_{i=1}^{N}\sum_{l=1}^{q}\hat{\chi}_i^l(t,\mathbf{p}_0)\hat{h}_i^l(t,\mathbf{p}_0) < \frac{\sigma_{\theta,\tau}}{2}, \tag{7.18}$$

for all $t \geq T_{2,\theta}$ and $p_0 \in \mathcal{P}$. First define

$$c_\phi := \max_{\substack{(\mathbf{x},\mathbf{y},\mathbf{z})\in\mathcal{F}\times\bar{\mathcal{Y}}\times\bar{\mathcal{Z}}\\ i\in[N],k\in[p]}} |\phi_i^k(\mathbf{x}_i,\mathbf{y}_{\mathcal{N}_i},\mathbf{z}_{\mathcal{N}_i})|,$$
$$c_\chi := \max_{\substack{(\mathbf{x},\mathbf{y},\mathbf{z})\in\mathcal{F}\times\bar{\mathcal{Y}}\times\bar{\mathcal{Z}}\\ i\in[N],l\in[q]}} |\chi_i^l(\mathbf{x}_i,\mathbf{y}_{\mathcal{N}_i},\mathbf{z}_{\mathcal{N}_i})|.$$

Note that such c_ϕ, c_χ exist because $\mathcal{F}$, $\bar{\mathcal{Y}}$ and $\bar{\mathcal{Z}}$ are compact. Now note that

$$\frac{d}{dt}(\hat{g}_i^k(t,\mathbf{p}_0)) \leq -\alpha\hat{g}_i^k(t,\mathbf{p}_0) + \sum_{j\in\mathcal{N}_i}(\dot{\psi}_{y_i^k}(t;\mathbf{p}_0) - \dot{\psi}_{y_j^k}(t)),$$
$$\frac{d}{dt}(\hat{h}_i^l(t,\mathbf{p}_0)) \leq -\alpha\hat{h}_i^l(t,\mathbf{p}_0) + \sum_{j\in\mathcal{N}_i}(\dot{\psi}_{z_i^l}(t;\mathbf{p}_0) - \dot{\psi}_{z_j^l}(t)).$$

Since the variables y_i^k, z_i^k are convergent by [197, Theorem 5.1],

$$\lim_{t\to\infty}\dot{\psi}_{y_i^k}(t;\mathbf{p}_0) = 0, \quad \forall i \in [N],\ k \in [p],$$
$$\lim_{t\to\infty}\dot{\psi}_{z_i^l}(t;\mathbf{p}_0) = 0, \quad \forall i \in [N],\ l \in [q].$$

for all $\mathbf{p}_0 \in \mathcal{P}$. Hence, there exists a time $\hat{T}_{2,\theta,\tau} > 0$ such that

$$\sum_{j\in\mathcal{N}_i}(\dot{\psi}_{y_i^k}(t;\mathbf{p}_0) - \dot{\psi}_{y_j^k}(t)) \leq \frac{\sigma_{\theta,\tau}}{8\alpha N p c_\phi},$$
$$\sum_{j\in\mathcal{N}_i}(\dot{\psi}_{z_i^l}(t;\mathbf{p}_0) - \dot{\psi}_{z_j^l}(t)) \leq \frac{\sigma_{\theta,\tau}}{8\alpha N p c_\chi}$$

for all $i \in [N]$, $k \in [p]$, $l \in [q]$ and $t \geq \hat{T}_{2,\theta,\tau}$, $\mathbf{p}_0 \in \mathcal{P}$. By the Comparison Lemma [199, Lemma 3.4], it holds that

$$\hat{g}_i^k(t, \mathbf{p}_0) \leq \hat{g}_i^k(\hat{T}_{2,\theta,\tau}, \mathbf{p}_0) e^{-\alpha(t-\hat{T}_{2,\theta,\tau})} + \frac{\sigma_{\theta,\tau}}{8Npc_\phi},$$
$$\hat{h}_i^l(t, \mathbf{p}_0) \leq \hat{h}_i^l(\hat{T}_{2,\theta,\tau}, \mathbf{p}_0) e^{-\alpha(t-\hat{T}_{2,\theta,\tau})} + \frac{\sigma_{\theta,\tau}}{8Npc_\chi}.$$

Since $\mathcal{F}$ is compact, $\psi_x(t; \mathbf{p}_0) \in \mathcal{F}$ by Lemma 7.2.8, $\psi_y(t; \mathbf{p}_0) \in \bar{\mathcal{Y}}$ and $\psi_{\mathbf{z}}(t; \mathbf{p}_0) \in \bar{\mathcal{Z}}$ for all $t \geq 0$, this implies that there exists a time $T_{2,\theta,\tau} > 0$ such that (7.18) holds for all $t \geq T_{2,\theta,\tau}$ and $\mathbf{p}_0 \in \mathcal{P}$. Now, let $T_{\theta,\tau} = \max\{T_{1,\theta,\tau}, T_{2,\theta,\tau}\}$. Then, it holds that for all $t \geq T_{\theta,\tau}$, $\frac{d}{dt}(f(\psi_{\mathbf{x}}(t; \mathbf{p}_0)) - f(\mathbf{x}^{*,\epsilon})) < 0$ if $\|\psi_{\mathbf{x}}(t; \mathbf{p}_0) - x^{*,\epsilon}\| > b_\theta$. Since $B_\theta \subseteq A_\theta$, this implies that A_θ is asymptotically stable relative to $\mathcal{F}$. Since $A_\theta \subseteq C_\theta$, it follows that C_θ is asymptotically stable relative to $\mathcal{F}$, hence completing the proof. Note that this argument is valid for all fixed $\tau > 0$. □

By Theorem 7.2.10, the trajectories of the $\mathbf{x}$ variable in SP-SGF converge arbitrarily close to the optimizer $\mathbf{x}^{*,\epsilon}$ provided that the timescale parameter τ is small enough. Moreover, if the feasible set $\mathcal{F}$ is bounded, asymptotic convergence holds for any timescale. The combination of the scalable and distributed character, cf. Remark 7.2.4, the anytime nature, cf. Lemma 7.2.8, and the convergence properties, cf. Theorem 7.2.10 means that SP-SGF provides an algorithmic solution that is distributed, anytime, and solves (7.21).

Example 7.2.11. (Resource allocation): We illustrate the behavior of SP-SGF in a resource allocation example. Consider 13 agents whose communication graph is an undirected line graph. Solving distributed optimization problems with this particular topology is challenging due to its low connectivity. Each agent's state variable is $\mathbf{x}_i = [x_{i,1}, x_{i,2}] \in \mathbb{R}^2$, where $x_{i,1}$ (resp. $x_{i,2}$) corresponds to the amount of resource 1 (resp. 2) allocated by agent i. Resource 1 is subject to an equality constraint and resource 2 is subject to an inequality constraint. Hence, the agents

solve the optimization problem,

$$\min_{\{\mathbf{x}_i\}_{i=1}^{13}} \sum_{i=1}^{13} \frac{1}{2} \|\mathbf{x}_i\|^2, \tag{7.19}$$
$$\text{s.t. } h(\{\mathbf{x}_i\}_{i=1}^{13}) = 5 - \sum_{i=1}^{13} p_i x_{i,1} = 0,$$
$$g(\{\mathbf{x}_i\}_{i=1}^{13}) = -3 + \sum_{i=1}^{13} e^{-x_{i,2}} \leq 0.$$

with $p_1 = 1$, $p_2 = 3$, $p_3 = 2$, $p_4 = 1$, $p_5 = 1$, $p_6 = 1$, $p_7 = 2$, $p_8 = 4$, $p_9 = 1$, $p_{10} = 1$, $p_{11} = 0.5$, $p_{12} = 2$, $p_{13} = 1$. Note that the condition in Lemma 7.2.6 holds and hence Assumption 4 holds. This implies by Proposition 7.2.10 that (7.15) is well-defined for (7.19). We use $\epsilon = 0.0001$ and $\alpha = 1$. Figure 7.1 illustrates the convergence of the x variables under SP-SGF.

Since the feasible set of (7.19) is unbounded, Proposition 7.2.10 states that convergence arbitrarily close to the optimizer can be achieved by taking τ sufficiently small. Figure 7.2 illustrates the convergence of the quantities $\sum_{i=1}^{13} x_{i,1}^2$ and $\sum_{i=1}^{13} x_{i,2}^2$ for different values of τ and shows that this quantity converges exactly to its optimal value for a wide range of values of τ, suggesting that the statement in Proposition 7.2.10 might be too conservative.

Figure 7.3 compares the evolution of the constraints of (7.19) under SP-SGF against two other algorithms: the projected saddle point dynamics (abbreviated SP), which is not distributed, and the projected saddle-point dynamics (abbreviated SP-CM) for its reformulation with constraint mismatch variables as in (7.9), which is distributed. SP-SGF satisfies the constraints at all times whereas SP and SP-CM do not. We note that, in this case, SP-SGF requires running a dynamical system with 104 scalar variables (8 for each agent), SP-CM requires running a dynamical system of 78 scalar variables (6 for each agent) and SP requires running a dynamical system with 28 scalar variables. •

7.3 Distributed Controller Design

In this section we design a distributed algorithmic solution to the problem formulated in Section 7.1. As it turns out, our solution builds upon [10] and

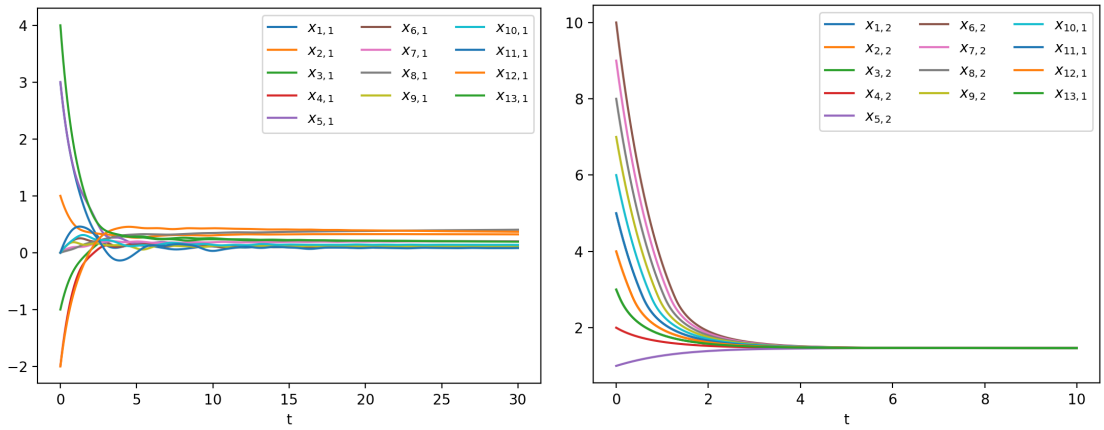


Figure 7.1: Evolution of the variables $x_{1,i}$ (top) and $x_{2,i}$ (bottom) for $i \in \{1, \dots, 13\}$ under SP-SGF for (7.19) with initial conditions $\mathbf{x}_1 = [3,5]$, $\mathbf{x}_2 = [1,4]$, $\mathbf{x}_3 = [-1,3]$, $\mathbf{x}_4 = [-2,2]$, $\mathbf{x}_5 = [3,1]$, $\mathbf{x}_6 = [0,10]$, $\mathbf{x}_7 = [0,9]$, $\mathbf{x}_8 = [0,8]$, $\mathbf{x}_9 = [0,7]$, $\mathbf{x}_{10} = [0,6]$, $\mathbf{x}_{11} = [0,5]$, $\mathbf{x}_{12} = [-2,4]$, $\mathbf{x}_{13} = [4,3]$, $v_{i,1} = v_{i,2} = z_i = y_i = \lambda_i = \mu_i = 0$ for all $i \in [13]$ and $\tau = 1$.

is valid for a more general setup, as we explain next. Assume that the agents' communication network is described by a connected undirected graph $\mathcal{G}$, as in Section 7.1. An edge (i, j) represents the fact that agent i can receive information from agent j and vice versa. We describe the dynamics of each agent $i \in [N]$ by

$$\dot{\boldsymbol{\xi}}_i = F_i(\boldsymbol{\xi}_i, \mathbf{u}_i) \tag{7.20}$$

where $F_i : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is a locally Lipschitz function for each $i \in [N]$, $\boldsymbol{\xi}_i \in \mathbb{R}^n$ is the state variable of agent i and $\mathbf{u}_i \in \mathbb{R}^m$ is its local control input. Additionally, let $f_i : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ and $g_i^k : \mathbb{R}^{n|\mathcal{N}_i|} \times \mathbb{R}^m \to \mathbb{R}$, with $i \in [N]$ and $k \in [p]$ be functions satisfying the following.

Assumption 5. (Regularity and convexity of the optimization problem): *For all $i \in [N]$ and $k \in [p]$, f_i and g_i^k are continuously differentiable functions with Lipschitz derivatives. We assume that for all $i \in [N]$ and $\boldsymbol{\xi}_i \in \mathbb{R}^n$, the functions $f_i(\boldsymbol{\xi}_i, \cdot)$ are strongly convex, and for all $i \in [N]$, $k \in [p]$ and $\bar{\boldsymbol{\xi}}_i \in \mathbb{R}^{n|\mathcal{N}_i|}$, the functions $g_i^k(\bar{\boldsymbol{\xi}}_i, \cdot)$ are convex.*

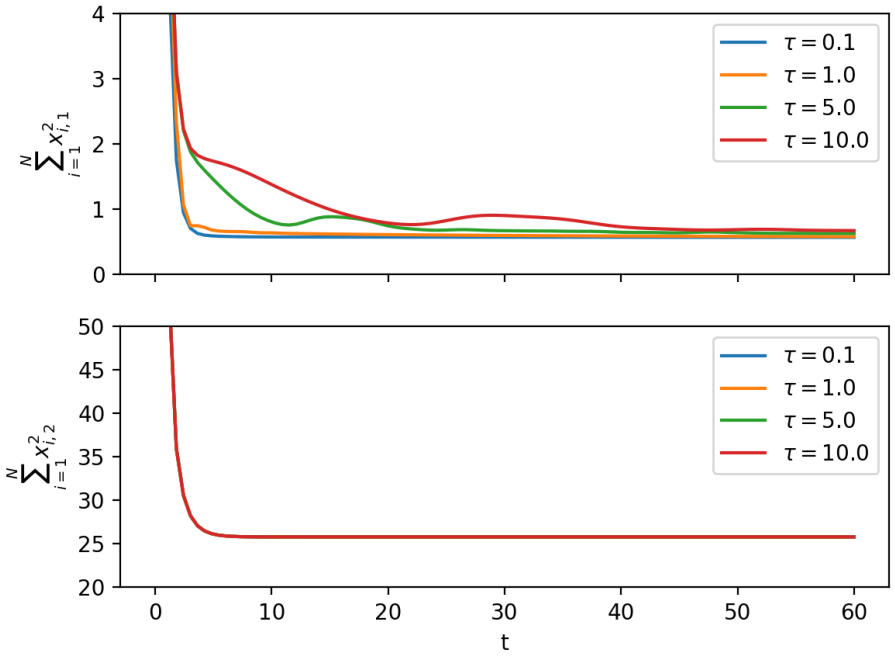


Figure 7.2: This plot shows the evolution of $\sum_{i=1}^{13} x_{i,1}^2$ and $\sum_{i=1}^{13} x_{i,2}^2$ under SP-SGF with initial conditions as in Figure 7.1 for different values of τ.

The agents need to coordinate to solve an optimization problem of the form

$$\begin{aligned} \min_{\{\mathbf{u}_i \in \mathbb{R}^m\}_{i=1}^N} & \sum_{i=1}^{N} f_i(\boldsymbol{\xi}_i, \mathbf{u}_i), \\ \text{s.t.} & \sum_{i \in V(\mathcal{G}_k)} g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i}, \mathbf{u}_i) \leq 0, \quad k \in [p]. \end{aligned} \tag{7.21}$$

where $\boldsymbol{\xi}_{\mathcal{N}_i} = \{\boldsymbol{\xi}_j\}_{j \in \mathcal{N}_i}$ and $\mathcal{G}_k$ is a connected subgraph of $\mathcal{G}$ for each $k \in [p]$, and $V(\mathcal{G}_k)$ denotes the set of vertices of graph $\mathcal{G}_k$. Note that (7.7) is a particular case of (7.21), where $f_i(\boldsymbol{\xi}_i, \mathbf{u}_i) = \frac{1}{2} \left\| \Gamma_i(\boldsymbol{\xi}_i)(\mathbf{u}_i - u_{\text{nom},i}(\boldsymbol{\xi}_i)) \right\|^2$ and $\mathcal{G}_k$ corresponds to the graph with nodes $\{i\} \cup \{j\}$ and an edge between $\{i\}$ and $\{j\}$ for the inter-agent collision avoidance constraint between agents i and j, and $\mathcal{G}_k$ corresponds to the singleton $\{i\}$ for the obstacle avoidance constraints of agent i. Moreover, for the inter-agent collision avoidance constraint between agents i and j,

$$\begin{aligned} g_i^k(\mathbf{p}_i, \theta_i, \mathbf{p}_j, \theta_j, \mathbf{u}_i) &= -2(\mathbf{p}_i - \mathbf{p}_j)^\top R(\theta_i) L^{-1} \mathbf{u}_i - \alpha_c^{ij} d(\mathbf{p}_i, \mathbf{p}_j), \\ g_j^k(\mathbf{p}_j, \theta_j, \mathbf{p}_i, \theta_i, \mathbf{u}_j) &= -2(\mathbf{p}_j - \mathbf{p}_i)^\top R(\theta_j) L^{-1} \mathbf{u}_j - \alpha_c^{ij} d(\mathbf{p}_i, \mathbf{p}_j). \end{aligned}$$

For the collision avoidance constraint of agent i with the kth obstacle, $g_i^k(\mathbf{p}_i, \theta_i, \mathbf{u}_i) = -\nabla h_k(\mathbf{p}_i)^\top R(\theta_i) L^{-1} \mathbf{u}_i - \alpha_k(h_k(\mathbf{p}_i) - \eta_k)$. Problem (7.21) can encode other types

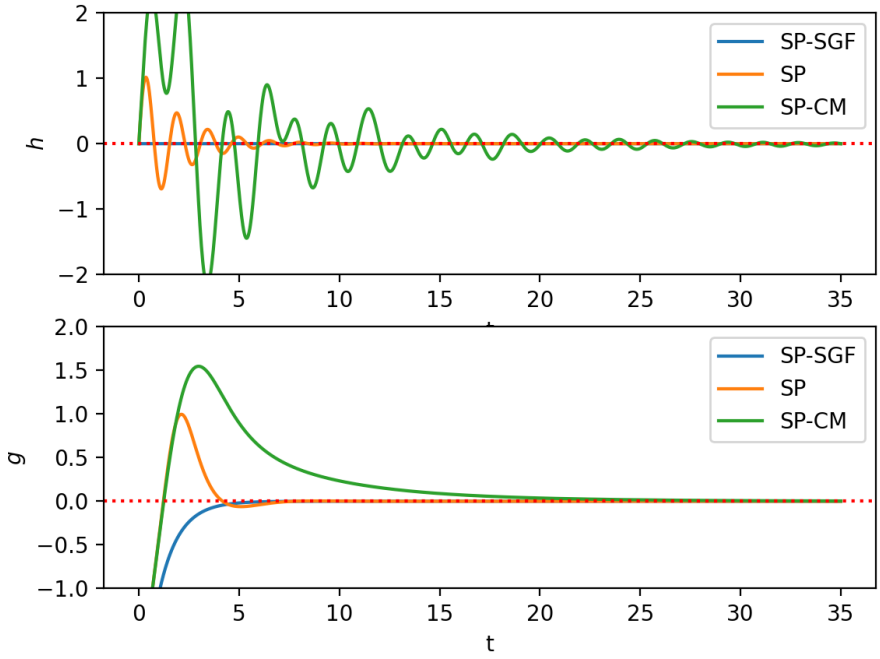


Figure 7.3: This plot shows the evolution of the constraints of (7.19) for SP-SGF with the same initial conditions as in Figure 7.1, SP with the same primal initial conditions as in Figure 7.1 and $\lambda = \mu = 0$ and SP-CM with the same initial conditions as in Figure 7.1 for $\mathbf{x}_i$, z_i, y_i, λ_i and μ_i for $i \in \{1, \dots, 13\}$.

of safety constraints and more general dynamics. We henceforth denote $\boldsymbol{\xi} = [\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_N] \in \mathbb{R}^{nN}$ and $\mathbf{u} = [\mathbf{u}_1, \cdots, \mathbf{u}_N] \in \mathbb{R}^{mN}$. We assume that (7.21) is feasible.

Assumption 6. *Problem* (7.21) *is feasible for all* $\boldsymbol{\xi} \in \mathbb{R}^{nN}$.

Assumption 6 is necessary for the solution of (7.21) to be well defined for all $\boldsymbol{\xi} \in R^{nN}$. If the constraints of (7.21) are defined by CBFs, such as those in (7.7), their joint feasibility can be characterized, cf. [4, 114, 201].

We let $u^\star : \mathbb{R}^{nN} \to \mathbb{R}^{mN}$ be the function mapping each $\xi \in \mathbb{R}^{nN}$ to the solution of (7.21). To tackle the design of our distributed algorithm, we first deal with the coupling induced by the inequality constraints by introducing *constraint mismatch variables* z_i^k for each agent and constraint in which it is involved. We use the same

notation as in Section 2.7 and reformulate (7.21) as

$$\min_{\mathbf{u}\in\mathbb{R}^{mN},\mathbf{z}\in\mathbb{R}^q} \sum_{i=1}^{N} f_i(\boldsymbol{\xi}_i,\mathbf{u}_i), \tag{7.22}$$
$$\text{s.t.} \quad g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i},\mathbf{u}_i) + \sum_{j\in\mathcal{N}_i\cap V(\mathcal{G}_k)} (z_i^k - z_j^k) \le 0,\ i\in V(\mathcal{G}_k),\ k\in[p].$$

In order to facilitate the analysis of the convergence properties of the algorithms that will follow, we regularize (7.22) by adding the term $\epsilon\sum_{k=1}^{p}\sum_{j\in V(\mathcal{G}_k)}(z_j^k)^2$, with $\epsilon>0$, in the objective function of (7.22). Details regarding this regularization are covered in the Appendix. With the added regularization term, the problem (7.22) has a strongly convex objective function and convex constraints, and therefore has a unique optimizer for every $\xi\in\mathbb{R}^{nN}$. Let $u^{\star,\epsilon}:\mathbb{R}^{nN}\to\mathbb{R}^{mN}$ and $z^{\star,\epsilon}:\mathbb{R}^{nN}\to\mathbb{R}^q$ be the functions mapping each $\boldsymbol{\xi}\in\mathbb{R}^{nN}$ to the corresponding unique optimizers in $\mathbf{u}$ and $\mathbf{z}$, respectively, of the regularized problem. We also let $\lambda^{\star,\epsilon}:\mathbb{R}^{nN}\to\mathbb{R}^q$ be the function mapping each $\boldsymbol{\xi}\in\mathbb{R}^{nN}$ to the optimal Lagrange multiplier of the regularized problem. Problem (7.22) (or its regularized version) cannot be decoupled into N local optimization problems because the optimal values of $\mathbf{z}$ in (7.22) require coordination among agents. However, for every fixed $\mathbf{z}$, (7.22) can be solved locally by agent i by just optimizing over $\mathbf{u}_i$ as follows:

$$\min_{\mathbf{u}_i\in\mathbb{R}^m} f_i(\boldsymbol{\xi}_i,\mathbf{u}_i), \tag{7.23}$$
$$\text{s.t.} \quad g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i},\mathbf{u}_i) + \sum_{j\in\mathcal{N}_i\cap V(\mathcal{G}_k)} (\mathbf{z}_i^k - \mathbf{z}_j^k) \le 0, \qquad k\in[p].$$

We let $\bar{u}_i:\mathbb{R}^{n|\mathcal{N}_i|}\times\mathbb{R}^{|\mathcal{N}_i|}\to\mathbb{R}^m$ be the function that maps every $(\boldsymbol{\xi}_{\mathcal{N}_i},\mathbf{z}_{\mathcal{N}_i})\in\mathbb{R}^{n|\mathcal{N}_i|}\times\mathbb{R}^{\Sigma_{j\in\mathcal{N}_i}|P_j|}$ to the optimizer of (7.23), and $\bar{u}=[\bar{u}_1,\cdots,\bar{u}_N]$. By construction, the controller $\bar{u}_i$ is **distributed**, as it only depends on variables which can be obtained through communication with agents in $\mathcal{N}_i$.

However, $\bar{u}_i$ depends on the chosen value of z. Since (7.22) contains a minimization over both u and $\mathbf{z}$, $\bar{u}_i$ coincides with the optimizer over u of (7.21), one must also optimize over the *constraint mismatch* variables $\mathbf{z}$. We do this by updating them with the projected saddle-point dynamics of the regularization of (7.22), cf. Figure 7.4.

We assume that the projected saddle-point dynamics can be run at a faster rate than the plant. Introducing a timescale separation parameter $\tau>0$ to model this,

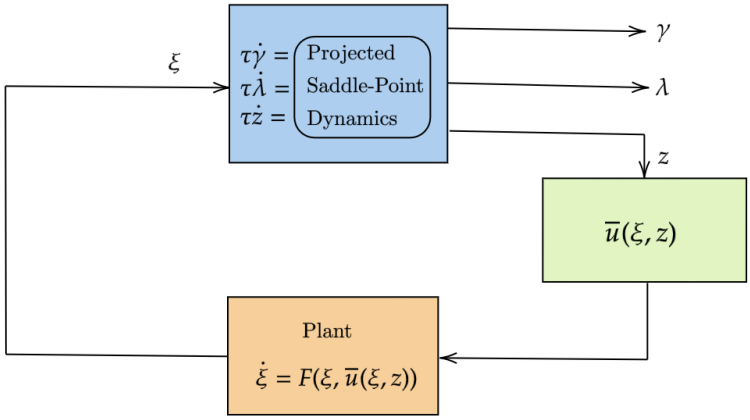


Figure 7.4: Block diagram of (7.24). The blue block updates the variables $\boldsymbol{\gamma}$, $\mathbf{z}$ and $\boldsymbol{\lambda}$ using the projected saddle-point dynamics of the regularized version of (7.22). In parallel, the plant is updated using the controller $\bar{u}$.

the interconnection of the projected saddle-point dynamics with the plant leads to the following dynamical system:

$$\tau\dot{\boldsymbol{\gamma}}_i = -\nabla_{\boldsymbol{\gamma}_i} f_i(\boldsymbol{\xi}_i, \boldsymbol{\gamma}_i) - \sum_{k\in P_i} \lambda_i^k \nabla_{\boldsymbol{\gamma}_i} g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i}, \boldsymbol{\gamma}_i), \tag{7.24a}$$

$$\tau\dot{z}_i^k = -\epsilon z_i^k - \sum_{j\in\mathcal{N}_i\cap\mathcal{G}_k} (\lambda_i^k - \lambda_j^k), \tag{7.24b}$$

$$\tau\dot{\lambda}_i^k = [g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i}, \boldsymbol{\gamma}_i) + \sum_{j\in\mathcal{N}_i\cap\mathcal{G}_k} (z_i^k - z_j^k)]_{\lambda_i^k}^+ , \tag{7.24c}$$

$$\dot{\boldsymbol{\xi}}_i = F_i(\boldsymbol{\xi}_i, \bar{u}_i(\boldsymbol{\xi}_i, \mathbf{z}_{\mathcal{N}_i})), \tag{7.24d}$$

for all $i \in [N]$ and $k \in P_i$. We henceforth denote $\boldsymbol{\gamma} = [\boldsymbol{\gamma}_1, \cdots, \boldsymbol{\gamma}_N]$, $\boldsymbol{\lambda}_i = \{\boldsymbol{\lambda}_i^k\}_{k\in P_i}$ for all $i \in [N]$ and $\boldsymbol{\lambda} = [\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_N]$. The auxiliary variables $\boldsymbol{\gamma}$ and $\boldsymbol{\lambda}$ play the role of the primal variable $\mathbf{u}$ and the Lagrange multipliers of the constraints in (7.22), respectively. Our proposed algorithmic solution is the controller $\bar{u}_i$ for all $i \in [N]$ implemented for the current value of the state variables $\boldsymbol{\xi}_i$ and $\mathbf{z}_{\mathcal{N}_i}$ in (7.24).

7.4 Analysis of the Solution: Distributed Character, Safety, and Stability

In this section we establish the properties of the controller proposed in Section 7.3. Throughout this section we use the same communication graph $\mathcal{G}$ in-

troduced in Section 7.3. First we introduce various assumptions regarding problem (7.23) and discuss their sensibleness.

Assumption 7. (Feasibility of optimization problem): *For all $i \in [N]$, the optimization problem* (7.23) *is feasible for all $\boldsymbol{\xi}_{\mathcal{N}_i} \in \mathbb{R}^{n|\mathcal{N}_i|}$ and $\mathbf{z}_{\mathcal{N}_i} \in \mathbb{R}^{\sum_{j\in\mathcal{N}_i}|P_j|}$.*

Remark 7.4.1. (Handling feasibility in practice): *Problem* (7.23) *is feasible if $\mathbf{z}_{\mathcal{N}_i} = z^{*,\epsilon}_{\mathcal{N}_i}(\boldsymbol{\xi})$: $u^{*,\epsilon}_i(\boldsymbol{\xi})$ is a solution of* (7.23) *because of Proposition 2.7.1 and Assumption 6. Hence, if $\mathbf{z}_{\mathcal{N}_i}$ is close to $\mathbf{z}^{*,\epsilon}_{\mathcal{N}_i}(\boldsymbol{\xi})$, then* (7.23) *is often feasible. Moreover, in practice, one can tune α^{ij}_c and α_k constraints in* (7.7) *only when they are close to being active to reduce the number of overall constraints and facilitate feasibility.* •

Assumption 8. (Availability of optimizer in real time): *The function $\bar{u}_i$ is instantaneously available to agent i for all $i \in [N]$.*

Assumption 8 is a reasonable abstraction of what happens in practical scenarios, such as (7.7), which is a quadratic program and can be solved efficiently [175]. In fact, if $M \leq 2$, $\bar{u}$ can even be found in closed form [118, Theorem 1].

Assumption 9. (Lipschitzness of optimizer): *The functions $u^{*,\epsilon}$, $z^{*,\epsilon}$ and $\bar{u}$ are locally Lipschitz.*

Remark 7.4.2. (Conditions that ensure Lipschitzness): *The works [32, 8] study different conditions under which the solution of parametric optimization problems such as* (7.23) *or* (7.22) *is locally Lipschitz.* •

We next show that the controller $\bar{u}$ is **safe** and **asymptotically** converges to $u^{*,\epsilon}$ when implemented in conjunction with the projected saddle-point dynamics as in (7.24). This, together with its distributed character, means that it meets all the desired properties. For the problem described in Section 7.1, this means that $\bar{u}$ achieves obstacle and inter-agent collision avoidance, and asymptotically converges to the closest controller to $u_{\text{nom}} = [u_{\text{nom},1}, \cdots, u_{\text{nom},N}]$ that satisfies the safety constraints. In particular, if the agents are far from any of the obstacles in the environment and the CBF constraints in (7.7) are inactive, $\bar{u}$ converges to

u_{nom} and steers the *leader* towards the desired waypoint and the *followers* towards their formation positions.

Proposition 7.4.3. (Convergence of algorithm): *Suppose that Assumptions 6-9 hold. Then,*

*(1) the controller $\bar{u}$ is **safe**, i.e., if the initial conditions of (7.24) are such that $g_i^k(\xi_{\mathcal{N}_i}(0), \bar{u}_i(\xi_i(0), z_{\mathcal{N}_i}(0))) \leq 0$ for all $k \in [p]$, then the trajectories of (7.24) satisfy*

$$\sum_{i \in V(\mathcal{G}_k)} g_i^k(\xi_{\mathcal{N}_i}(t), \bar{u}_i(\xi_i(t), z_{\mathcal{N}_i}(t))) \leq 0, \tag{7.25}$$

for all $k \in [p]$ and $t \geq 0$;

(2) if the origin is asymptotically stable for the dynamical system $\dot{\boldsymbol{\xi}} = F(\boldsymbol{\xi}, u^{*,\epsilon}(\boldsymbol{\xi}))$ with Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$, and Γ is a Lyapunov sublevel set of V contained in its region of attraction, then, for any initial condition of (7.24) $\mathbf{c}_0 := (\boldsymbol{\gamma}_0, \mathbf{z}_0, \boldsymbol{\lambda}_0, \boldsymbol{\xi}_0) \in \mathbb{R}^{nN} \times \mathbb{R}^q \times \mathbb{R}^q \times \mathbb{R}^{nN}$, with $\boldsymbol{\xi}_0 \in \Gamma$, $\delta > 0$ and $\epsilon > 0$, there exist $\tau_{c_0,\delta,\epsilon} > 0$ and r_{ξ_0} such that, if

$$\max\{\|\boldsymbol{\gamma}_0 - u^{*,\epsilon}(\boldsymbol{\xi}_0)\|, \|\mathbf{z}_0 - z^{*,\epsilon}(\boldsymbol{\xi}_0)\|, \|\boldsymbol{\lambda}_0 - \boldsymbol{\lambda}^{*,\epsilon}(\boldsymbol{\xi}_0)\|\} < r_{\boldsymbol{\xi}_0},$$

and $\tau < \tau_{c_0,\delta,\epsilon}$, then the trajectories of (7.24) are such that, for all $t > 0$,

$$\begin{aligned} &\|\gamma(t) - u^{*,\epsilon}(\xi(t))\| \leq \delta, \ \ \|z(t) - z^{*,\epsilon}(\xi(t))\| \leq \delta, \\ &\|\lambda(t) - \lambda^{*,\epsilon}(\xi(t))\| \leq \delta, \ \ \|\bar{u}(\xi(t), z(t)) - u^{*,\epsilon}(\xi(t))\| \leq \delta, \end{aligned}$$

and there exists $T_{c_0,\delta,\epsilon} > 0$ such that $\|\xi(t)\| \leq \delta$ for all $t > T_{c_0,\delta,\epsilon} > 0$.

Proof. First we show 1. By definition of $\bar{u}$, we have

$$g_i^k(\xi_{\mathcal{N}_i}(t), \bar{u}_i(\xi_i(t), z_{\mathcal{N}_i}(t))) + \sum_{j \in \mathcal{N}_i \cap V(\mathcal{G}_k)} (z_i^k(t) - z_j^k(t)) \leq 0, \tag{7.26}$$

for all $i \in [N]$, $k \in [p]$ and $t \geq 0$. Adding (7.26) for all $i \in V(\mathcal{G}_k)$, we obtain (7.25) for all $k \in [p]$ and $t \geq 0$. Next we show 2. Since the dynamics in (7.24) are not differentiable due to the presence of the $[\cdot]_+$ operator, the standard version of Tikhonov's

theorem for singular perturbations [121, Theorem 11.2] is not applicable. Instead we use [200], which gives a Tikhonov-type singular perturbation statement for differential inclusions. For non-smooth ODEs like (7.24) we need to check the following assumptions. First, the dynamics (7.24) are well-defined because Assumption 7 guarantees that $\bar{u}(\boldsymbol{\xi}, \mathbf{z})$ is well-defined for all $\boldsymbol{\xi} \in \mathbb{R}^{nN}$ and $\mathbf{z} \in \mathbb{R}^q$. Second, the dynamics (7.24) are locally Lipschitz because of the Lipschitzness of the gradients of f and g, and the *max* operator, as well as the Lipschitzness of F_i for all $i \in \mathbb{R}^n$ and assumption 9. Third, the existence and uniqueness of the equilibrium of the fast dynamics follows from the fact that (7.28) has a strongly convex objective function and convex constraints, which implies that it has a unique KKT point. Fourth, Lipschitzness and asymptotic stability of the reduced-order model

$$\dot{\boldsymbol{\xi}} = F(\boldsymbol{\xi}, \bar{\mathbf{u}}(\boldsymbol{\xi}, z^{*,\epsilon}(\boldsymbol{\xi}))). \tag{7.27}$$

Lipschitzness follows from Assumption 9, and asymptotic stability follows from the fact that $\bar{\mathbf{u}}(\boldsymbol{\xi}, z^{*,\epsilon}(\boldsymbol{\xi})) = u^{*,\epsilon}(\boldsymbol{\xi})$ for all $\boldsymbol{\xi} \in \mathbb{R}^n$ (cf. Proposition 2.7.1) and the hypothesis that the origin of $\dot{\boldsymbol{\xi}} = F(\boldsymbol{\xi}, u^{*,\epsilon}(\boldsymbol{\xi}))$ is asymptotically stable. Fifth, the asymptotic stability of the fast dynamics for every fixed value of the slow variable follows from [197, Theorem 5.1]. Finally, the origin is the only equilibrium of (7.27) by assumption. The result follows from [200, Theorem 3.1 and Corollary 3.4], by adapting the results therein to the case where the origin of (7.27) has a bounded region of attraction. □

If the constraints in (7.21) correspond to the CBF conditions of some set, as it is the case in (7.7), Proposition 7.4.3(i) implies that the set is forward invariant under the dynamics (7.24). Moreover, if $\dot{\boldsymbol{\xi}} = F(\boldsymbol{\xi}, u^{*,\epsilon}(\boldsymbol{\xi}))$ is globally asymptotically stable, then Proposition 7.4.3(ii) holds for any $\boldsymbol{\xi}_0 \in \mathbb{R}^n$.

Remark 7.4.4. (Proximity of the constraint mismatch variables to their optimal values and choice of timescale): *Proposition 7.4.3 requires that the initial conditions of $\boldsymbol{\gamma}$, $\mathbf{z}$ and $\boldsymbol{\lambda}$ are close enough to $\gamma^{*,\epsilon}(\boldsymbol{\xi}_0), z^{*,\epsilon}(\boldsymbol{\xi}_0)$ and $\lambda^{*,\epsilon}(\boldsymbol{\xi}_0)$. This is due to the technical nature of the proof of [200, Theorem 3.1], which requires the fast variables to be in a small ball around the solution manifold to show the stability of the interconnected system. The satisfaction of these conditions can be achieved by*

exploiting the asymptotic stability properties of the projected saddle-point dynamics and running them for the regularized version of (7.22) *offline for a fixed value of the state* $\boldsymbol{\xi}$ *equal to* $\boldsymbol{\xi}_0$ *within an accuracy smaller than* $r_{\boldsymbol{\xi}_0}$*. Proposition 7.4.3 also requires* τ *to be sufficiently small. In practice we have observed that convergence of the state variables is achieved for a wide range of values of* τ*. Moreover, since safety holds for any* τ*, the value of* τ *can be decreased during the execution of the algorithm to ensure convergence to the desired waypoint.* •

Remark 7.4.5. (Asymptotic stability assumption): *Proposition 7.4.3 2 requires that the controller* $u^{\star,\epsilon}$ *is asymptotically stabilizing. In the context of the problem outlined in Section 7.1, this means that in a neighborhood of the origin, enforcing the obstacle avoidance and inter-agent collision avoidance constraints does not disrupt the stabilizing character of the nominal controllers (i.e., their steering towards the desired waypoints or desired formation positions of interest), which can be achieved by taking the values of* α_c^{ij} *and* α_k *sufficiently large. Recent work [37, 4] gives conditions under which the solution of a CBF-based QP of the form* (7.7) *with a nominal stabilizing controller retains its stability properties. Such conditions can be used to derive a subset contained in the region of attraction of the origin, in which the result in Proposition 7.4.3 2 can be applied.* •

7.5 Experimental validation

Here we show the performance of the proposed distributed control design (7.24) in simulation and in physical robotic platforms for a team of differential-drive robots, cf. Section 7.1.

7.5.1 Parameter Tuning

Our experiments underscore the sensitivity of the control design to the choice of parameters. In particular, certain sequences of waypoints might lead to some of the agents of the team reaching deadlocks near the obstacles. This is a well-known issue of CBF-based controllers, cf. [34, 4]. In practice, we have observed that this

behavior can be avoided by choosing a sequence of waypoints such that straight-lines connecting consecutive waypoints lie in the safe region, and promoting larger values of the angular velocity input, which allow the vehicle more *manoeuvrability*, by selecting the matrix Γ_i as the constant matrix $[5, 0; 0, 1]$). We keep the other design parameters constant across the different experiments, with values $l = 0.2$, $\alpha_c^{ij} = 2.0$ for all $i \in [N]$, $j \in N_i$, $\alpha_k = 2.0$ for all $k \in [M]$, $d_{\min} = 1.0$, $\eta_k = 1.5$ for all $k \in [M]$, $\epsilon = 0.001$, and $\tau = 0.1$. Given the initial condition $x(0)$, we follow the procedure in Remark 7.4.4 to initialize the variables γ, z and λ in (7.24) before executing the controller. For each robot i, the set N_i is taken as the two closest robots to agent i in the initial positions.

7.5.2 Experiments

We have tested our algorithm in different simulation and hardware environments. For the simulation environments we have employed a high-fidelity Unity simulator on an Ubuntu Laptop with Intel Core i7-1355U (4.5 GHz). We numerically integrate (7.24) and implement $\bar{u}$ using the convex optimization library `CVXOPT` [202]. The first simulation environment consists of a series of red cilindrical, cubic, and spherical obstacles. A team of 5 Husky[1] robots initially in a x-like formation traverses the environment while avoiding collision with obstacles and other robots of the team[2]. The simulated robots have the same LIDAR and sensor capabilities as the real ones, and these are used to run a SLAM system that allows each robot to localize itself in the environment and obtain its current state, which is needed to run (7.24) and implement $\bar{u}$. Figure 7.5 shows 3 snapshots of the experiment and the trajectories followed by the robots. The robots successfully complete the task by avoiding collisions and reaching all the waypoints while maintaining the desired formation. Figure 7.6 shows the evolution of the distance to the desired formation position for each follower and the distance to the different obstacles for the leader agent.

In the second simulation, initially a team of three Husky robots are located in

[1]Spec. sheets for the Husky and Jackal robots can be found at https://clearpathrobotics.com
[2]Video of the simulation: https://tinyurl.com/distributedcbfs

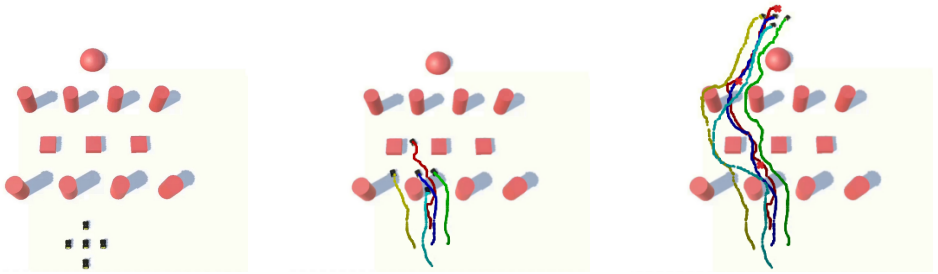


Figure 7.5: Snapshots of the first simulation environment with color coded trajectories for the different robots. The intensity of the color decreases with time. In the last snapshot, the red x's indicate the three different waypoints for the leader of the team (in magenta). The environment has dimensions 20m × 30m.

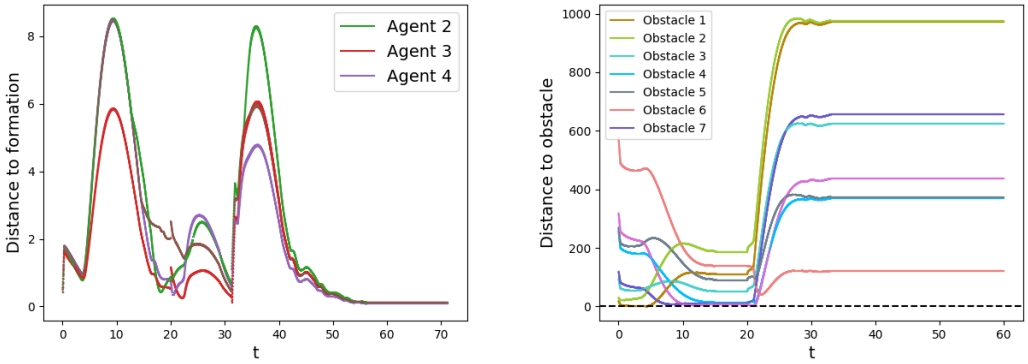


Figure 7.6: Evolution in the first simulation environment, cf. Figure 7.5. (left): Distance to the desired formation position over time for the different followers. (right): Distance to the different obstacles over time for the *leader*.

one of the rooms in the environment, cf. Figure 7.7(left). The team traverses the environment while maintaining a triangular formation. The walls are modelled as obstacles using a set of ellipsoidal barrier functions. The team successfully completes the task by avoiding collisions while maintaining the desired formation.

We have also validated our design in hardware in a team of 3 Jackal[1] robots with GPS, IMU, and LIDAR sensors, which they use to run a SLAM system to localize itself in the environment. The team is initially positioned as shown in Figure 7.8(left). The blue and grey cilinders are modelled as obstacles using CBFs. The team traverses the environment while maintaining a triangular formation. All computations are done onboard with the computers of each of the robots.

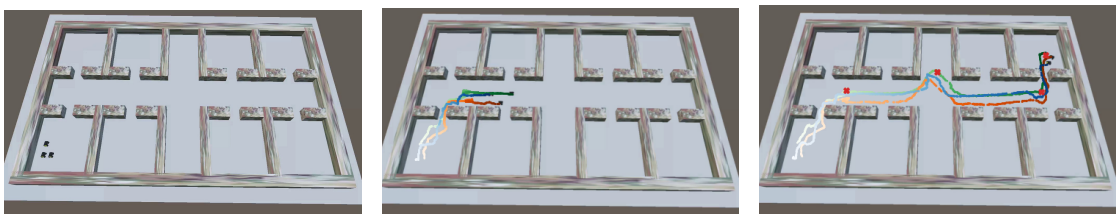


Figure 7.7: Snapshots of the second simulation environment with color coded trajectories for the different robots. The intensity of the color increases with time. In the last snapshot, the red x's indicate the four different waypoints for the leader of the team. The environment has dimensions 20m × 50m.

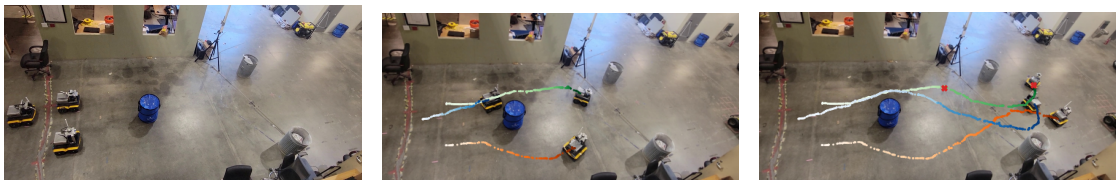


Figure 7.8: Snapshots of the hardware experiment with color coded trajectories for the different robots. The intensity of the color increases with time. In the last snapshot, the red x's indicate the two different waypoints for the leader of the team. The environment has dimensions 4m × 9m.

7.6 Appendix

The regularized version of (7.22) takes the following form:

$$\min_{\mathbf{u}\in\mathbb{R}^{mN},\mathbf{z}\in\mathbb{R}^{q}} \sum_{i=1}^{N} f_i(\boldsymbol{\xi}_i,\mathbf{u}_i) + \epsilon \sum_{k=1}^{p} \sum_{j\in V(\mathcal{G}_k)} (z_j^k)^2, \tag{7.28}$$
$$\text{s.t.} \quad g_i^k(\boldsymbol{\xi}_{\mathcal{N}_i},\mathbf{u}_i) + \sum_{j\in\mathcal{N}_i\cap V(\mathcal{G}_k)} (z_i^k - z_j^k) \le 0,\ i\in V(\mathcal{G}_k),\ k\in[p].$$

The next sensitivity result shows that the solution to (7.28) and (7.22) can be made close by choosing ϵ sufficiently small.

Lemma 7.6.1. (Sensitivity of regularized problem): *Let $u^\star$ be continuous, and assume $u^{\star,\epsilon}$ is continuous for all $\epsilon > 0$. Let $\mathcal{K} \subset \mathbb{R}^{nN}$ be compact and $\delta > 0$. Then, there exists $\bar{\epsilon}_{\mathcal{K},\delta} > 0$ such that if $\epsilon < \bar{\epsilon}_{\mathcal{K},\delta}$, then $\|u^{\star,\epsilon}(\boldsymbol{\xi}) - u^\star(\boldsymbol{\xi})\| \le \delta$ for all $\boldsymbol{\xi} \in \mathcal{K}$.*

Proof. By [10, Lemma 4.2], for each $\boldsymbol{\xi} \in \mathcal{K}$, there exists $\bar{\epsilon}_{\boldsymbol{\xi},\delta} > 0$ such that if $\epsilon < \bar{\epsilon}_{\boldsymbol{\xi},\delta}$, then $\|u^{\star,\epsilon}(\boldsymbol{\xi}) - u^\star(\boldsymbol{\xi})\| \le \frac{\delta}{2}$. Now, since $u^{\star,\epsilon}$ and $u^\star$ are continuous, there exists a neighborhood $\mathcal{N}_{\boldsymbol{\xi}}$ of $\boldsymbol{\xi}$ such that $\|u^{\star,\epsilon}(\hat{\boldsymbol{\xi}}) - u^\star(\hat{\boldsymbol{\xi}})\| \le \delta$ for all $\hat{\boldsymbol{\xi}} \in \mathcal{N}_{\boldsymbol{\xi}}$. Since $\cup_{\boldsymbol{\xi}\in\mathcal{K}}\mathcal{N}_{\boldsymbol{\xi}}$

is an open covering of the compact set $\mathcal{K}$, there exists a finite subcover, i.e., there exists $N_{\mathcal{K}} \in \mathbb{Z}_{>0}$ and $\{\boldsymbol{\xi}_i\}_{i=1}^{N_{\mathcal{K}}}$ such that $\mathcal{K} \subset \cup_{i=1}^{N_{\mathcal{K}}} \mathcal{N}_{\boldsymbol{\xi}_i}$. The result follows by letting $\bar{\epsilon}_{\mathcal{K},\delta} := \min_{i \in [N_{\mathcal{K}}]} \{\bar{\epsilon}_{\boldsymbol{\xi}_i,\delta}\}$. □

Chapter 8

Safe and Dynamically-Feasible Motion Planning using Control Lyapunov and Barrier Functions

In this chapter we consider the problem of designing motion planning algorithms for control-affine systems that generate collision-free paths from an initial to a final destination and can be executed using safe and dynamically-feasible controllers.

We introduce the `C-CLF-CBF-RRT` algorithm, which produces collision-free paths with such properties and leverages rapidly exploring random trees (RRTs), as well as CLFs and CBFs. we show that `C-CLF-CBF-RRT` is computationally efficient for linear systems with polytopic and ellipsoidal constraints, and establish its probablistic completeness. We showcase the performance of `C-CLF-CBF-RRT` in different simulation and hardware experiments.

8.1 Problem Statement

Let $\mathcal{R}$ be a compact and convex set in $\mathbb{R}^n$ containing M known obstacles $\{\mathcal{O}_l\}_{l=1}^M$, with $\text{Int}(\mathcal{O}_i) \cap \text{Int}(\mathcal{O}_j) = \varnothing$ for all $i \neq j \in [M]$. Let $\mathscr{F} := \mathcal{R} \backslash \cup_{l=1}^M \mathcal{O}_l$ denote the *safe* space. For each $l \in [M]$, we assume that there exists a positive integer $N_l \in \mathbb{Z}_{>0}$ and known continuously differentiable functions $\{h_{i,l} : \mathbb{R}^n \to \mathbb{R}\}_{i \in [N_l]}$ such that

$\mathcal{O}_l \coloneqq \{\mathbf{x} \in \mathbb{R}^n : h_l(\mathbf{x}) = \max_{i \in [N_l]} h_{i,l}(\mathbf{x}) < 0\}$.

Even though this imposes a specific structure on the set $\mathcal{O}_l$, one can obtain more complex obstacles by considering sets of the form $\cup_{i \in \mathcal{M}} \mathcal{O}_i$, with $\mathcal{M}$ a subset of $[M]$.

The robot dynamics are control-affine of the form (3.1), with $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^m$ locally Lipschitz. For each $l \in [M]$, h_l is a BNCBF of $\mathbb{R}^n \backslash \mathcal{O}_l$ for these dynamics, with associated extended class $\mathcal{K}_\infty$ function α_l. We also assume

$$\nabla h_{i,l}(\mathbf{x})^\top g(\mathbf{x}) \neq \mathbf{0}_m, \quad \forall \mathbf{x} \in \mathscr{F},\, l \in [M],\, i \in [N_l],$$

i.e., one differentiation of $h_{i,l}$ already makes the input $\mathbf{u}$ appear explicitly. Given an initial state $x_{\text{init}} \in \mathcal{R}$ and a final goal set $\mathcal{X}_{\text{goal}} \subset \mathcal{R}$, our aim is to develop a sampling-based motion planning algorithm that constructs a collision-free path $\mathcal{A} \coloneqq \{\mathbf{x}_i\}_{i=1}^{N_a}$ from x_{init} to $\mathcal{X}_{\text{goal}}$ that is dynamically feasible, i.e., such that for each pair of consecutive waypoints in $\mathcal{A}$, there exists a control law that generates a safe trajectory that connects them. Our approach to solve this problem leverages the theory of CLFs and BNCBFs to design controllers which (i) have safety and stability guarantees by design, and (ii) can be implemented efficiently to help reduce the computational burden of generating dynamically feasible trajectories.

8.2 CLF and BNCBF Compatibility Verification

The key challenge in our proposed approach to the problem outlined in Section 8.1 is that the optimization problem (2.14) defining the CLF-CBF-based controller has to be feasible at all points along the trajectory. In this section we tackle this problem and show how such a feasibility check can be performed in general, and how it is efficient in two specific cases of interest.

8.2.1 Compatibility Verification for General Dynamics and Obstacles

In this section we consider the problem of verifying that a CLF and a BNCBF are compatible in systems for general dynamics and obstacles. The following result

gives a characterization for when a CLF and a BNCBF are compatible in the region $\mathcal{R}$.

Proposition 8.2.1. (Characterization of CLF-BNCBF Compatibility): *Given* $\mathbf{q} \in \mathscr{F}$, *let* $V_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ *be a CLF of* (3.1) *with respect to* $\mathbf{q}$. *Let* $l \in [M]$ *and assume that* h_l *is a BNCBF of* $\mathbb{R}^n \backslash \mathcal{O}_l$. *Let* $W_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ *be a positive definite function with respect to* $\mathbf{q}$ *and* $\alpha_l : \mathbb{R} \to \mathbb{R}$ *be an extended class* $\mathcal{K}_\infty$ *function. For each* $\mathcal{J} \subset \mathcal{P}([N_l])$, *let* $Z_{l,\mathcal{J}} := \{\mathbf{x} \in \mathbb{R}^n : \mathcal{I}_l(\mathbf{x}) = \mathcal{J}\}$ *denote the set of points where the active constraints defining obstacle* $\mathcal{O}_l$ *correspond to the indices in* $\mathcal{J}$. *For* $\Gamma \subset \mathcal{R}$, *define*

$$\zeta_1 = \min_{\substack{\mathbf{x}\in\Gamma \\ \{\beta_i\in\mathbb{R}\}_{i\in\mathcal{J}}}} \left\| \sum_{i\in\mathcal{J}} \beta_i L_g h_{i,l}(\mathbf{x}) - L_g V_q(\mathbf{x}) \right\|^2 \tag{8.1a}$$

$$s.t. \quad \beta_i \geq 0, \ i \in \mathcal{J}, \tag{8.1b}$$

$$h_{j,l}(\mathbf{x}) \leq h_{i,l}(\mathbf{x}), \ \forall j \notin \mathcal{J}, i \in \mathcal{J}, \tag{8.1c}$$

$$h_l(\mathbf{x}) \geq 0. \tag{8.1d}$$

If $\zeta_1 \neq 0$, *then* V_q *and* h_l *are compatible in* $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. *Otherwise, if* $\zeta_1 = 0$, *let*

$$\zeta_2 = \min_{\substack{\mathbf{x}\in\Gamma \\ \{\beta_i\in\mathbb{R}\}_{i\in\mathcal{J}}}} \Phi(\mathbf{x}, \{\beta_i\}_{i\in\mathcal{J}}), \tag{8.2a}$$

$$s.t. \quad \sum_{i\in\mathcal{J}} \beta_i L_g h_{i,l}(\mathbf{x}) = L_g V_q(\mathbf{x}), \tag{8.2b}$$

$$\beta_i \geq 0, \ i \in \mathcal{J}, \tag{8.2c}$$

$$h_{j,l}(\mathbf{x}) \leq h_{i,l}(\mathbf{x}), \ \forall j \notin \mathcal{J}, i \in \mathcal{J}, \tag{8.2d}$$

$$h_l(\mathbf{x}) \geq 0, \tag{8.2e}$$

for $\Phi(\mathbf{x}, \{\beta_i\}_{i\in\mathcal{J}}) = -W_q(\mathbf{x}) - L_f V_q(\mathbf{x}) + \sum_{i\in\mathcal{J}} \beta_i (L_f h_{i,l}(\mathbf{x}) + \alpha_l(h_{i,l}(\mathbf{x})))$. *If* $\zeta_2 \geq 0$, *then* $V_{\mathbf{q}}$ *and* h_l *are compatible in* $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. *Conversely, if* $V_{\mathbf{q}}$ *and* h_l *are compatible in* $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$ *then there exists an extended class* $\mathcal{K}_\infty$ *function* α_l *and a positive definite function* W_q *with respect to* $\mathbf{q}$ *such that either* $\zeta_1 \neq 0$ *or* $\zeta_1 = 0$ *and* $\zeta_2 \geq 0$.

Proof. First note that if $\zeta_1 = 0$, the optimization problem (8.2) is feasible and therefore ζ_2 is well-defined. By Farkas' Lemma [203], $V_{\mathbf{q}}$ and h_l are compatible

at $\mathbf{x} \in Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$ if and only if for some positive definite function $W_{\mathbf{q}}$ with respect to $\mathbf{q}$ and some extended class $\mathcal{K}_\infty$ function α_l, there do not exist $\beta_0 \in \mathbb{R}_{\geq 0}$, $\{\beta_i\}_{i\in\mathcal{J}} \subset \mathbb{R}_{\geq 0}$ such that

$$\beta_0 L_g V_{\mathbf{q}}(\mathbf{x}) = \sum_{i\in\mathcal{J}} \beta_i L_g h_{i,l}(\mathbf{x}), \tag{8.3a}$$
$$\beta_0(-L_f V_{\mathbf{q}}(\mathbf{x}) - W(\mathbf{x})) + \sum_{i\in\mathcal{J}} \beta_i(\alpha_l(h_{i,l}(\mathbf{x})) + L_f h_{i,l}(\mathbf{x})) < 0.$$

First suppose that for some W_q and α_l, either $\zeta_1 \neq 0$ or $\zeta_1 = 0$ and $\zeta_2 \geq 0$. Suppose there exists a solution $\mathbf{s}_1^* = (\mathbf{x}^*, \beta_0^*, \{\beta_i^*\}_{i\in\mathcal{I}_l(\mathbf{x})})$ of (8.3) and let us reach a contradiction. If $\beta_0^* = 0$, then, (8.3) implies that the constraints $L_f h_{i,l}(\mathbf{x}) + L_g h_{i,l}(\mathbf{x})\mathbf{u} \geq -\alpha_l(h_{i,l}(\mathbf{x}))$ are not simultaneously feasible, which means that h_l is not a BNCBF, hence arriving at a contradiction. Therefore, $\mathbf{s}_1^*$ must be such that $\beta_0^* > 0$. By taking $\tilde{\beta}_i = \frac{\beta_i}{\beta_0}$ for $i \in \mathcal{J}$, we deduce that $(\mathbf{x}^*, \{\tilde{\beta}_i\}_{i\in\mathcal{J}})$ is a solution of (8.1) with a value of the objective function equal to zero. This means that if $\zeta_1 \neq 0$, the solution $\mathbf{s}_1^*$ does not exist and V_q and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. Otherwise, if $\zeta_1 = 0$, then $(\mathbf{x}^*, \{\tilde{\beta}_i\}_{i\in\mathcal{J}})$ is a solution of (8.2) with a strictly negative value of the objective function. This means that if $\zeta_1 = 0$ and $\zeta_2 \geq 0$, the solution $\mathbf{s}_1^*$ does not exist and $V_{\mathbf{q}}$ and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. Conversely, suppose that V_q and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. This implies that there exists $W_{\mathbf{q}}$ and α_l such that (8.3) has no solution. If (8.3a) has no solution, then $\zeta_1 \neq 0$. If (8.3a) has a solution but (**??**) does not, then $\zeta_1 = 0$ and $\zeta_2 \geq 0$. □

Note that Proposition 8.2.1 is valid for any set $\Gamma \subset \mathcal{R}$. Intuitively, since the CLF and BNCBF conditions define half-spaces in the control input $\mathbf{u}$, (8.1) checks whether the normal vectors of the hyperplanes defining such half-spaces are linearly independent. If this condition does not hold, (8.2) checks whether the input-independent terms of the CLF and BNCBF conditions leave enough space for such conditions to be compatible. Additionally, optimization problems (8.1) and (8.2) need to be checked for every possible set of active constraints. The constraints (8.1c) and (8.2d) ensure that $\mathcal{J}$ is the set of active constraints at $\mathbf{x}$. Often, one is interested in verifying the compatibility of a CLF and a BNCBF only in a small subset of $\mathcal{R}$, in which case the flexibility provided by the set Γ is useful.

Remark 8.2.2. (Checking for all Possible Sets of Active Constraints): Given a subset $\mathcal{J} \subset \mathcal{P}([N_l])$ of functions $\{h_{i,l}\}$, Proposition 8.2.1 provides a way to verify if the CLF and the BNCBF are compatible at the points in the region of interest $\Gamma \cap \mathscr{F}$ where such functions are active. Let $H_{l,\mathcal{J}} \coloneqq \{\mathbf{x} \in \Gamma : \mathcal{I}_l(\mathbf{x}) = \mathcal{J}\}$ be the points in Γ where the constraints with index in $\mathcal{J}$ are active, and $\mathcal{S}_l \coloneqq \{\mathcal{J} \subset \mathcal{P}([N_l]) : H_{l,\mathcal{J}} \neq \varnothing\}$ be the sets of indices for which the above set is nonempty. The class $\mathcal{S}_l$ contains all possible sets of active constraints in Γ. By checking the condition in Proposition 8.2.1 for all $\mathcal{J}$ in $\mathcal{S}_l$, we can verify if the CLF and the BNCBF are compatible in $\Gamma \cap \mathscr{F}$. In practice, given a region Γ where we are interested in checking the compatibility of V_q and h_l, one can often identify the indices that can achieve a maximum value in Γ (for example, for polytopic obstacles in the plane, only a few of the functions $h_{i,l}$ have points in Γ where they take positive values). This means that the cardinality of $\mathcal{S}_l$ is often small and the number of checks using Proposition 8.2.1 can be kept small. •

Remark 8.2.3. (Verifying Compatibility for Multiple BNCBFs): Proposition 8.2.1 actually provides a way to check whether the optimization problem (2.14) is feasible at *all* points of Γ. This can be done as follows: one first finds all $l \in [M]$ such that $\Gamma \cap \mathcal{O}_l \neq \varnothing$. If Γ can be expressed as the 0-sublevel set of a convex differentiable function γ, i.e., $\Gamma \coloneqq \{\mathbf{x} \in \mathbb{R}^n : \gamma(\mathbf{x}) \leq 0\}$, and the functions $h_{i,l}$ are convex, then this can be solved efficiently by checking that the solution of the convex problem

$$\begin{aligned} &\min_{\mathbf{x} \in \mathbb{R}^n} \gamma(\mathbf{x}) \\ &\text{s.t.} \quad h_{i,l}(\mathbf{x}) \leq 0, \quad \forall i \in [N_l] \end{aligned}$$

is non-positive. The BNCBF constraints associated with those $l' \in [M]$ such that $\Gamma \cap \mathcal{O}_{l'} = \varnothing$ can be neglected since, given a controller that satisfies all the other BNCBF constraints, it can be shown to also satisfy the BNCBF constraints for such $l' \in [M]$ by taking the corresponding extended class $\mathcal{K}_\infty$ function $\alpha_{l'}$ linear with sufficiently large slope. On the other hand, for $l' \in [M]$ such that $\Gamma \cap \mathcal{O}_{l'} \neq \varnothing$, Proposition 8.2.1 ensures that there exists a small neighborhood around $\partial\mathcal{O}_{l'}$, not containing points of any other obstacle, where V and $h_{l'}$ are compatible. By taking the extended class $\mathcal{K}_\infty$ functions of the other CBF constraints as linear functions

with sufficiently large slope, (2.14) is feasible in each of these neighborhoods. Finally, for points in Γ not belonging to any of these neighborhoods, the extended class $\mathcal{K}_\infty$ functions can also be taken as linear with sufficiently large slope to guarantee that (2.14) is feasible. •

Remark 8.2.4. (About the Choice of CLF and Class $\mathcal{K}_\infty$ Function): Note that, when solving the optimization problems (8.1) and (8.2) for fixed $V_{\mathbf{q}}$, α_l, and $W_{\mathbf{q}}$, it is not guaranteed that $\zeta_1 \neq 0$ or $\zeta_1 = 0$ and $\zeta_2 \geq 0$. If $\tilde{\alpha}$ is an extended class $\mathcal{K}_\infty$ function with $\tilde{\alpha}(s) \geq \alpha(s)$ for all $s \in \mathbb{R}$, the objective function Φ of (8.2) does not decrease at any point, which means that the value of ζ_1 remains the same, but the condition $\zeta_2 \geq 0$ becomes easier to satisfy. A similar behavior occurs if $\tilde{W}$ is a positive definite function with $\tilde{W}(\mathbf{x}) \leq W(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$. We leverage these observations in Section 8.3 when we introduce our proposed motion planning algorithm. •

Remark 8.2.5. (Regularity Properties of the Controller): If V_q and h_l are compatible in $\mathcal{R}$ for all $l \in [M]$, the CLF-CBF-based controller (2.14) is well defined, i.e., the optimization (2.14) is feasible for all points in $\mathcal{R}$. However, slightly stronger conditions are needed to ensure that such CLF-CBF-based controller is locally Lipschitz and therefore can be used to render $\mathcal{C}$ forward invariant and the origin asymptotically stable. We refer the reader to [8] for a survey on different conditions that ensure continuity, Lipschitzness, and other regularity properties of optimization-based controllers of the form (2.14). These conditions are often satisfied in practice and are mostly related to the dynamics and the specific obstacles, which in our problem here are given and not subject to design. Therefore, throughout this work, we assume that (2.14) satisfies at least one of the sufficient conditions outlined in [8] that ensure that the resulting controller is locally Lipschitz. •

Remark 8.2.6. (Input Constraints): In many applications, one is interested in verifying whether the CLF and BNCBF conditions are simultaneously feasible with a control input $\mathbf{u}$ constrained to lie on the set $\{\mathbf{u} \in \mathbb{R}^m : C_1\mathbf{u} \leq c_2\}$, with $C_1 \in \mathbb{R}^{c \times m}$,

$\mathbf{c}_2 \in \mathbb{R}^c$, and $c \in \mathbb{Z}_{>0}$. Equivalently, we seek to verify whether the inequalities

$$\begin{aligned} &L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})\mathbf{u} \geq -\alpha_{i,l}(h_{j,l}(\mathbf{x})), \ \forall j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &L_f V_i(\mathbf{x}) + L_g V_i(\mathbf{x})\mathbf{u} + W_i(\mathbf{x}) \leq 0, \\ &C_1\mathbf{u} \leq c_2, \end{aligned} \tag{8.4}$$

are simultaneously feasible. This problem can also be treated using Farkas' Lemma [203] to obtain a result analogous to Proposition 8.2.1. For example, the objective function in (8.1) should be adjusted to $\left\|\sum_{i\in\mathcal{J}} \beta_j L_g h_{i,l}(\mathbf{x}) - L_g V_{\mathbf{q}}(\mathbf{x}) - C_1^T\bar{\boldsymbol{\beta}}\right\|^2$, where $\bar{\boldsymbol{\beta}} \in \mathbb{R}^c$ is an additional optimization variable with entries that are required to be positive. Instead, the objective function in (8.2) should be adjusted to $\bar{\beta}^T\mathbf{c}_2 - W_q(x) - L_f V_{\mathbf{q}}(\mathbf{x}) + \sum_{i\in\mathcal{J}} \beta_i(L_f h_{i,l}(\mathbf{x}) + \alpha_l(h_{i,l}(\mathbf{x})))$. •

Proposition 8.2.1 shows that the problem of checking whether a CLF and a BNCBF are compatible in a region of interest can be reduced to solving a pair of optimization problems. However, in general, the optimization problems (8.1) and (8.2) are not convex and can be computationally intractable. Our forthcoming exposition provides two particular cases of dynamics and obstacles for which these two optimization problems are computationally tractable.

8.2.2 Compatibility Verification for Linear Systems and Polytopic Obstacles

In this section we particularize our discussion to linear dynamics,

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u}, \tag{8.5}$$

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, and the obstacles are polytopic (i.e., the functions $h_{i,l}$ are affine). We start by introducing some useful notation. For each $l \in [M]$, let $\mathbf{a}_{i,l} \in \mathbb{R}^n$, $b_{i,l} \in \mathbb{R}$ be such that $h_{i,l}(\mathbf{x}) = \mathbf{a}_{i,l}^T\mathbf{x} + b_{i,l}$. We further assume that h_l is a BNCBF, i.e., there exists an extended class $\mathcal{K}_\infty$ function α_l such that, for all $\mathbf{x} \in \mathbb{R}^n \backslash \mathcal{O}_l$, there exists $\mathbf{u} \in \mathbb{R}^m$ with

$$\mathbf{a}_{i,l}^T(A\mathbf{x} + B\mathbf{u}) \geq -\alpha_l(\mathbf{a}_{i,l}^T\mathbf{x} + b_{i,l})$$

for all $i \in \mathcal{I}_l(\mathbf{x})$.

We further assume that given $\mathbf{q} \in \mathbb{R}^n$, a quadratic CLF is available, i.e., we have a positive definite matrix $P \in \mathbb{R}^{n\times n}$ such that $V_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$, defined as $V_{\mathbf{q}}(\mathbf{x}) = (\mathbf{x}-\mathbf{q})^\top P(\mathbf{x}-\mathbf{q})$, is a CLF with respect to $\mathbf{q}$ in $\mathbb{R}^n$ of (8.5) with associated positive definite function $W_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$.

The following result follows by applying Proposition 8.2.1 to the case when dynamics are linear and obstacles polytopic.

Proposition 8.2.7. (CLF-BNCBF Compatibility for Linear Dynamics and Polytopic Obstacles): *Let $\Gamma \subset \mathcal{R}$, $l \in [M]$, $\mathcal{J} \in \mathcal{P}([N_l])$, $\mathbf{q} \in \mathscr{F}$, and define*

$$\zeta_1 := \min_{\substack{\mathbf{x}\in\Gamma \\ \{\beta_i\in\mathbb{R}\}_{i\in\mathcal{J}}}} \left\| \sum_{i\in\mathcal{J}} \beta_i B^\top \mathbf{a}_{i,l} - B^\top P(\mathbf{x}-\mathbf{q}) \right\|^2 \tag{8.6a}$$

$$s.t.\ \beta_i \geq 0,\ \forall i \in \mathcal{J}, \tag{8.6b}$$

$$\mathbf{a}_{j,l}^T \mathbf{x} + b_{j,l} \leq \mathbf{a}_{i,l}^T \mathbf{x} + b_{i,l},\ \forall j \notin \mathcal{J}, i \in \mathcal{J}, \tag{8.6c}$$

$$\mathbf{a}_{i,l}^T \mathbf{x} + b_{i,l} \geq 0,\ i \in \mathcal{J}. \tag{8.6d}$$

If $\zeta_1 \neq 0$, then V_q and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. Otherwise, if $\zeta_1 = 0$, let

$$\zeta_2 := \min_{\substack{\mathbf{x}\in\Gamma \\ \{\beta_i\in\mathbb{R}\}_{i\in\mathcal{J}}}} \Phi(\mathbf{x}, \{\beta_i\}_{i\in\mathcal{J}}) \tag{8.7a}$$

$$s.t.\ \sum_{i\in\mathcal{J}} \beta_i B^\top \mathbf{a}_{i,l} = B^\top P(\mathbf{x}-\mathbf{q}), \tag{8.7b}$$

$$\beta_i \geq 0,\ \forall i \in \mathcal{J}, \tag{8.7c}$$

$$\mathbf{a}_{j,l}^\top \mathbf{x} + b_{j,l} \leq \mathbf{a}_{i,l}^\top \mathbf{x} + b_{i,l},\ \forall j \notin \mathcal{J}, i \in \mathcal{J}, \tag{8.7d}$$

$$\mathbf{a}_{i,l}^\top \mathbf{x} + b_{i,l} \geq 0,\ i \in \mathcal{J}, \tag{8.7e}$$

with $\Phi(\mathbf{x}, \{\beta_i\}_{i\in\mathcal{J}}) = -W_{\mathbf{q}}(\mathbf{x}) - (\mathbf{x}-\mathbf{q})^\top PA\mathbf{x} + \sum_{i\in\mathcal{J}} \beta_i(\alpha_l(\mathbf{a}_{i,l}^\top \mathbf{x} + b_{i,l}) + \mathbf{a}_{i,l}^\top A\mathbf{x})$. If $\zeta_2 \geq 0$, then $V_{\boldsymbol{q}}$ and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$. Conversely, if $V_{\boldsymbol{q}}$ and h_l are compatible in $Z_{l,\mathcal{J}} \cap \Gamma \cap \mathscr{F}$, then there exists an extended class $\mathcal{K}_\infty$ function α_l and a positive definite function $W_{\boldsymbol{q}}$ with respect to q such that either $\zeta_1 \neq 0$ or $\zeta_1 = 0$ and $\zeta_2 \geq 0$.

We end this section by discussing the tractability of the optimizations (8.6) and (8.7). If $W_{\boldsymbol{q}}$ is a quadratic function (as it is often the case in practice),

$\alpha(s) = \alpha_0 s$, with $\alpha_0 > 0$, and Γ is given by a sublevel set of a quadratic function (e.g., if it is the sublevel set a quadratic CLF $V_{\boldsymbol{q}}$), then (8.6) and (8.7) both have quadratic objective functions and quadratic constraints, i.e., they are quadratically constrained quadratic programs (QCQPs). Moreover, if Γ is the sublevel set of a convex quadratic function, then (8.6) is a convex QCQP (whereas in general, (8.7) is non-convex). If instead Γ is the sublevel set of a piecewise linear function, both (8.6) and (8.7) have affine constraints and therefore are quadratic programs (QPs). Moreover, (8.6) is a convex QP. In either case, even if the resulting QCQPs or QPs are non-convex, there exist efficient heuristics [204, 205] to solve these programs. Finally, Proposition 8.2.7 can be applied to settings where obstacles are not polytopic by constructing outer approximations of them using polytopes and considering the resulting union of convex sets.

8.2.3 Compatibility Verification for Linear Systems and Ellipsoidal Obstacles

In this section, we again consider linear dynamics (8.5), but now assume obstacles are ellipsoidal, i.e., $\mathcal{O}_l = \{\mathbf{x} \in \mathbb{R}^n : r_l^2 > (\mathbf{x} - \mathbf{c}_l)^\top R_l (\mathbf{x} - \mathbf{c}_l)\}$, for some positive definite matrix $R_l \in \mathbb{R}^{n \times n}$, $\mathbf{c}_l \in \mathbb{R}^n$, and $r_l > 0$. In this case, we take $h_l(\mathbf{x}) = -r_l^2 + (\mathbf{x} - \mathbf{c}_l)^T R_l (\mathbf{x} - \mathbf{c}_l)$ (which is continuously differentiable and therefore $N_l = 1$ for all $l \in [M]$) and $V_{\mathbf{q}}(\mathbf{x}) = (\mathbf{x} - \mathbf{q})^\top P (\mathbf{x} - \mathbf{q})$, for some positive definite matrix $P \in \mathbb{R}^{n \times n}$. Then the following result follows from applying Proposition 8.2.1 to the case when dynamics are linear and obstacles are ellipsoidal.

Proposition 8.2.8. (Sufficient Condition for CLF-BNCBF Compatibility for Linear Dynamics and Ellipsoidal Obstacles): *Let* $\Gamma \subset \mathcal{R}$, $l \in [M]$, $\mathbf{q} \in \mathscr{F}$, $\alpha_l > 0$, *and define*

$$\zeta_1 := \min_{\mathbf{x} \in \Gamma, \mathbf{y} \in \mathbb{R}^n, \beta \in \mathbb{R}} \left\| B^\top \mathbf{y} - B^\top P (\mathbf{x} - \mathbf{q}) \right\|^2 \tag{8.8a}$$

$$s.t.\ \beta \geq 0,\ h_l(\mathbf{x}) \geq 0,\ \mathbf{y} = -2\beta R_l (\mathbf{x} - \mathbf{c}_l). \tag{8.8b}$$

If $\zeta_1 \neq 0$, then $V_{\mathbf{q}}$ and h_l are compatible in $\Gamma \cap \mathscr{F}$. Otherwise, if $\zeta_1 = 0$, let

$$\zeta_2 := \min_{\mathbf{x}\in\Gamma, \mathbf{y}\in\mathbb{R}^n, \beta\in\mathbb{R}} \Phi(\mathbf{x}, \mathbf{y}, \beta) \tag{8.9a}$$

$$s.t.\ B^\top \mathbf{y} = B^\top P(\mathbf{x} - \mathbf{q}), \tag{8.9b}$$

$$\beta \geq 0,\ h_l(\mathbf{x}) \geq 0,\ \mathbf{y} = -2\beta R_l(\mathbf{x} - \mathbf{c}_l), \tag{8.9c}$$

with $\Phi(\mathbf{x}, \mathbf{y}, \beta) = -W_q(\mathbf{x}) - (\mathbf{x} - \mathbf{q})^\top PA\mathbf{x} - \beta\alpha_l r_l^2 - \alpha_l(\mathbf{x} - \mathbf{c}_l)^\top \frac{\mathbf{y}}{2} + \mathbf{y}^\top A\mathbf{x}$. If $\zeta_2 \geq 0$, then V_q and h_l are compatible in $\Gamma \cap \mathscr{F}$.

If Γ is the sublevel set of a quadratic function and W_q is quadratic, both (8.8) and (8.9) are QCQPs and can therefore be solved efficiently [204, 205].

Let us next further restrict our attention to single-integrator dynamics, i.e.,

$$\dot{\mathbf{x}} = \mathbf{u}, \tag{8.10}$$

and circular obstacles, i.e., $\mathcal{O}_l = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{c}_l\| < r_l\}$ for some $\mathbf{c}_l \in \mathbb{R}^n$ and $r_l > 0$. In this case, we take $h_l(\mathbf{x}) = \|\mathbf{x} - \mathbf{c}_l\|^2 - r_l^2$, $V_q(\mathbf{x}) = \|\mathbf{x} - \mathbf{q}\|^2$, and $W_{\mathbf{q}}(\mathbf{x}) = (\mathbf{x} - \mathbf{q})^\top Q(\mathbf{x} - \mathbf{q})$, where $Q \in \mathbb{R}^{n\times n}$ is a positive definite matrix. In this case, the optimization problems in Proposition 8.2.1 can be solved in closed-form.

Proposition 8.2.9. (Sufficient Condition for CLF-BNCBF Compatibility for Single Integrator Dynamics and Circular Obstacles): *Let $l \in [M]$, $\alpha_l > 0$, $\mathbf{x}_0 \in \mathbb{R}^n \backslash \{\mathbf{q}\}$, $\mathbf{q} \in \mathscr{F}$, $\Gamma := \{\mathbf{x} \in \mathbb{R}^n : V_q(\mathbf{x}) \leq V_q(\mathbf{x}_0)\}$, $B_l := \|\mathbf{q} - \mathbf{c}_l\|_Q^2 - 2\alpha_l r_l^2$,*

$$\beta_+ := \frac{\sqrt{B_l^2 + 4\alpha_l^2 r_l^2(\|\mathbf{q} - \mathbf{c}_l\|^2 - r_l^2)} - B_l}{2\alpha_l r_l^2},$$

and suppose that one of the following holds:

- $\|\mathbf{x}_0 - \mathbf{q}\| - \|\mathbf{c}_l - \mathbf{q}\| > 0$ *and* $\frac{\|\mathbf{x}_0 - \mathbf{q}\|}{\|\mathbf{x}_0 - \mathbf{q}\| - \|\mathbf{c}_l - \mathbf{q}\|} > 1 + \frac{\|\mathbf{c}_l - \mathbf{q}\|}{r_l}$;
- $\|\mathbf{x}_0 - \mathbf{q}\| - \|\mathbf{c}_l - \mathbf{q}\| > 0$, $\frac{\|\mathbf{x}_0 - \mathbf{q}\|}{\|\mathbf{x}_0 - \mathbf{q}\| - \|\mathbf{c}_l - \mathbf{q}\|} \leq 1 + \frac{\|\mathbf{c}_l - \mathbf{q}\|}{r_l}$ *and* $\beta_+ \geq 1 + \frac{\|\mathbf{c}_l - \mathbf{q}\|}{r_l}$;
- $\|\mathbf{x}_0 - \mathbf{q}\| - \|\mathbf{c}_l - \mathbf{q}\| \leq 0$.

Then, $V_{\mathbf{q}}$ and h_l are compatible in $\Gamma \cap \mathscr{F}$.

Proof. We rely on Proposition 8.2.1. In the setting considered here, (8.1) reads as

$$\zeta_1 \coloneqq \min_{\mathbf{x}\in\Gamma,\beta\in\mathbb{R}} \|2\beta(\mathbf{x}-\mathbf{c}_l)-2(\mathbf{x}-\mathbf{q})\|^2 \tag{8.11a}$$

$$\text{s.t. } \beta \geq 0, \tag{8.11b}$$

$$\|\mathbf{x}-\mathbf{c}_l\|^2 - r_l^2 \geq 0. \tag{8.11c}$$

It follows that $\zeta_1 = 0$ if and only if there exists $\mathbf{x} \in \Gamma$ and $\beta \in \mathbb{R}\backslash\{1\}$ (note that $\beta = 1$ and $\zeta_1 = 0$ are not possible because $q \in \mathscr{F}$) such that $\mathbf{x} = \frac{1}{\beta-1}(\beta\mathbf{c}_l - \mathbf{q})$, $\beta \geq 0$ and $\|\mathbf{x}-\mathbf{c}_l\|^2 - r_l^2 \geq 0$. Equivalently, $\zeta_1 = 0$ if and only if there exists $\beta \in \mathbb{R}\backslash\{1\}$ such that $\beta \geq 0$, $|\beta - 1| \leq \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$ and $\beta(\|\mathbf{x}_0-\mathbf{q}\| - \|\mathbf{c}_l-\mathbf{q}\|) \geq \|\mathbf{x}_0-\mathbf{q}\|$. Note that since $\mathbf{q} \in \mathscr{F}$, $\|\mathbf{c}_l-\mathbf{q}\| \geq r_l$, and therefore the condition $\beta \geq 1 - \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$ trivially holds if $\beta \geq 0$. Hence, $\zeta_1 = 0$ if and only if there exists $\beta \in \mathbb{R}\backslash\{1\}$ such that $\beta \geq 0$, $\beta \leq 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$, and $\beta(\|\mathbf{x}_0-\mathbf{q}\| - \|\mathbf{c}_l-\mathbf{q}\|) \geq \|\mathbf{x}_0-\mathbf{q}\|$. We distinguish two cases: (i) suppose that $\|\mathbf{x}_0-\mathbf{q}\| - \|\mathbf{c}_l-\mathbf{q}\| \leq 0$. Then, since $\mathbf{x}_0 \neq q$, it follows that $\beta(\|\mathbf{x}_0-\mathbf{q}\| - \|\mathbf{c}_l-\mathbf{q}\|) \geq \|\mathbf{x}_0-\mathbf{q}\|$ can not hold. Therefore, $\zeta_1 \neq 0$ and $V_\mathbf{q}$ and h_l are compatible in Γ; (ii) suppose instead that $\|\mathbf{x}_0-\mathbf{q}\| - \|\mathbf{c}_l-\mathbf{q}\| > 0$. Then, $\zeta_1 = 0$ if and only if $\frac{\|\mathbf{x}_0-\mathbf{q}\|}{\|\mathbf{x}_0-\mathbf{q}\|-\|\mathbf{c}_l-\mathbf{q}\|} \leq 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$. Consequently, if $\frac{\|\mathbf{x}_0-\mathbf{q}\|}{\|\mathbf{x}_0-\mathbf{q}\|-\|\mathbf{c}_l-\mathbf{q}\|} > 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$, then $V_\mathbf{q}$ and h_l are compatible in Γ. Consider then the case when $\frac{\|\mathbf{x}_0-\mathbf{q}\|}{\|\mathbf{x}_0-\mathbf{q}\|-\|\mathbf{c}_l-\mathbf{q}\|} \leq 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$ so that $\zeta_1 = 0$. Then, (8.2) reads

$$\zeta_2 \coloneqq \min_{\beta\in\mathbb{R}\backslash\{1\}} \frac{1}{(\beta-1)^2}\hat{\Phi}(\beta) \tag{8.12a}$$

$$\text{s.t. } \frac{\|\mathbf{x}_0-\mathbf{q}\|}{\|\mathbf{x}_0-\mathbf{q}\|-\|\mathbf{c}_l-\mathbf{q}\|} \leq \beta \leq 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}, \tag{8.12b}$$

where $\hat{\Phi}(\beta) = \beta(\alpha_l\|\mathbf{q}-\mathbf{c}_l\|^2 - \alpha_l r_l^2(1-\beta)^2 - \beta(\mathbf{q}-\mathbf{c}_l)^\top Q(\mathbf{q}-\mathbf{c}_l))$. By computing the roots of $\hat{\Phi}(\beta) = 0$, it follows that if $\beta_+ \geq 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}$, then $\hat{\Phi}(\beta) \geq 0$ for all $\beta \in [0, \beta_+]$, which implies that $\hat{\Phi}(\beta) \geq 0$ for all $\beta \in [\frac{\|\mathbf{x}_0-\mathbf{q}\|}{\|\mathbf{x}_0-\mathbf{q}\|-\|\mathbf{c}_l-\mathbf{q}\|}, 1 + \frac{\|\mathbf{c}_l-\mathbf{q}\|}{r_l}]$, from which it follows that $\zeta_2 \geq 0$ and $V_\mathbf{q}$ and h_l are compatible in Γ. □

Proposition 8.2.9 provides a test for compatibility over a Lyapunov level set that only requires checking a set of algebraic conditions. Therefore, checking the compatibility of $V_\mathbf{q} = \|\mathbf{x}-\mathbf{q}\|^2$ and $h_l(\mathbf{x}) = \|\mathbf{x}-\mathbf{c}_l\|^2 - r_l^2$ over a Lyapunov sublevel set for a single integrator system can be done very efficiently.

8.2.4 Compatibility Verification for Higher Relative Degree Systems

Here we extend the results of Section 8.2.1 to a larger class of system dynamics and barrier functions, specifically High-Order Control Barrier Functions (HOCBFs) [206]. Let $h : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function defining a safe set of the form (2.6). Consider the situation where h has to be differentiated $\bar{m} \in \mathbb{Z}_{>0}$ times along the dynamics (3.1) until the control $\mathbf{u}$ appears explicitly (this is referred to as m being the relative degree of h under system (3.1), cf. [199]).

This means that, in order to ensure that the value of h remains positive at all times (i.e., $\mathcal{C}$ is positively invariant), we need to reason with its higher-order derivatives. To do so, given differentiable extended class $\mathcal{K}_\infty$ functions $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(\bar{m}-1)}$, define a series of functions $\phi_0, \ldots, \phi_{\bar{m}-1} : \mathbb{R}^n \to \mathbb{R}$ as follows: $\phi_0 = h$ and

$$\phi_i(\mathbf{x}) = L_f\phi_{i-1}(\mathbf{x}) + \alpha^{(i)}(\phi_{i-1}(\mathbf{x})), \quad i \in \{1, \cdots, \bar{m} - 1\}.$$

We further define sets $\mathcal{C}_1, \cdots, \mathcal{C}_{\bar{m}}$ as $\mathcal{C}_1 = \mathcal{C}$ and

$$\mathcal{C}_i = \{\mathbf{x} \in \mathbb{R}^n : \phi_{i-1}(\mathbf{x}) \geq 0\}, \quad i \in \{2, \cdots, \bar{m}\}.$$

The function h is a high-order control barrier function (HOCBF) of $\mathcal{C}$ if one can find differentiable, extended class $\mathcal{K}_\infty$ functions $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(m)}$ such that, for all $\mathbf{x} \in \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$, there exists $u \in \mathbb{R}^m$ satisfying

$$L_f\phi_{\bar{m}-1}(\mathbf{x}) + L_g\phi_{\bar{m}-1}(\mathbf{x})\mathbf{u} + \alpha^{(\bar{m})}(\phi_{\bar{m}-1}(\mathbf{x})) \geq 0. \tag{8.13}$$

If $\bar{m} = 1$, this definition corresponds to the notion of CBF. According to [206, Theorem 5], any locally Lipschitz controller that satisfies (8.13) at each $\mathbf{x} \in \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$ renders the set $\mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$ positively invariant for system (3.1).

We next give an analogue of Definition 2.6.3 for HOCBFs.

Definition 8.2.10. (Compatibility of CLF-HOCBF pair): *Let $\mathcal{D} \subset \mathbb{R}^n$ be open, $\mathcal{C} \subset \mathcal{D}$ be closed, V a CLF on $\mathcal{D}$ and h a HOCBF of $\mathcal{C}$. Then, V and h are compatible at $x \in \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$ if there exists $u \in \mathbb{R}^m$ satisfying* (2.5) *and* (8.13) *simultaneously. We refer to both functions as compatible in a set $\tilde{\mathcal{D}}$ if they are compatible at every point in $\tilde{\mathcal{D}}$.*

The following result is an analogue of Proposition 8.2.1 for the case when h is a HOCBF. Its proof follows an analogous argument and we omit it for space reasons.

Proposition 8.2.11. (Characterization of CLF-HOCBF Compatibility): *Given $\mathbf{q} \in \mathscr{F}$, let $V_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ be a CLF of (3.1) with respect to $\mathbf{q}$. Let h be a HOCBF of $\mathcal{C}$ with relative degree $\bar{m} \in \mathbb{Z}_{>0}$. Let $W_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ be a positive definite function with respect to $\mathbf{q}$ and $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(\bar{m})}$ be differentiable extended class $\mathcal{K}_\infty$ functions. For $\Gamma \subset \mathcal{R}$, let*

$$\zeta_1 = \min_{\mathbf{x}\in\Gamma, \beta\in\mathbb{R}} \left\| \beta L_g \phi_{\bar{m}-1}(\mathbf{x}) - L_g V_{\mathbf{q}}(\mathbf{x}) \right\|^2, \tag{8.14a}$$

$$s.t. \quad \beta \geq 0, \ \phi_i(\mathbf{x}) \geq 0, \ i \in [\bar{m} - 1]. \tag{8.14b}$$

If $\zeta_1 \neq 0$, then V_q and h are compatible in $\Gamma \cap \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \mathcal{C}_{\bar{m}}$. Otherwise, if $\zeta_1 = 0$, let

$$\zeta_2 = \min_{\mathbf{x}\in\Gamma, \beta\in\mathbb{R}} \tilde{\Phi}(\mathbf{x}, \beta) \tag{8.15a}$$

$$s.t. \quad \beta \geq 0, \ \phi_i(x) \geq 0, \ i \in [\bar{m} - 1], \tag{8.15b}$$

where $\tilde{\Phi}(\mathbf{x}, \beta) = -W_{\mathbf{q}}(\mathbf{x}) - L_f V_{\mathbf{q}}(\mathbf{x}) + \beta(L_f \phi_{\bar{m}-1}(\mathbf{x}) + \alpha^{(\bar{m})}(\phi_{\bar{m}-1}(\mathbf{x})))$. If $\zeta_2 \geq 0$, then $V_{\mathbf{q}}$ and h are compatible in $\Gamma \cap \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \mathcal{C}_{\bar{m}}$. Conversely, if $V_{\mathbf{q}}$ and h are compatible in $\Gamma \cap \mathcal{C} \cap \mathcal{C}_2 \cap \cdots \mathcal{C}_m$, then there exists a set of differentiable extended class $\mathcal{K}_\infty$ functions $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(\bar{m})}$ and a positive definite function $W_{\mathbf{q}}$ with respect to $\mathbf{q}$ such that either $\zeta_1 \neq 0$ or $\zeta_1 = 0$ and $\zeta_2 \geq 0$.

To conclude this section, we consider the case of double-integrator dynamics and circular obstacles. The double-integrator dynamics are given by

$$\begin{pmatrix} \dot{\mathbf{x}} \\ \dot{\mathbf{v}} \end{pmatrix} = \begin{pmatrix} \mathbf{0}_k & \mathbf{I}_k \\ \mathbf{0}_k & \mathbf{0}_k \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{v} \end{pmatrix} + \begin{pmatrix} \mathbf{0}_k \\ \mathbf{I}_k \end{pmatrix} \mathbf{u}, \tag{8.16}$$

with $k \in \mathbb{Z}_{>0}$ such that $n = 2k$, states $\mathbf{x} \in \mathbb{R}^k$ and $\mathbf{v} \in \mathbb{R}^k$, and input $\mathbf{u} \in \mathbb{R}^k$. As pointed out in [207], only states of the form $(\mathbf{x}_f, \mathbf{0}_k) \in \mathbb{R}^n$ are stabilizable for (8.16), and for any $\mathbf{x}_f \in \mathbb{R}^k$, if we let $\mathbf{q} = (\mathbf{x}_f, \mathbf{0}_n)$, then $V_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ defined as $V_{\mathbf{q}}(\mathbf{x}, \mathbf{v}) = \|\mathbf{x} - \mathbf{x}_f\|^2 + \|\mathbf{v}\|^2 + (\mathbf{x} - \mathbf{x}_f)^\intercal \mathbf{v}$ is a CLF with respect to $\mathbf{q}$. Next, consider $h : \mathbb{R}^n \to \mathbb{R}$ given by $h(\mathbf{x}, \mathbf{v}) = \|\mathbf{x} - \mathbf{x}_c\|^2 - r^2$, for some $\mathbf{x}_c \in \mathbb{R}^k$ and $r > 0$. The

following result shows that for this choice of V and h, (8.14) and (8.15) take a tractable form.

Corollary 8.2.12. (CLF-HOCBF Compatibility for Circular Obstacles and Double Integrator): *Consider the double integrator dynamics* (8.16). *Let* $\mathbf{q} = (\mathbf{x}_f, \mathbf{0}_k) \in \mathbb{R}^n$, *and let* $V_q(\mathbf{x}, \mathbf{v}) = \|\mathbf{x} - \mathbf{x}_f\|^2 + \|\mathbf{v}\|^2 + (\mathbf{x} - \mathbf{x}_f)^\top \mathbf{v}$ *be a CLF with respect to* $\mathbf{q}$, $W_\mathbf{q} : \mathbb{R}^n \to \mathbb{R}$ *a positive definite function with respect to* $\mathbf{q}$, *and* $h(\mathbf{x}, \mathbf{v}) = \|\mathbf{x} - \mathbf{x}_c\|^2 - r^2$ *for some* $\mathbf{x}_c \in \mathbb{R}^k$, $r > 0$ *a HOCBF. Let* $\alpha_1 > 0$, $\alpha_2 > 0$, *and* $\phi_0 : \mathbb{R}^n \to \mathbb{R}$, $\phi_1 : \mathbb{R}^n \to \mathbb{R}$ *defined as:*

$$\phi_0(\mathbf{x}, \mathbf{v}) = h(\mathbf{x}),$$
$$\phi_1(\mathbf{x}, \mathbf{v}) = 2(\mathbf{x} - \mathbf{x}_c)^\top \mathbf{v} + \alpha_1(\|\mathbf{x} - \mathbf{x}_c\|^2 - r^2),$$

and $\mathcal{C}_1 = \{(\mathbf{x}, \mathbf{v}) \in \mathbb{R}^{2n} : \phi_1(\mathbf{x}, \mathbf{v}) \geq 0\}$. *For* $\Gamma \subset \mathcal{R}$, *let*

$$\hat{\zeta}_1 = \min_{\mathbf{x} \in \Gamma, \beta \in \mathbb{R}, \tilde{\mathbf{x}} \in \mathbb{R}^k} \|2\tilde{\mathbf{x}} - 2\mathbf{v} - (\mathbf{x} - \mathbf{x}_f)\|^2, \tag{8.17a}$$

$$s.t. \quad \beta \geq 0, \ \phi_i(\mathbf{x}) \geq 0, \ i \in \{0, 1\}, \tag{8.17b}$$

$$\beta(\mathbf{x} - \mathbf{x}_c) - \tilde{\mathbf{x}} \leq 0, \ \tilde{\mathbf{x}} - \beta(\mathbf{x} - \mathbf{x}_c) \leq 0. \tag{8.17c}$$

If $\hat{\zeta}_1 \neq 0$, *then* $V_\mathbf{q}$ *and* h *are compatible in* $\Gamma \cap \mathcal{C} \cap \mathcal{C}_1$. *Otherwise, if* $\hat{\zeta}_1 = 0$, *let*

$$\hat{\zeta}_2 = \min_{\substack{(\mathbf{x}, \mathbf{v}) \in \Gamma, \beta \in \mathbb{R}, \\ \tilde{\mathbf{x}} \in \mathbb{R}^k, \tilde{\mathbf{v}} \in \mathbb{R}^k}} \hat{\Phi}(\mathbf{x}, \mathbf{v}, \tilde{\mathbf{x}}, \tilde{\mathbf{v}}) \tag{8.18a}$$

$$s.t. \quad \beta \geq 0, \ \phi_i(\mathbf{x}) \geq 0, \ i \in \{0, 1\}, \tag{8.18b}$$

$$2\tilde{\mathbf{x}} - 2\mathbf{v} + \mathbf{x} - \mathbf{x}_f \leq 0, \tag{8.18c}$$

$$-2\tilde{\mathbf{x}} + 2\mathbf{v} - (\mathbf{x} - \mathbf{x}_f) \leq 0, \tag{8.18d}$$

$$\beta(\mathbf{x} - \mathbf{x}_c) - \tilde{\mathbf{x}} \leq 0, \ \tilde{\mathbf{x}} - \beta(\mathbf{x} - \mathbf{x}_c) \leq 0, \tag{8.18e}$$

$$\beta\mathbf{v} - \tilde{\mathbf{v}} \leq 0, \ -\beta\mathbf{v} + \tilde{\mathbf{v}} \leq 0, \tag{8.18f}$$

where $\hat{\Phi}(\mathbf{x}, \mathbf{v}, \tilde{\mathbf{x}}, \tilde{\mathbf{v}}) = 2\tilde{\mathbf{v}}^\top \mathbf{v} + \alpha_1 \tilde{\mathbf{x}}^\top \mathbf{v} + 2\alpha_2 \tilde{\mathbf{x}}^\top \mathbf{v} + \alpha_2 \alpha_1 \tilde{\mathbf{x}}^\top (\mathbf{x} - \mathbf{x}_c) - \alpha_1 \alpha_2 r^2 \beta - 2(\mathbf{x} - \mathbf{x}_f)^\top \mathbf{v} - \|\mathbf{v}\|^2 - W_\mathbf{q}(\mathbf{x}, \mathbf{v})$. *If* $\hat{\zeta}_2 \geq 0$, *then* $V_\mathbf{q}$ *and* h *are compatible in* $\Gamma \cap \mathcal{C} \cap \mathcal{C}_1$.

Proof. The result follows from Proposition 8.2.11 and by introducing the new variables $\tilde{\mathbf{x}} = \beta(\mathbf{x} - \mathbf{x}_c)$, $\tilde{\mathbf{v}} = \beta\mathbf{v}$. □

Note that (8.17) is a QCQP, and if W_q is quadratic, (8.18) is also a QCQP and can therefore be solved efficiently [205].

8.3 C-CLF-CBF-RRT

In this section, we introduce a novel motion planning algorithm, which we term `Compatible-CLF-CBF-RRT` (`C-CLF-CBF-RRT`), that leverages the compatibility results from Section 8.2 to generate collision-free paths that can be tracked using CLF-CBF based controllers.

8.3.1 CLF-CBF Compatible Paths

We start by defining formally the type of paths that we seek to find using our motion planning algorithm. Intuitively, a path is *CLF-CBF compatible* if the CLF-CBF controller (2.14) successfully connects pairs of consecutive waypoints in the path.

Definition 8.3.1. (CLF-CBF Compatible Path): *Let* $\mathcal{A} = \{\mathbf{x}_i\}_{i=1}^{N_a} \subset \mathscr{F}$ *be a sequence of points, with* $N_a \in \mathbb{Z}_{>0}$, $\mathbf{x}_1 = \mathbf{x}_{init}$ *and* $\mathbf{x}_{N_a} \in \mathcal{X}_{goal} := \mathcal{B}(\mathbf{x}_{goal}, \delta_{goal})$, *where* $\mathbf{x}_{goal} \in \mathbb{R}^n$ *and* $\delta_{goal} > 0$. $\mathcal{A}$ *is a CLF-CBF compatible path if for each* $i \in [N_a - 1]$,

(1) there exists a CLF $V_i : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ *with respect to* $\mathbf{x}_{i+1}$ *in an open set containing* $\Gamma_i := \{\mathbf{x} \in \mathbb{R}^n : V_i(\mathbf{x}) \leq V_i(\mathbf{x}_i)\}$ *for system* (3.1)*;*

(2) there exist extended class $\mathcal{K}_\infty$ *functions* $\{\alpha_{i,l} : \mathbb{R} \to \mathbb{R}\}_{l \in [M]}$ *and positive definite functions* $W_i : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ *with respect to* $\mathbf{x}_{i+1}$ *such that the optimization problem*

$$\begin{aligned} &\min_{\mathbf{u} \in \mathbb{R}^m} \frac{1}{2} \|\mathbf{u}\|^2 \\ &s.t.\ L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x}) u \geq -\alpha_{i,l}(h_{j,l}(\mathbf{x})),\ \ \forall j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &\quad L_f V_i(\mathbf{x}) + L_g V_i(\mathbf{x}) u + W_i(\mathbf{x}) \leq 0. \end{aligned} \tag{8.19}$$

is feasible for all $\mathbf{x} \in \Gamma_i \cap \mathscr{F}$.

For each $i \in [N_a - 1]$, let $u_i^* : \Gamma_i \cap \mathscr{F} \to \mathbb{R}^m$ be a function mapping each $\mathbf{x} \in \Gamma_i \cap \mathscr{F}$ to the solution of (8.19).

Under the assumption that u_i^* is locally Lipschitz, cf. Remark 8.2.5, the feasibility of (8.19) ensures that the solution of the closed-loop system $\dot{\mathbf{x}} = f(\mathbf{x}) +$

$g(\mathbf{x})u_i^*(\mathbf{x})$ with initial condition $\mathbf{x}_i$ (which we denote as $\mathbf{x}(\cdot;\mathbf{x}_i)$) is collision-free and asymptotically converges to $\mathbf{x}_{i+1}$. Indeed,

(1) the satisfaction of the CLF constraint $L_fV_i(\mathbf{x})+L_gV_i(\mathbf{x})u+W_i(\mathbf{x}) \leq 0$ at time $t \geq 0$ ensures that $\frac{d}{dt}V(x(t;\mathbf{x}_i)) < 0$, and $x(t;\mathbf{x}_i)$ asymptotically converges to $\mathbf{x}_{i+1}$;

(2) the satisfaction of the BNCBF constraint $L_fh_{j,l}(\mathbf{x})+L_gh_{j,l}(\mathbf{x})\mathbf{u} \geq -\alpha_{i,l}(h_{j,l}(\mathbf{x}))$ for all $j \in \mathcal{I}_l(x)$, $l \in [M]$ at time $t \geq 0$ ensures that $\frac{d}{dt}h_{j,l}(x(t;\mathbf{x}_i)) \geq -\alpha_l(h_{j,l}(x(t;\mathbf{x}_i)))$ for all $j \in \mathcal{I}_l(x)$, $l \in [M]$, and $x(t;\mathbf{x}_i)$ is collision-free.

Because $\mathbf{x}_i \in \Gamma_i \cap \mathscr{F}$, this ensures that as long as the CLF and BNCBF constraints are satisfied, $x(t;\mathbf{x}_i) \in \Gamma_i \cap \mathscr{F}$. In turn, since the definition of CLF-CBF compatible path ensures that (8.19) is feasible for all $\mathbf{x} \in \Gamma_i \cap \mathscr{F}$, this implies that the controller $u_i^*(x(t;\mathbf{x}_i))$ is well-defined for all $t \geq 0$, and $x(\cdot;\mathbf{x}_i)$ is collision-free and asymptotically converges to $\mathbf{x}_{i+1}$. Therefore, CLF-CBF compatible paths guarantee that the controller obtained by solving (8.19) for each waypoint steers an agent obeying the dynamics (3.1) towards the next waypoint while remaining collision-free. Even though the convergence to the waypoint $\mathbf{x}_{i+1}$ is only achieved in infinite time, one can execute the controller u_i^* until the agent is sufficiently close to $\mathbf{x}_{i+1}$ and then switch to the next controller u_{i+1}^*. We elaborate more on this point in Section 8.4, where we identify conditions on the CLF-CBF compatible path under which the controllers $\{u_i^*\}_{i=1}^{N_a-1}$ can steer the agent from a neighborhood of each waypoint to a neighborhood of the next one, hence ensuring that (8.19) is feasible at all times if we switch to the next controller u_{i+1}^* when the agent is sufficiently close to $\mathbf{x}_{i+1}$.

Remark 8.3.2. (Controllability Requirements for CLF-CBF Compatible Paths): Definition 8.3.1 requires each of the points in the path $\mathcal{A}$ to be asymptotically stabilizable. This condition imposes some structural properties on the class of systems that admit such paths, which we examine next:

Same number of inputs and state variables: In the case when $m = n$ and $g(\mathbf{x})$ is invertible for all $\mathbf{x} \in \mathbb{R}^n$, CLF-CBF compatible paths exist because any point $\mathbf{q} \in \mathbb{R}^n$ is asymptotically stabilizable. Indeed, in this setting the

function $V_{\mathbf{q}} : \mathbb{R}^n \to \mathbb{R}$ defined by $V_{\mathbf{q}}(\mathbf{x}) = \frac{1}{2}\|\mathbf{x} - \mathbf{q}\|^2$ is a CLF with respect to $\mathbf{q}$;

Fewer inputs than state variables: In the case when $m < n$, the set of stabilizable points is limited. For instance, for linear systems with $f(\mathbf{x}) = A\mathbf{x}$ and $g(\mathbf{x}) = B$, with $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$, only the points $\mathbf{q} \in \mathbb{R}^n$ such that $A\mathbf{q} \in \mathrm{Im}(B)$ are stabilizable. This is not a major restriction in a lot of cases of interest. For example, for a double-integrator system, where $m = k$ and $n = 2k$, with $k \in \mathbb{Z}_{>0}$, and

$$A = \begin{pmatrix} \mathbf{0}_k & \mathbf{I}_k \\ \mathbf{0}_k & \mathbf{0}_k \end{pmatrix}, \quad B = \begin{pmatrix} \mathbf{0}_k \\ \mathbf{I}_k \end{pmatrix},$$

this condition restricts the set of stabilizable points to those that have a zero velocity, but arbitrary position, as pointed out in Section 8.2.4. In general, if $m < n$, there often exists a smooth change of coordinates $\psi : \mathbb{R}^n \to \mathbb{R}^m$ that transforms the dynamics into a single integrator in $\mathbb{R}^m$. In [190, Section IV.A] and [9], for instance, this is achieved for unicycle dynamics, by taking the transformation $\psi(x_1, x_2, \theta) = [x_1 + l_0\cos(\theta), x_2 + l_0\sin(\theta)]$ (where $l_0 > 0$ is a positive design parameter). Then, for any $\mathbf{q} \in \mathrm{Im}(\psi)$, the set $M_{\mathbf{q}} = \{\mathbf{x} \in \mathbb{R}^n : \psi(\mathbf{x}) = \mathbf{q}\}$ can be asymptotically stabilized. Therefore, if $m < n$ but such a transformation ψ exists, Definition 8.3.1 can be adapted so that the points in $\mathcal{A}$ are in sets of the form $M_{\mathbf{q}}$. •

8.3.2 Algorithm Description

In this section we introduce the `C-CLF-CBF-RRT` algorithm, which builds upon RRT, cf. [63] (more concretely, `GEOM-RRT`, as defined in Section 2.8), and generates CLF-CBF compatible paths. Algorithm 2 presents the pseudocode description.

The input for `C-CLF-CBF-RRT` consists of a compact, convex set $\mathcal{R} \subset \mathbb{R}^n$, an initial configuration $\mathbf{x}_{\text{init}} \in \mathbb{R}^n$, a goal region $\mathcal{X}_{\text{goal}} \subset \mathbb{R}^n$, the number of iterations $k \in \mathbb{Z}_{>0}$ of the algorithm, the number of iterations $\tau \in \mathbb{Z}_{>0}$ for the compatibility check, a set of extended class $\mathcal{K}_\infty$ functions $\{\alpha_l\}_{l=1}^M$, the steering parameter $\eta > 0$,

Algorithm 2 `C-CLF-CBF-RRT`

Parameters: $\mathcal{R}$, $\mathbf{x}_{\text{init}}$, $\mathcal{X}_{\text{goal}}$, k, τ, η, $\{h_l, \alpha_l\}_{l=1}^{M}$
$\mathcal{T}$.init($\mathbf{x}_{\text{init}}$)
for $i \in [1, \cdots, k]$ **do**
    $\mathbf{x}_{\text{rand}} \leftarrow$ `RANDOM_STATE`()
    $\mathbf{x}_{\text{near}} \leftarrow$ `NEAREST_NEIGHBOR`($\mathbf{x}_{\text{rand}}, \mathcal{T}$)
    $\mathbf{x}_{\text{new}} \leftarrow$ `NEW_STATE`($\mathbf{x}_{\text{rand}}, \mathbf{x}_{\text{near}}, \eta$)
    if not `FREE_SPACE`($\mathbf{x}_{\text{new}}$) **then**
     skip to next iteration
    end if
    $V, W \leftarrow$ `FIND_CLF`($\mathbf{x}_{\text{new}}$)
    if `COMPATIBILITY`($\mathbf{x}_{\text{near}}, \mathbf{x}_{\text{new}}, \tau, \{h_l, \alpha_l\}_{l=1}^{M}, V, W$) **then**
        $\mathcal{T}$.`add_vertex`($\mathbf{x}_{\text{new}}$)
        $\mathcal{T}$.`add_edge`($\mathbf{x}_{\text{near}}, \mathbf{x}_{\text{new}}$)
        if $\mathbf{x}_{\text{new}} \in \mathcal{X}_{\text{goal}}$ **then**
            return $\mathcal{T}$
        end if
    end if
end for
return $\mathcal{T}$

and a set of obstacles $\{\mathcal{O}_l\}_{l=1}^{M}$ defined by functions $h_l : \mathbb{R}^n \to \mathbb{R}$ for $l \in [M]$. At the beginning, a tree $\mathcal{T}$ is initialized with a single node at $\mathbf{x}_{\text{init}}$ and no edges.

The `C-CLF-CBF-RRT` algorithm operates similarly to the `GEOM-RRT` algorithm described in Section 2.8.

> At each iteration, steps 4:-6: are the same as in Algorithm 1. In general, `RANDOM_STATE` samples $\mathcal{R}$ uniformly, but if we know that only a subset of the points in $\mathcal{R}$ is stabilizable, one can choose to sample uniformly only over such points. The functions `NEAREST_NEIGHBOR` and `NEW_STATE` operate identically to how they do in `GEOM-RRT`. We note that, since $\mathcal{R}$ is convex, $\mathbf{x}_{\text{new}}$ is guaranteed to belong to it. Next, the function `FREE_SPACE` checks whether $\mathbf{x}_{\text{new}} \in \mathscr{F}$. If $\mathbf{x}_{\text{new}} \notin \mathscr{F}$, it skips to the next iteration. Otherwise, `FIND_CLF` finds a CLF V and associated positive definite function W with respect to $\mathbf{x}_{\text{new}}$. Then, the `COMPATIBILITY` function checks whether there exists a CLF-CBF based controller that steers the system from $\mathbf{x}_{\text{near}}$ to $\mathbf{x}_{\text{new}}$. If the `COMPATIBILITY` function returns a value of `True`, then $\mathbf{x}_{\text{new}}$ is added as a vertex to $\mathcal{T}$ and is connected by an edge from x_{near}. If $\mathbf{x}_{\text{new}} \in \mathcal{X}_{\text{goal}}$, there exists a single path in $\mathcal{T}$ from $\mathbf{x}_{\text{init}}$ to $\mathbf{x}_{\text{new}}$.

In Section 8.3.3, we discuss in detail the definition of the function `COMPATIBILITY`. The function `FIND_CLF` aims to find a control Lyapunov function, which is a challenging problem for general control systems. Beyond what we noted in Remark 8.3.2, one can use for this a variety of tools, such as sum-of-squares techniques [208, 209], neural networks [210, 211], or the learner-falsifier framework [212].

Remark 8.3.3. (Sampling in Systems with Fewer Inputs than State Variables): A requirement for step 7: of Algorithm 2 to return a value of `True` is that $\mathbf{x}_{\text{new}}$ is stabilizable. Since this point is obtained through random sampling, in general this might not be the case. However, if we know the set of points that are stabilizable (for instance, an m-dimensional manifold $\mathcal{M}$ in the case of systems with $m < n$ controls, cf. Remark 8.3.2), then we can project $\mathbf{x}_{\text{new}}$ onto such set. •

8.3.3 The `COMPATIBILITY` function

Here we define the operation of the `COMPATIBILITY` function. Given the CLF V and the positive definite function W with respect to $\mathbf{x}_{\text{new}}$ found by `FIND_CLF`,

it checks whether the optimization problem

$$\begin{aligned} &\min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\|\mathbf{u}\|^2, \\ &\quad \text{s.t. } L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})u \geq -\alpha_l(h_{j,l}(\mathbf{x})),\ j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &\qquad L_f V(\mathbf{x}) + L_g V(\mathbf{x})\mathbf{u} + W(\mathbf{x}) \leq 0. \end{aligned} \tag{8.20}$$

is feasible for all $\mathbf{x} \in \Theta \cap \mathscr{F}$, where $\Theta = \{\mathbf{x} \in \mathbb{R}^n : V(\mathbf{x}) \leq V(\mathbf{x}_{\text{near}})\}$ and α_l is the class $\mathcal{K}_\infty$ function associated with h_l.

1. Find obstacles that intersect domain of interest: To check whether (8.20) is feasible, we first find the obstacles that intersect Θ, i.e., we find $l \in [M]$ such that $\text{Cl}(\mathcal{O}_l) \cap \Theta \neq \varnothing$. This can be done by solving the following optimization problem for every $l \in [M]$:

$$\begin{aligned} &\min_{\mathbf{x}\in\mathbb{R}^n} V(\mathbf{x}) \\ &\quad \text{s.t. } h_{i,l}(\mathbf{x}) \leq 0, \quad \forall i \in [N_l]. \end{aligned} \tag{8.21}$$

Then, $\text{Cl}(\mathcal{O}_l) \cap \Theta \neq \varnothing$ iff the optimal value of (8.21) is smaller than or equal to $V(\mathbf{x}_{\text{near}})$. Problem (8.21) is tractable under the settings considered in Section 8.2, where V is quadratic and the constraints are affine (in which case (8.21) is a quadratic program) or ellipsoidal (in which case (8.21) is a QCQP).

2. Reduce number of constraints and check for compatibility: Next, we check the compatibility of the CLF with each of the CBFs associated with the obstacles in $\mathcal{L} := \{l \in [M] : \Theta \cap \text{Cl}(\mathcal{O}_l) \neq \varnothing\}$ (Lemma 8.6.1 ensures this step retains consistency). Then, `COMPATIBILITY` uses Proposition 8.2.1 for each $l \in \mathcal{L}$. First, for each $l \in \mathcal{L}$, it solves the optimization problem (8.1) with $\Gamma = \Theta$ and obtains the value $\zeta_{1,l}$. If $\zeta_{1,l} = 0$, it solves (8.2) with $\Gamma = \Theta$ and obtains the value $\zeta_{2,l}$. If for all $l \in \mathcal{L}$, the obtained values of $\zeta_{1,l}$ and $\zeta_{2,l}$ are such that $\zeta_{1,l} \neq 0$ or $\zeta_{1,l} = 0$ and $\zeta_{2,l} \geq 0$, then V and h_l are compatible in $\Theta \cap \mathscr{F}$ for all $l \in \mathcal{L}$ and `COMPATIBILITY` returns `True`.

3. If unsuccessful, increase feasibility set and recheck: Otherwise, it updates the set of extended class $\mathcal{K}_\infty$ functions and the function W in a way that increases the feasible set of (8.20), and performs again the same check about its feasibility. In every subsequent iteration, we use a new W obtained by multiplying the previous one by a constant factor $\sigma \in (0, 1)$, and use linear extended class $\mathcal{K}_\infty$ functions

$\alpha_l(s) = \alpha_{0,l}s$ with the parameter $\alpha_{0,l}$ being multiplied by a constant factor $\bar{\sigma} > 1$ at every iteration. With this choice, the objective function Φ of (8.2) does not decrease at any point, which means that the value of ζ_1 remains the same but the condition $\zeta_2 \geq 0$ becomes easier to satisfy, which makes it easier for `COMPATIBILITY` to return a value of `True`. If after τ of those updates the function still has not returned a value of `True`, it returns a value of `False`. We can also employ other heuristics to make it even easier for `COMPATIBILITY` to return a value of `True`. For example, instead of using constant factors σ, $\bar{\sigma}$, one can increase such factors at every iteration.

Remark 8.3.4. (No Loss of Generality in Assuming Linear Class $\mathcal{K}_\infty$ Function): Since the set Θ is compact (because V is proper), for each $l \in [M]$ and $j \in [N_l]$, the function $h_{j,l}$ is bounded in Θ, i.e., there exists $M_{j,l} > 0$ such that $h_{j,l}(x) < M_{j,l}$ for all $x \in \Theta$. Now suppose that V_q and h_l are compatible in Θ, i.e., there exists a controller $u_{\text{com}} : \mathbb{R}^n \to \mathbb{R}^m$ such that

$$\begin{aligned} &L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x}) u_{\text{com}}(\mathbf{x}) + \alpha_l(h_{j,l}(\mathbf{x})) \geq 0, \ \ \forall j \in \mathcal{I}_l(\mathbf{x}), \\ &L_f V_q(\mathbf{x}) + L_g V_q(\mathbf{x}) u_{\text{com}}(\mathbf{x}) + W(\mathbf{x}) \leq 0, \end{aligned}$$

for all $\mathbf{x} \in \Theta$. Note that there exists $M_{\text{com}} > 0$ sufficiently large such that $M_{\text{com}} z > \alpha_l(z)$ for all $z \in [0, M_{j,l}]$. Using that $h_{j,l}(\mathbf{x}) < M_{j,l}$ for all $\mathbf{x} \in \Theta$, we deduce

$$\begin{aligned} &L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x}) u_{\text{com}}(\mathbf{x}) + M_{\text{com}} h_{j,l}(\mathbf{x}) \geq 0, \ \ \forall j \in \mathcal{I}_l(\mathbf{x}), \\ &L_f V_{\mathbf{q}}(\mathbf{x}) + L_g V_{\mathbf{q}}(\mathbf{x}) u_{\text{com}}(\mathbf{x}) + W(\mathbf{x}) \leq 0, \end{aligned}$$

for all $\mathbf{x} \in \Theta$. Therefore, $V_{\mathbf{q}}$ and h_l are also compatible in Θ using a linear class $\mathcal{K}_\infty$ function $\alpha(z) = M_{\text{comp}} z$. Therefore, without loss of generality, we can assume that the class $\mathcal{K}_\infty$ function used in the `COMPATIBILITY` function is linear. •

8.4 Analysis of `C-CLF-CBF-RRT`

In this section we establish the probabilistic completeness of `C-CLF-CBF-RRT`. We do this by first showing that if `C-CLF-CBF-RRT` returns a tree with a vertex in $\mathcal{X}_{\text{goal}}$, then this tree contains a CLF-CBF compatible path; and then showing that,

under suitable conditions, `C-CLF-CBF-RRT` in fact returns a tree with a vertex in $\mathcal{X}_{\text{goal}}$ with high probability.

Proposition 8.4.1. (`C-CLF-CBF-RRT` and CLF-CBF Compatible Path): *Suppose that `C-CLF-CBF-RRT` returns a tree $\mathcal{T}$ that contains a vertex $\mathbf{q}_{goal} \in \mathcal{X}_{goal}$. Then, the single path in $\mathcal{T}$ from x_{init} to $\mathbf{q}_{goal}$ is CLF-CBF compatible.*

Proof. Let $N_a \in \mathbb{Z}_{>0}$ and $\mathcal{A} = \{\mathbf{x}_i\}_{i=1}^{N_a}$ be the path obtained from `C-CLF-CBF-RRT`, with $\mathbf{x}_1 = \mathbf{x}_{\text{init}}$ and $\mathbf{x}_{N_a} \in \mathcal{X}_{\text{goal}}$. First, `FREE_SPACE` ensures that $\mathbf{x}_i \in \mathscr{F}$ for all $i \in [N_a]$. Moreover, `FIND_CLF` ensures that, for all $i \in [N_a - 1]$, there exists a CLF V_i with respect to $\mathbf{x}_{i+1}$, and `COMPATIBILITY` ensures that there exists a set of class $\mathcal{K}_\infty$ functions $\{\alpha_{i,l}\}_{l=1}^{M}$ and a positive definite function W_i with respect to x_{i+1} such that the optimization problem (8.19) is feasible for all points in the set $\{\mathbf{x} \in \mathbb{R}^n : V_i(\mathbf{x}) \leq V_i(\mathbf{x}_i)\} \cap \mathscr{F}$. This ensures that $\mathcal{A}$ is CLF-CBF compatible. □

We next show that, under some extra assumptions, `C-CLF-CBF-RRT` returns a tree with a vertex in $\mathcal{X}_{\text{goal}}$ with probability one as the number of iterations k goes to infinity. In doing so, our next result is critical as it provides conditions under which there exist neighborhoods around a CLF-CBF compatible path for which points of two consecutive neighborhoods can be connected with a CLF-CBF-based controller.

Lemma 8.4.2. (Compatibility in Neighboring Vertices): *Let $\mathcal{A} = \{\mathbf{x}_i\}_{i=1}^{N_a}$, $N_a \in \mathbb{Z}_{>0}$, be a CLF-CBF compatible path such that there exists $\delta_{clear} > 0$ with $\mathcal{B}(\mathbf{x}_i, \delta_{clear}) \subset \mathscr{F}$ for all $i \in \{2, \cdots, N_a\}$. Let $\mathcal{N}_1 = \{\mathbf{x}_{init}\}$. For each $i \in \{2, \cdots, N_a\}$, assume that there exist sets $\mathcal{N}_i$, with $\mathbf{x}_i \in \mathcal{N}_i$, and $\hat{\Gamma}_i$, with $\Gamma_i \subset \hat{\Gamma}_i$ (and Γ_i defined as in Definition 8.3.1), satisfying the following properties:*

(1) for each $\mathbf{y} \in \mathcal{N}_i$, there exists a CLF $V_{\mathbf{y}} : \hat{\Gamma}_i \to \mathbb{R}$ with respect to $\mathbf{y}$ in $\hat{\Gamma}_i$ (with associated positive definite function $W_{\mathbf{y}}$) and a bounded controller $\hat{u}_{\mathbf{y}} : \hat{\Gamma}_i \to \mathbb{R}^m$ satisfying the corresponding CLF condition in $\hat{\Gamma}_i$;

(2) there exists a bounded controller $u_i^* : \hat{\Gamma}_i \cap \mathscr{F} \to \mathbb{R}^m$ that satisfies the constraints in (8.19) for all points in $\hat{\Gamma}_i$ and, for each $\mathbf{y} \in \mathcal{N}_i$,

$$|(\nabla V_{\mathbf{y}}(\mathbf{x}) - \nabla V_i(\mathbf{x}))^T (f(\mathbf{x}) + g(\mathbf{x})u_i^*(\mathbf{x}))| < W_i(\mathbf{x}), \tag{8.22}$$

for all $\mathbf{x} \in \mathcal{Z} = \{\mathbf{z} \in \mathscr{F} : \exists l \in [M] \text{ s.t. } d(\mathbf{z}, \mathcal{O}_l) \leq \frac{\delta_{clear}}{2}\}$;

(3) for each $\mathbf{y}_2 \in \mathcal{N}_i$ *and* $\mathbf{y}_1 \in \mathcal{N}_{i-1}$, $\Gamma_{\mathbf{y}_1,\mathbf{y}_2} := \{\mathbf{x} \in \mathbb{R}^n : V_{\mathbf{y}_2}(\mathbf{x}) \leq V_{\mathbf{y}_2}(\mathbf{y}_1)\} \subset \hat{\Gamma}_i$;

(4) whenever $\mathbf{x}_{new} \in \mathcal{N}_i$, *global solutions to the optimization problems* (8.1) *and* (8.2) *in* `COMPATIBILITY` *are found.*

Then, for each $i \in \{2, \cdots, N_a\}$, $\mathbf{y}_2 \in \mathcal{N}_i$, *and* $\mathbf{y}_1 \in \mathcal{N}_{i-1}$, *there exists a set of extended class* $\mathcal{K}_\infty$ *functions* $\{\bar{\alpha}_{i,l}\}_{l=1}^M$ *and* $\bar{\sigma} > 0$ *(both dependent on* $\mathbf{y}_1$, $\mathbf{y}_2$*) such that, by taking* $W_{\mathbf{y}_2}^{\bar{\sigma}}(\mathbf{x}) = \bar{\sigma} W_{\mathbf{y}_2}(\mathbf{x})$, *it holds that*

$$\texttt{COMPATIBILITY}(\mathbf{y}_1, \mathbf{y}_2, 1, \{h_l, \bar{\alpha}_{i,l}\}_{l=1}^M, V_{\mathbf{y}_2}, W_{\mathbf{y}_2}^{\bar{\sigma}}) = \texttt{True}.$$

Proof. Given $i \in \{2, \cdots, N_a\}$, $\mathbf{y}_2 \in \mathcal{N}_i$, and $\mathbf{y}_1 \in \mathcal{N}_{i-1}$, our goal is to show that there exists a set of extended class $\mathcal{K}_\infty$ functions $\{\bar{\alpha}_{i,l}\}_{l=1}^M$ and a sufficiently small $\bar{\sigma} > 0$ such that

$$\begin{aligned} &\min_{\mathbf{u} \in \mathbb{R}^m} \frac{1}{2} \|\mathbf{u}\|^2, \\ &\text{s.t. } L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})\mathbf{u} \geq -\bar{\alpha}_{i,l}(h_{j,l}(\mathbf{x})), \ \forall j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &\quad \nabla V_{\mathbf{y}_2}(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})\mathbf{u}) + \bar{\sigma} W_{\mathbf{y}_2}(\mathbf{x}) \leq 0, \end{aligned} \tag{8.23}$$

is feasible for all $\mathbf{x} \in \Gamma_{\mathbf{y}_1,\mathbf{y}_2} \cap \mathscr{F}$. Figure 8.1 provides a visual aid for the argument that follows. The set $\Gamma_{\mathbf{y}_1,\mathbf{y}_2}$ is depicted in red, the sets $\mathcal{N}_i$ in blue, $\mathcal{Z}$ in light purple, and the obstacles $\{\mathcal{O}_l\}_{l=1}^M$ in green. For convenience, we let $T_{\mathbf{y}_1,\mathbf{y}_2} = \Gamma_{\mathbf{y}_1,\mathbf{y}_2} \cap \mathcal{Z}$ (depicted in dark purple).

Feasibility on $(\Gamma_{\mathbf{y}_1,\mathbf{y}_2} \backslash T_{\mathbf{y}_1,\mathbf{y}_2}) \cap \mathscr{F}$: Since $T_{\mathbf{y}_1,\mathbf{y}_2}$ contains all points that are closer than $\frac{\delta_{\text{clear}}}{2}$ from the boundary, there exists $h_0 > 0$ such that $h_{j,l}(\mathbf{x}) > h_0$ for all $\mathbf{x} \in (\Gamma_{\mathbf{y}_1,\mathbf{y}_2} \backslash T_{\mathbf{y}_1,\mathbf{y}_2}) \cap \mathscr{F}$, $l \in [M]$ and $j \in \mathcal{I}_l(\mathbf{x})$. Therefore, by taking $\alpha_{i,l}^* > 0$, with

$$\alpha_{i,l}^* > \frac{\sup\limits_{\substack{x \in (\Gamma_{\mathbf{y}_1,\mathbf{y}_2} \backslash T_{\mathbf{y}_1,\mathbf{y}_2}) \cap \mathscr{F}, \\ j \in \mathcal{I}_l(\mathbf{x})}} |L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x}) \hat{u}_{\mathbf{y}_2}(x)|}{h_0},$$

for each $l \in [M]$ (which exists because $\hat{u}_{\mathbf{y}_2}$ is bounded on $\hat{\Gamma}_i$ by 1), it holds that

$$\begin{aligned} &L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})\hat{u}_{\mathbf{y}_2}(\mathbf{x}) + \alpha^*_{i,l} h_{j,l}(\mathbf{x}) \geq 0, \\ &\qquad\qquad\qquad\qquad\qquad\qquad \forall j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &\nabla V_{\mathbf{y}_2}(\mathbf{x})^T (f(\mathbf{x}) + g(\mathbf{x})\hat{u}_{\mathbf{y}_2}(\mathbf{x})) + \sigma W_{\mathbf{y}_2}(\mathbf{x}) \leq 0, \end{aligned}$$

for all $\mathbf{x} \in (\Gamma_{\mathbf{y}_1,\mathbf{y}_2} \backslash T_{\mathbf{y}_1,\mathbf{y}_2}) \cap \mathscr{F}$ and $\sigma \in (0,1)$, where we have used that $\hat{u}_{\mathbf{y}_2}$ satisfies the CLF condition for $V_{\mathbf{y}_2}$ by 1.

Feasibility on $T_{\mathbf{y}_1,\mathbf{y}_2}$: From (ii), there exists a bounded controller u_i^* satisfying the constraints in (8.19) for all $\mathbf{x} \in \hat{\Gamma}_i$. Since $\Gamma_{\mathbf{y}_1,\mathbf{y}_2} \subset \hat{\Gamma}_i$, cf. 3, u_i^* satisfies the constraints in (8.19) for all $\mathbf{x} \in \Gamma_{\mathbf{y}_1,\mathbf{y}_2}$. Moreover, since (8.22) holds for all $\mathbf{x} \in \mathcal{Z}$ (note that this is only possible because $\mathcal{B}(\mathbf{x}_i, \delta_{\text{clear}}) \subset \mathscr{F}$ and therefore $\mathbf{x}_i \notin \mathcal{Z}$, which means that the right-hand side of (8.22) is strictly positive), by 2 it follows that

$$\nabla V_{\mathbf{y}_2}(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})u_i^*(\mathbf{x})) < 0,$$

for all $\mathbf{x} \in T_{\mathbf{y}_1,\mathbf{y}_2}$. Since $\mathcal{Z}$ is compact, this implies that there exists $\bar{\sigma} \in (0,1)$ sufficiently small such that

$$\begin{aligned} &L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})u_i^*(\mathbf{x}) + \alpha_{i,l}(h_{j,l}(\mathbf{x})) \geq 0, \ \ \forall j \in \mathcal{I}_l(\mathbf{x}), l \in [M], \\ &\nabla V_{\mathbf{y}_2}(\mathbf{x})^\top (f(\mathbf{x}) + g(\mathbf{x})u_i^*(\mathbf{x})) + \bar{\sigma} W_{\mathbf{y}_2}(\mathbf{x}) \leq 0. \end{aligned}$$

for all $\mathbf{x} \in T_{\mathbf{y}_1,\mathbf{y}_2}$.

Hence, by taking $\bar{\alpha}_{i,l}$ as an extended class $\mathcal{K}_\infty$ function such that $\bar{\alpha}_{i,l}(s) > \max\{\alpha_{i,l}(s), \alpha^*_{i,l} s\}$ for all $s \geq 0$, and $\bar{\sigma} \in (0,1)$ sufficiently small as described above, (8.23) is feasible for all $\mathbf{x} \in \Gamma_{\mathbf{y}_1,\mathbf{y}_2} \cap \mathscr{F}$. Since `COMPATIBILITY` finds the global solutions of the optimization problems (8.1) and (8.2), cf. 4, it follows that $\texttt{COMPATIBILITY}(\mathbf{y}_1, \mathbf{y}_2, 1, \{h_l, \bar{\alpha}_{i,l}\}_{l=1}^M, V_{\mathbf{y}_2}, W^{\bar{\sigma}}_{\mathbf{y}_2}) = \texttt{True}$ (note that since (8.23) includes CBF constraints for $l \in [M]$, this argument is valid independently of the set $\mathcal{L}$ found by solving (8.21)). □

Remark 8.4.3. (Verification of Assumptions of Lemma 8.4.2 for Specific Classes of Systems): For systems with the same number of inputs as state variables, the

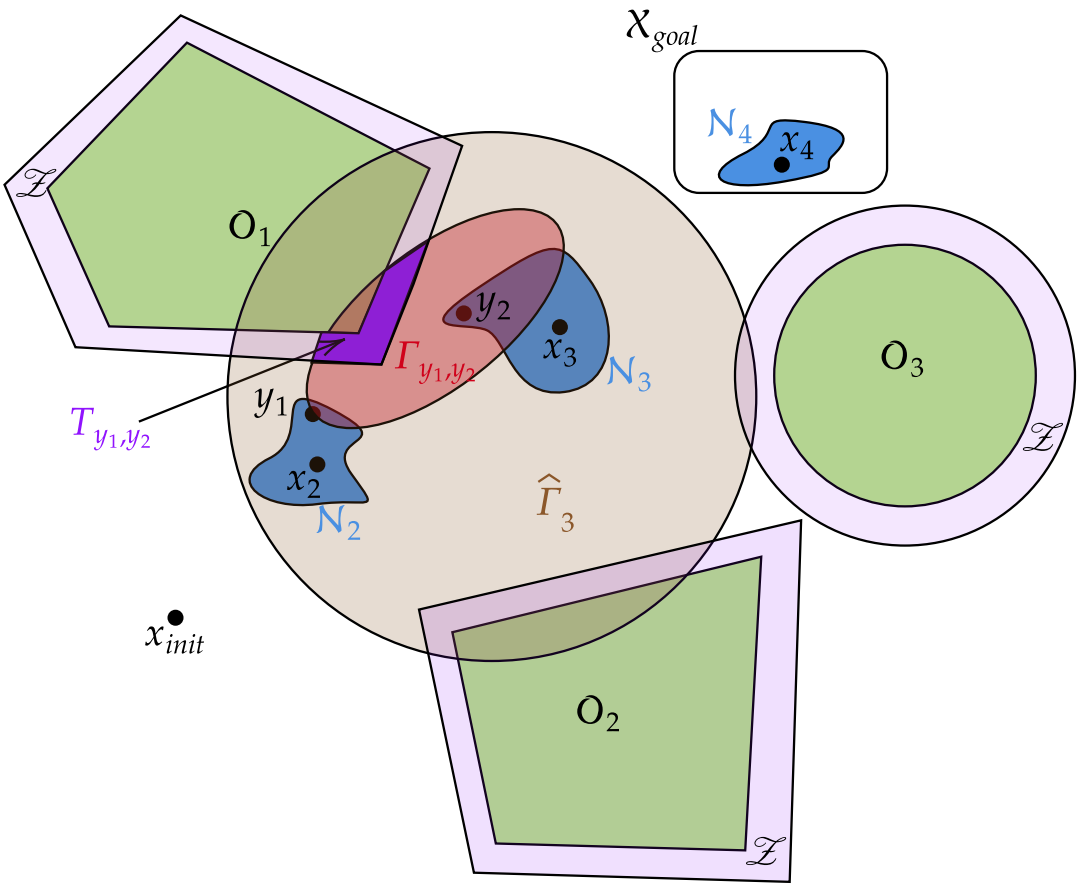


Figure 8.1: Visual aid for the arguments described in the proof of Lemma 8.4.2.

set $\mathcal{N}_i$ in Lemma 8.4.2 can be taken as a ball centered at the waypoint x_i. As mentioned in Remark 8.3.2, for such systems, $V_{\mathbf{y}}(\mathbf{x}) = \frac{1}{2}\|\mathbf{x}-\mathbf{y}\|^2$ is a CLF for any $\mathbf{y} \in \mathbb{R}^n$. Moreover, we can take $W_{\mathbf{y}}(\mathbf{x}) = \|\mathbf{x}-\mathbf{y}\|^2$ and the controller $\hat{u} : \mathbb{R}^n \to \mathbb{R}^n$ defined as $\hat{u}(\mathbf{x}) = -\frac{(\mathbf{x}-\mathbf{y}_2)^\top f(\mathbf{x}) + \|\mathbf{x}-\mathbf{y}_2\|^2}{\|g(\mathbf{x})^\top(\mathbf{x}-\mathbf{y}_2)\|^2} g(\mathbf{x})^\top(\mathbf{x}-\mathbf{y}_2)$ is such that $(\mathbf{x}-\mathbf{y}_2)^\top(f(\mathbf{x}) + g(\mathbf{x})\hat{u}(\mathbf{x})) + \|\mathbf{x}-\mathbf{y}_2\|^2 \leq 0$ for all $\mathbf{x} \in \Gamma_{\mathbf{y}_1,\mathbf{y}_2}$ and is bounded, since

$$\begin{aligned}\|\hat{u}(\mathbf{x})\| &\leq \frac{\|\mathbf{x}-\mathbf{y}_2\|\left(\|f(\mathbf{x})\| + \|\mathbf{x}-\mathbf{y}_2\|\right)}{\|g(\mathbf{x})^\top(\mathbf{x}-\mathbf{y}_2)\|} \frac{\|g(\mathbf{x})^{-1}g(\mathbf{x})(\mathbf{x}-\mathbf{y}_2)\|\left(\|f(\mathbf{x})\| + \|\mathbf{x}-\mathbf{y}_2\|\right)}{\|g(\mathbf{x})^\top(\mathbf{x}-\mathbf{y}_2)\|} \\ &\leq \left\|g(\mathbf{x})^{-1}\right\| \|\mathbf{x}-\mathbf{y}_2\|.\end{aligned}$$

Given that an explicit expression for the CLF is available, the conditions 2, 3 in Lemma 8.4.2 can be verified directly and one can choose the radius of the balls defining $\mathcal{N}_i$ to satisfy them. Furthermore, Propositions 8.2.7 and 8.2.9 provide two settings where condition 4 holds.

A similar argument can be made for the *double integrator* in dimension $2k \in \mathbb{Z}_{>0}$. As mentioned in Remark 8.3.2, in that case only the points of the form $(\mathbf{x}_f, \mathbf{0}_k) \in \mathbb{R}^{2k}$ are stabilizable. Hence, the sets $\mathcal{N}_i$ in Lemma 8.4.2 can be taken in the form $\mathcal{N}_i := \{(\mathbf{x}, \mathbf{0}_k) \in \mathbb{R}^{2k} : \|\mathbf{x} - \mathbf{x}_f\| < \nu_i\}$ for some $\nu_i > 0$. Furthermore, one can use the explicit expression of the CLF provided in Section 8.2.4 and choose the parameters ν_i in order to verify the rest of the assumptions in Lemma 8.4.2. •

In general, if the neighborhood $\mathcal{N}_i$ around $\mathbf{x}_i$ in Lemma 8.4.2 is sufficiently small and $\nabla V_{\mathbf{y}}$ is continuous in $\mathbf{y}$ (with the assumption that $V_{\mathbf{x}_i} = V_i$), the left-hand side of (8.22) can be made sufficiently small so that the inequality holds. Note that Assumptions 1, 3, and 4 are not restrictive and hold in several cases of interest, as outlined in Remark 8.4.3.

Overall, the assumptions in Lemma 8.4.2 ensure that there exist neighborhoods around every waypoint of a CLF-CBF compatible path such that the controller obtained as the solution of (8.19) can connect a point from each neighborhood to any point in the neighborhood of the next waypoint. We next leverage this property to show the probabilistic completeness of `C-CLF-CBF-RRT`.

Proposition 8.4.4. (Probabilistic Completeness of `C-CLF-CBF-RRT`): *Suppose that there exists a CLF-CBF compatible path $\mathcal{A} = \{\mathbf{x}_i\}_{i=1}^{N_a}$, $N_a \in \mathbb{Z}_{>0}$, and suppose that all the assumptions in Lemma 8.4.2 regarding $\mathcal{A}$ hold. Further suppose that*

(1) there exists a positive probabiliy p_i that ***`RANDOM_STATE`*** *returns a point from $\mathcal{N}_i$;*

(2) for each $\mathbf{y} \in \mathcal{N}_i$, ***`FIND_CLF`*** *returns $V_{\mathbf{y}}$ and $W_{\mathbf{y}}$ (as defined in item 1 of Lemma 8.4.2);*

(3) the extended class $\mathcal{K}_\infty$ functions $\{\alpha_{i,l}\}_{i\in[N_a],l\in[M]}$ in (8.19) are upper bounded by linear extended class $\mathcal{K}_\infty$ functions, i.e., there exist $\hat{\alpha}_{i,l} > 0$ for $i \in [N_a]$ and $l \in [M]$ such that $\alpha_{i,l}(s) \leq \hat{\alpha}_{i,l} s$ for all $s \geq 0$;

(4) the steering parameter η in ***`NEW_STATE`*** *is such that*

$$\eta > \max_{i\in[N_a-1]} \max_{\mathbf{y}_2\in\mathcal{N}_{i+1},\mathbf{y}_1\in\mathcal{N}_i} \|\mathbf{y}_2 - \mathbf{y}_1\| .$$

Then, there exists $\tau^* \in \mathbb{Z}_{>0}$ such that if $\tau > \tau^*$, the probability of C-CLF-CBF-RRT *(executed with parameters τ, η, and any set of extended class $\mathcal{K}_\infty$ functions $\{\alpha_l\}_{l\in[M]}$) returning a tree without a vertex in $\mathcal{X}_{goal}$ tends to zero as the number of iterations k goes to infinity.*

Proof. The proof follows a similar reasoning to [108, Theorem 1] that proves probabilistic completeness for `GEOM-RRT`. Let $i \in [N_a - 1]$. First, we show that if $\mathcal{N}_i$ contains a vertex $\mathbf{x}_{\text{near}}$ from the tree $\mathcal{T}$ in `C-CLF-CBF-RRT`, then with probability $p_i > 0$ in the next iteration a vertex will be added from $\mathcal{N}_{i+1}$. To see this, note that by assumption there exists a probability $p_i > 0$ that the function `RANDOM_STATE` returns a point $\mathbf{x}_{\text{rand}}$ from $\mathcal{N}_{i+1}$. Given (iv), the distance between $\mathbf{x}_{\text{near}} \in \mathcal{N}_i$ and $\mathbf{x}_{\text{rand}} \in \mathcal{N}_{i+1}$ is less than η, and therefore $\mathbf{x}_{\text{new}} = \mathbf{x}_{\text{rand}}$. Now, Lemma 8.4.2 ensures that there exists a set of extended class $\mathcal{K}_\infty$ functions $\{\bar{\alpha}_{i,l}\}_{l=1}^M$, a CLF $V_{\mathbf{x}_{\text{rand}}}$ with respect to $\mathbf{x}_{\text{rand}}$ and a positive definite function $W^{\bar{\sigma}}_{\mathbf{x}_{\text{rand}}}$ with respect to $\mathbf{x}_{\text{rand}}$ such that `COMPATIBILITY`$(\mathbf{x}_{\text{near}}, \mathbf{x}_{\text{rand}}, \tau, \{h_l, \bar{\alpha}_{i,l}\}_{l=1}^M, V_{\mathbf{x}_{\text{rand}}}, W^{\bar{\sigma}}_{\mathbf{x}_{\text{rand}}})$ returns `True`. Moreover, since the functions $\{\alpha_{i,l}\}_{l=1}^M$ are upper bounded by linear extended class $\mathcal{K}_\infty$ functions with slopes $\{\hat{\alpha}_{i,l}\}_{l=1}^M$, by performing the updates in the extended class $\mathcal{K}_\infty$ functions described in Section 8.3.3, it follows that there exists τ^* sufficiently large such that if $\tau > \tau^*$, the updated linear extended class $\mathcal{K}_\infty$ functions used in `COMPATIBILITY` have slopes larger than $\{\hat{\alpha}_{i,l}\}_{l=1}^M$ respectively and the coefficient multiplying $W_{\mathbf{x}_{\text{rand}}}$ is smaller than $\bar{\sigma}$, which makes the `COMPATIBILITY` function return `True`. This means that $\mathbf{x}_{\text{rand}}$ is added to $\mathcal{T}$ with the corresponding edge from $\mathbf{x}_{\text{near}}$ to $\mathbf{x}_{\text{rand}}$, as stated.

Next, in order for `C-CLF-CBF-RRT` to reach $\mathcal{X}_{\text{goal}}$ from $\mathbf{x}_{\text{init}}$, the algorithm needs to successively select points from $\mathcal{N}_{i+1}$ as described previously for $i \in [N_a - 1]$. For k iterations of `C-CLF-CBF-RRT`, this stochastic process can be described as k Bernouilli trials [213, Definition 2.5] with success probabilities $\{p_i\}_{i=1}^{N_a-1}$. The algorithm reaches $\mathcal{X}_{\text{goal}}$ from x_{init} after $N_a - 1$ successful outcomes. Let $p := \min_{i\in[N_a-1]} p_i$. Using the same argument as in [108, Theorem 1], the probability that this stochastic process does not have $N_a - 1$ successful outcomes after k iterations is smaller than $\frac{(N_a-1)!}{(N_a-2)!}k^{N_a-1}e^{-pk}$. This means that the probability of `C-CLF-CBF-RRT` returning a tree without a vertex in $\mathcal{X}_{\text{goal}}$ tends to zero as the number of iterations k goes

to infinity. □

Remark 8.4.5. (Verification of Assumptions of Proposition 8.4.4): As mentioned in Remark 8.4.3, for systems with the same number of inputs as state variables, the set $\mathcal{N}_i$ in Lemma 8.4.2 can be taken as a ball centered at the waypoint $\mathbf{x}_i$. If `RANDOM_STATE` samples $\mathcal{R}$ uniformly, it returns a point in such ball with probability equal to its relative volume in $\mathcal{R}$. Furthermore, in this case `FIND_CLF` can simply return $V_{\mathbf{y}}(\mathbf{x}) = \frac{1}{2}\|\mathbf{x}-\mathbf{y}\|^2$ and $W_{\mathbf{y}}(\mathbf{x}) = \|\mathbf{x}-\mathbf{y}\|^2$ for any $\mathbf{y} \in \mathcal{N}_i$. For the *double integrator* in dimension $2k \in \mathbb{Z}_{>0}$, as mentioned in Remark 8.4.3, the sets $\mathcal{N}_i$ in Lemma 8.4.2 can be taken in the form $\mathcal{N}_i := \{(\mathbf{x}, \mathbf{0}_k) \in \mathbb{R}^{2k} : \|\mathbf{x}-\mathbf{x}_f\| < \nu_i\}$ for some $\nu_i > 0$ and if `RANDOM_STATE` samples uniformly points of the form $(\mathbf{x}_f, \mathbf{0}_k) \in \mathbb{R}^{2k}$, then 1 in Proposition 8.4.4 holds. Furthermore, `FIND_CLF` can return the explicit expression of the CLF provided in [207, Section V.A]. We note also that Assumption 3 is not restrictive, and Assumption 4 holds by taking the parameter η sufficiently large. •

Remark 8.4.6. (Computational Complexity of `C-CLF-CBF-RRT`): The computational complexity of `C-CLF-CBF-RRT` is the same as `GEOM-RRT` except for the added complexity of the `COMPATIBILITY` function. In general, the optimization problems (8.1), (8.2), and (8.21) required by `COMPATIBILITY` can be non-convex, which makes them not computationally tractable. However, in the setting considered in Proposition 8.2.7, the worst-case complexity of `COMPATIBILITY` is that of solving τ QCQPs, for which efficient heuristics exist [205]. In the setting considered in Proposition 8.2.9, (8.1), (8.2), and (8.21) can be solved in closed form, which means that `C-CLF-CBF-RRT` has the same computational complexity as `GEOM-RRT`. •

Remark 8.4.7. (`C-CLF-CBF-RRT` for Differentially Flat Systems): Here we explain how `C-CLF-CBF-RRT` is applicable to differentially flat systems. Differentially flat systems [214] are control systems for which the states and inputs can be written as algebraic functions of carefully selected *flat outputs* and their derivatives. Many robotic systems of interest, such as the unicycle [215] or the quadrotor [216] are differentially flat. This property facilitates the generation of smooth trajectories. Differentially flat systems are equivalent to dynamic feedback linearizable

systems [217] (i.e., systems that can be feedback linearized after adding an appropriate number of dynamic inputs). This means that differentially flat systems can be transformed into linear systems after an appropriate change of coordinates and control inputs (the same also applies to static feedback linearizable systems, for which no dynamic inputs need to be added). Furthermore, by constructing an outer approximation of the obstacles using polytopes, and expressing it as a union of convex polytopes, the results in Proposition 8.2.7 apply, and the optimization problems (6) and (7) are easier to solve, cf. Section 8.2.2. •

Remark 8.4.8. (Controller Execution): Given a CLF-CBF compatible path $\mathcal{A}$, executing the controller (8.19) has the agent converge from one waypoint to the next asymptotically. However, under the assumptions of Proposition 8.4.4, there exist neighborhoods around the waypoints of $\mathcal{A}$ such that any two points of two consecutive neighborhoods can be connected with a CLF-CBF controller (possibly, with adjusted CLF, and extended class $\mathcal{K}_\infty$ functions, cf. Lemma 8.4.2). Therefore, by executing the controller (8.19) for a sufficiently large but finite time, the agent can visit these different neighborhoods and trace a path whose waypoints are close to those of $\mathcal{A}$. •

Remark 8.4.9. (`C-CLF-CBF-RRT` for Higher-Relative Degree Systems): The algorithm `C-CLF-CBF-RRT` can be adapted to the setting where h is a HOCBF, cf. Section 8.2.4, with the following modifications:

(1) $\mathbf{x}_{\text{init}}$ and $\mathcal{X}_{\text{goal}}$ lie in $\mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$;

(2) `RANDOM_STATE` returns states from $\mathcal{C} \cap \mathcal{C}_2 \cap \cdots \cap \mathcal{C}_{\bar{m}}$ (or a subset of it consisting of stabilizable points);

(3) `COMPATIBILITY` employs the conditions described in Proposition 8.2.11 instead of those in Proposition 8.2.1 to check the compatibility of CLFs and HOCBFs. •

8.5 Simulation and Experimental Validation

Here we illustrate the performance of `C-CLF-CBF-RRT` in simulation and hardware experiments. Throughout the section, we deal with a differential-drive robot following the unicycle dynamics:

$$\dot{x} = v\cos(\theta), \tag{8.24a}$$

$$\dot{y} = v\sin(\theta), \tag{8.24b}$$

$$\dot{\theta} = \omega, \tag{8.24c}$$

where $\mathbf{s} = [x, y] \in \mathbb{R}^2$ is the position of the robot, θ its heading, and v and ω are its linear and angular velocity control inputs, respectively. Following [190, Section IV], we set

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \quad p = \begin{bmatrix} x \\ y \end{bmatrix} + l_0 R(\theta) \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

where $l_0 > 0$ is a design parameter. This defines $\mathbf{p}$ as a point orthogonal to the wheel axis of the robot. Moreover, let

$$L = \begin{bmatrix} 1 & 0 \\ 0 & 1/l_0 \end{bmatrix}.$$

Even though the dynamics (8.24) are nonlinear, it follows that $\dot{\mathbf{p}} = R(\theta)L^{-1}\mathbf{u}$, where $\mathbf{u} = [v, w]^T$. By defining the new control input $\tilde{\mathbf{u}} = R(\theta)L^{-1}u$, the state $\mathbf{p}$ follows single integrator dynamics. The original angular and linear velocity inputs can be easily obtained from $\tilde{\mathbf{u}}$ as $\mathbf{u} = LR(\theta)^{-1}\tilde{\mathbf{u}}$. Since $\mathbf{p}$ can be made arbitrarily close to $[x, y]$ by taking l_0 sufficiently small, in what follows we consider $\mathbf{p}$ as our state variable. Throughout the experiments, we use $\alpha_l(s) = 5s$ for all $l \in [M]$ and $\eta = 2m$. We also use $\tau = 5$ and constants $\sigma = 0.5$, $\bar{\sigma} = 2$ as defined in Section 8.3. The results we present in this section have been obtained without the need to resort to increase the value of σ or $\bar{\sigma}$ at every iteration, or perform other similar heuristics. Once the robot is within $0.5m$ of a given waypoint, we switch the controller so that it steers the robot towards the next waypoint.

8.5.1 Computer Simulations

We have tested `C-CLF-CBF-RRT` in different simulation environments in a high-fidelity Unity simulator on an Ubuntu PC with Intel Core i9-13900K 3 GHz 24-Core processor. We utilize the function `minimize` from the library `SCIPY` [218] to solve the optimization problems in the `COMPATIBILITY` function. The robots used in the simulation are Clearpath Husky[1] robots, which have the same LIDAR and sensor capabilities as the real ones, and these are used to run a SLAM system that allows each robot to localize itself in the environment and obtain its current state, which is needed to implement the controller from (8.19). The first simulation environment consists of a series of red obstacles whose projection on the navigation plane is either a circle or a polytope. The second simulation consists of an environment with different rooms. The different walls are modeled as obstacles using nonsmooth CBFs, given that their projection on the navigation plane are quadrilaterals. To ensure that the whole physical body of the robot remains safe, we add a slack term to the CBF that takes into account the robot dimensions. For example, for a circular obstacle with center at $\mathbf{x}_c \in \mathbb{R}^2$ and radius $r > 0$, and a circular robot with radius $r_0 > 0$, the CBF can be taken as $h(\mathbf{x}) = \|\mathbf{x} - \mathbf{x}_c\|^2 - (r + r_0)^2$. Both simulation environments have dimensions $20m \times 50m$, and in each of them the projection of the obstacles in the navigation plane is either a circle or a polytope, so the `COMPATIBILITY` function runs efficiently (cf. Section 8.2). Figure 8.2 shows the tree generated by `C-CLF-CBF-RRT` in both simulation experiments, as well as the corresponding trajectory executed by the robot using the controller obtained as the solution of (8.19), which successfully reaches the end goal while remaining collision-free.

8.5.2 Hardware Experiments

We have also tested `C-CLF-CBF-RRT` in a physical environment using a Clearpath Jackal robot. The robot is equipped with GPS, IMU and LIDAR sensors, which are used to run a SLAM system to localize its position in the environment and

[1]Spec. sheets for the Husky and Jackal robots can be found at https://clearpathrobotics.com

execute the controller from (8.19). The environment, with dimensions $4m \times 9m$, consists of different obstacles whose projection on the navigation plane is either a circle or a polytope. We ensure the whole physical body of the robot remains safe using a slack term in the CBF formulation, as described in Section 8.5.1. Figure 8.3(a) shows the tree generated by `C-CLF-CBF-RRT` as well as the trajectory executed by the robot, successfully reaching its goal. We use $\alpha_l(s) = 5s$ for all $l \in [M]$ and choose $\eta = 2m$. Once the robot is within $0.5m$ of a given waypoint, we switch the controller so that it steers the robot towards the next waypoint.

8.5.3 Comparison with `GEOM-RRT`

Here we compare the performance of `C-CLF-CBF-RRT` with `GEOM-RRT` in both the simulation and hardware environments. Figure 8.3(b) shows the tree generated by `GEOM-RRT` as well as the trajectory executed by the robot in the hardware environment using the controller obtained from (8.19). One can observe that the trajectory generated by the robot is unable to reach the end goal and stops rather early, at a point where the optimization problem (8.19) becomes infeasible. This occurs because `GEOM-RRT` does not take into account the dynamic feasibility of the path it generates.

We should point out that the steering parameter η critically affects the performance of `GEOM-RRT`. To show this, we run various executions of `GEOM-RRT` in the simulation environment with obstacles depicted in Figure 8.2(a). Table 8.1 shows that smaller values of η yield a higher percentage of feasible paths but with a higher average execution time. For comparison, the average execution time of `C-CLF-CBF-RRT`, whose paths are always dynamically feasible, for the same simulation environment and with $\eta = 4m$, is 8.72 seconds. To match the dynamic feasibility of the produced paths, `GEOM-RRT` has to be run with $\eta = 1m$, at a significantly higher computational cost.

Remark 8.5.1. (Convergence to waypoints): Since the robot asymptotically converges to each waypoint, we observe in the experiments that it tends to slow down when reaching a waypoint and speed up when switching to the next one. Here we describe ways in which this behavior can be alleviated:

η (meters)	Percentage of feasible paths	Average execution time (seconds)
1	100%	154.36
2	90%	140.62
4	50%	130.62
8	30%	4.83
16	5%	1.84

Table 8.1: Comparison of the percentage of feasible paths (i.e., paths for which the controller in (2.14) steers the robot from the initial point to the end goal by following the waypoints generated by the path) and the average execution time of `GEOM-RRT` (over 20 executions). The paths are generated for the simulation environment with obstacles in Figure 8.2(a).

(1) **Modifying the objective function**: The minimum-norm controller in (8.19) naturally seeks the smallest control action, which can lead to the observed *slowing down* effect near waypoints. Alternatively, given a nominal controller $u_{\text{nom}} : \mathbb{R}^n \to \mathbb{R}^m$ with a desired behavior (towards a waypoint or the end goal), one can modify the objective function in (8.19) by $\frac{1}{2}\left\|\mathbf{u} - u_{\text{nom}}(\mathbf{x})\right\|^2$ and implement the resulting controller.

(2) **Finite-time CLFs**: Fixed-time Control Lyapunov Function [219] can be used to design controllers that guarantee convergence to a desired waypoint within a specified time horizon. By extending the notion of compatibility to consider BNCBFs and finite-time CLFs, the optimization problems (8.1) and (8.2) can be reformulated using finite-time CLFs. Then, these optimization problems can be utilized to define a version of `C-CLF-CBF-RRT` that accounts for finite-time CLFs. We leave the study of the properties of such an algorithm for future work.

(3) **CLF convergence rate**: given a closed-loop system satisfying the CLF condition (2.5), the function W dictates the rate of decrease of trajectories to the origin. For example, by taking $W(\mathbf{x}) = \gamma V(\mathbf{x})$, with $\gamma > 0$, trajectories of the closed-loop system converge to the origin at a rate γ. Therefore, by increasing γ, the rate of convergence can be increased. However, it should

be pointed out that an increased rate of convergence might compromise the compatibility of V with a CBF. •

8.5.4 Comparison with `CBF-RRT` and `LQR-CBF-RRT*`

Here we compare `C-CLF-CBF-RRT` with other related algorithms in the literature leveraging CBFs. First, we compare it with `CBF-RRT`, a sampling-based motion planning algorithm proposed in [79] that also employs control barrier functions. Initially, `CBF-RRT` starts with a tree consisting of a single node in $\mathbf{x}_{\text{init}}$. Then, each iteration of `CBF-RRT` operates as follows. First, it randomly samples a vertex $\mathbf{x}_0$ from the current tree. Next, it generates a reference input, e.g., one steering the robot from x_0 to the goal set $\mathcal{X}_{\text{goal}}$ (cf. [79, Section 5] for more details). Finally, for a fixed period of simulated time T_0, at every state it executes the controller closest to the reference input that satisfies the CBF conditions associated to all obstacles. This quadratic optimization program is solved using the convex optimization library `CVXOPT` [202]. The state $\mathbf{x}_{\text{new}}$ reached by the robot after this period of time T_0 gets added to the tree.

To generate the trajectory, we numerically integrate the closed-loop system using the `odeint` method from the Python library `SCIPY` [218] and use a time discretization step of 0.005 seconds. We have ran multiple times `C-CLF-CBF-RRT` and `CBF-RRT` in the simulation environment with obstacles of Figure 8.2(a). Note that `CBF-RRT` is more computationally costly, as it requires running a trajectory for every new node added to the tree. Furthermore, this trajectory is generated by a controller that is obtained as the solution of an optimization problem at every point. In contrast, `C-CLF-CBF-RRT` only requires solving a single optimization problem (and, in the cases discussed in Section 8.2.3, not even that, since an algebraic check is enough) for every new node added to the tree. For example, if T_0 is small (e.g., $T_0 = 5$), the average execution time of `CBF-RRT` exceeds one minute. For $T_0 = 15$, the average execution time of `CBF-RRT` (over 10 different runs) is 384.58 seconds. The average execution time is similar for $T_0 = 10$, $T_0 = 20$. These numbers seem to indicate that smaller values of T_0 find a feasible path more rapidly, but such paths contain a larger number of waypoints. In contrast, larger values

of T_0 lead to paths with a smaller number of waypoints but require more time to be found. In comparison, the average execution time of `C-CLF-CBF-RRT` with the same initial point and end goal (and with $\alpha_l(s) = 5s$ for all $l \in [M]$ and $\eta = 4m$) is 8.72 seconds, almost two orders of magnitude faster. We should also point out that there exists a trade-off between the computational complexity of CBF-RRT and the underlying safety guarantees. Indeed, since the CBF-QP controller cannot be solved continuously, CBF-RRT [79] solves the CBF-QP optimization problem periodically along the generated trajectory with sampling time T_0. As a consequence, in-between the times when the CBF-QP is solved, safety violations may occur. One way to remedy this is to solve the CBF-QP at a higher frequency. However, this increases the computational complexity of CBF-RRT, since the overall number of optimization problems to be solved is higher.

Finally, we compare `C-CLF-CBF-RRT` with `LQR-CBF-RRT*`. This is a sampling-based algorithm proposed in [81] which generates reference trajectories using LQR-based controllers of linearized dynamics around a new added node to the RRT, and checks the CBF condition at a finite set of points along this reference trajectory. The resolution with which such CBF condition is checked affects the safety of the overall trajectory (theoretically, it is safe only if every point satisfies the CBF condition). Table 8.2 compares different resolutions with which the CBF condition checks are made, along with the corresponding average execution times (over 20 runs) and safety violations (which, to have a fair comparison with `C-CLF-CBF-RRT`, has been implemented without the adaptive sampling procedure described in [81, Section V.C]). Smaller resolutions naturally lead to larger execution times and a smaller percentage of safety violations. We note that a resolution of $0.01m$ leads to no safety violations and only has a slightly higher execution time compared to `C-CLF-CBF-RRT`. However, this lack of safety violations is not theoretically guaranteed in general and it is not known a priori what resolution results in no safety violations.

Resolution (m)	Average execution time (s)	Safety violations
0.5	0.26	60 %
0.1	1.09	40 %
0.05	1.7	5 %
0.01	11.31	0 %

Table 8.2: Comparison of the resolution with which the CBF checks are made in `LQR-CBR-RRT*` and the corresponding average execution time (over 20 executions). The paths are generated for the simulation environment with obstacles in Figure 2(a).

8.6 Appendix

The following result shows that the problem of checking whether the optimization problem (8.20) is feasible can be simplified by only checking the pairwise feasibility of the CLF constraint and the CBF constraints associated with the obstacles that intersect with Θ (as defined in Section 8.3.3).

Lemma 8.6.1. (Checking pairwise compatibility of a reduced set of CBFs): *Let* $\mathbf{x}_{near} \in \mathbb{R}^n$, $\mathbf{x}_{new} \in \mathbb{R}^n$, *and* $V : \mathbb{R}^n \to \mathbb{R}$ *be a CLF with respect to* $\mathbf{x}_{new}$. *Define* $\Theta = \{\mathbf{x} \in \mathbb{R}^n : V(\mathbf{x}) \leq V(\mathbf{x}_{near})\}$. *Let* $\mathcal{L} := \{l \in [M] : \Theta \cap Cl(\mathcal{O}_l) = \varnothing\}$. *Suppose that there exists a set of extended class* $\mathcal{K}_\infty$ *functions* $\{\alpha_l\}_{l\in\mathcal{L}}$ *such that for each* $l \in \mathcal{L}$, *the problem*

$$\begin{aligned} \min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\|\mathbf{u}\|^2 \\ s.t.\ L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})\mathbf{u} \geq -\alpha_l(h_{j,l}(\mathbf{x})),\ j \in \mathcal{I}_l(\mathbf{x}), \\ L_f V(\mathbf{x}) + L_g V(\mathbf{x})\mathbf{u} + W(\mathbf{x}) \leq 0, \end{aligned} \tag{8.25}$$

is feasible for all $\mathbf{x} \in \Theta \cap \mathscr{F}$ *and there exists a set of disjoint open sets* $\{\mathcal{Y}_l\}_{l\in\mathcal{L}}$ *(with* $\mathcal{Y}_l$ *being a neighborhood of* $\partial\mathcal{O}_l$ *satisfying* $\mathcal{Y}_l \cap \mathcal{O}_{l'} = \varnothing$ *for all* $l' \neq l$*) and a bounded controller* $\hat{u}$ *satisfying the constraints in* (8.25) *for each* $\mathbf{x} \in \mathcal{Y}_l \cap \Theta \cap \mathscr{F}$ *and* $l \in \mathcal{L}$. *Then, there exists a set of extended class* $\mathcal{K}_\infty$ *functions* $\{\bar{\alpha}_l\}_{l\in[M]}$ *such that*

$$\begin{aligned} \min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\|\mathbf{u}\|^2 \\ s.t.\ L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x})\mathbf{u} \geq -\bar{\alpha}_l(h_{j,l}(\mathbf{x})),\ \forall j \in \mathcal{I}_l(\mathbf{x}), l \in \mathcal{L}, \\ L_f V(\mathbf{x}) + L_g V(\mathbf{x})\mathbf{u} + W(\mathbf{x}) \leq 0. \end{aligned} \tag{8.26}$$

is feasible for all $\mathbf{x} \in \Theta \cap \mathscr{F}$.

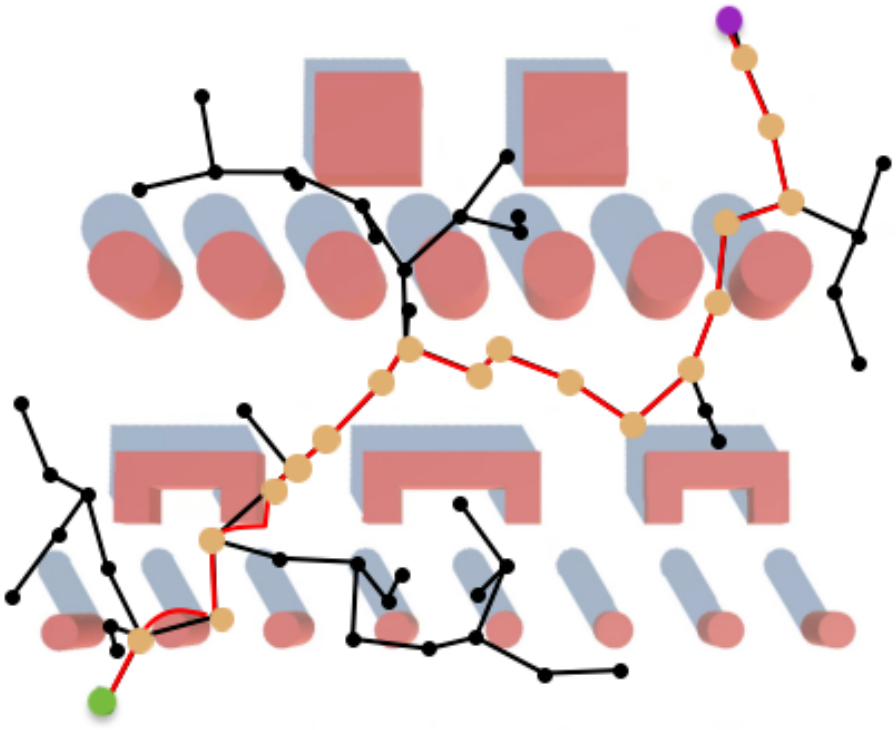
Proof. Let $l \in \mathcal{L}$. Note that since $\mathcal{Y}_l \cap \mathcal{O}_{l'} = \varnothing$ for all $l' \in [M]\backslash\{l\}$, there exists $d_l > 0$ such that $h_{l'}(\mathbf{x}) \geq d_l$ for all $l' \in [M]\backslash\{l\}$ and $\mathbf{x} \in \mathcal{Y}_l \cap \Theta \cap \mathscr{F}$. Now, take $\hat{\alpha}_l > 0$ such that

$$\hat{\alpha}_l > \frac{\sup_{\mathbf{x} \in \mathcal{Y}_l \cap \Theta \cap \mathscr{F}} |L_f h_{j,l'}(\mathbf{x}) + L_g h_{j,l'}(\mathbf{x}) \hat{u}(\mathbf{x})|}{d_l}$$

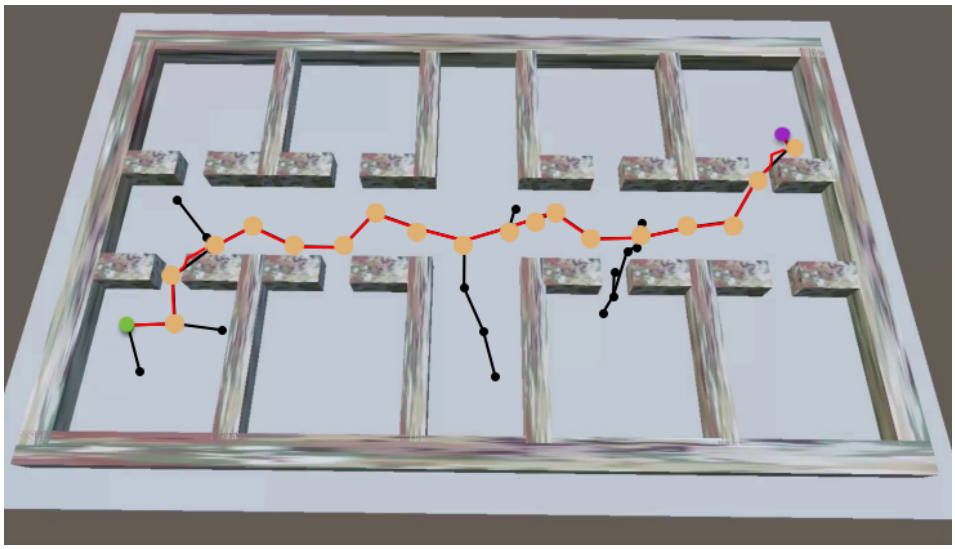
for all $l' \in [M]\backslash\{l\}$ and $j \in \mathcal{I}_{l'}(\mathbf{x})$. Note that such $\hat{\alpha}_l$ exists because $\hat{u}$ is bounded and Θ is compact. Further let $\hat{\alpha} > \hat{\alpha}_l$ for all $l \in \mathcal{L}$, and take $\bar{\alpha}_l$ so that $\bar{\alpha}_l(s) > \max\{\alpha_l(s), \hat{\alpha} s\}$ for all $s \geq 0$. Now, $\hat{u}(\mathbf{x})$ is feasible for (8.26) for any $\mathbf{x} \in \left(\bigcup_{l \in \mathcal{L}} \mathcal{Y}_l\right) \cap \Theta \cap \mathscr{F}$. On the other hand, there exists $d_{-1} > 0$ such that $h_l(\mathbf{x}) > d_{-1}$ for all $l \in [M]$ and $\mathbf{x} \in \Theta \cap \mathscr{F} \backslash \left(\bigcup_{l \in \mathcal{L}} \mathcal{Y}_l\right)$. Now, take $\hat{\alpha}_{-1} > 0$ such that

$$\hat{\alpha}_{-1} > \frac{\sup_{\mathbf{x} \in \Theta \cap \mathscr{F} \backslash (\bigcup_{l \in \mathcal{L}} \mathcal{Y}_l)} |L_f h_{j,l}(\mathbf{x}) + L_g h_{j,l}(\mathbf{x}) \hat{u}(\mathbf{x})|}{d_{-1}},$$

for all $l \in [M]$ and $j \in \mathcal{I}_l(x)$. Again, such $\hat{\alpha}_{-1}$ exists because $\hat{u}$ is bounded and Θ is compact. Further let $\hat{\alpha}_* > \max\{\hat{\alpha}, \hat{\alpha}_{-1}\}$ and take $\bar{\alpha}_l$ so that $\bar{\alpha}_l(s) > \max\{\alpha_l(s), \hat{\alpha}_* s\}$ for all $s \geq 0$. Hence, $\hat{u}(\mathbf{x})$ is feasible for (8.26) for any $\mathbf{x} \in \Theta \cap \mathscr{F}$. □

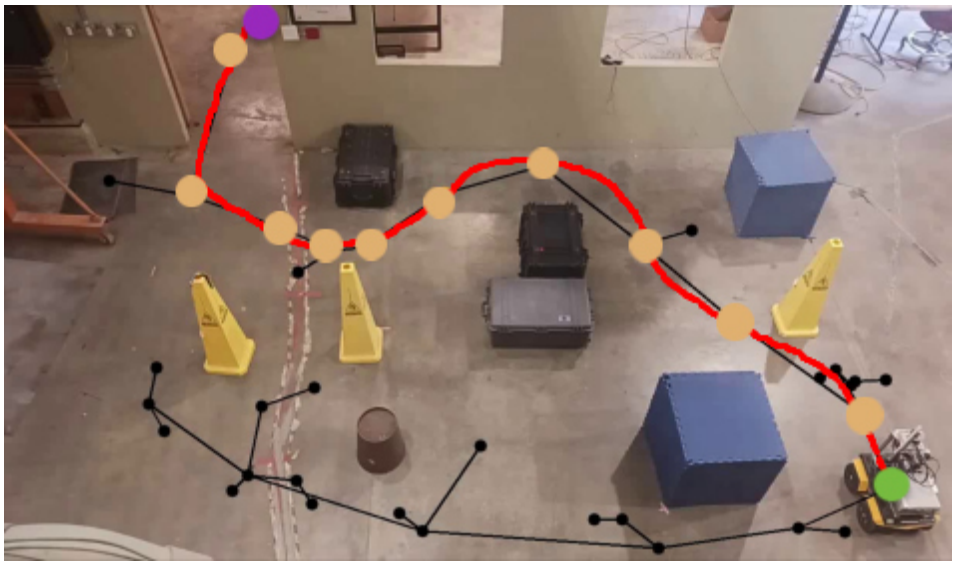


(a) Environment with obstacles

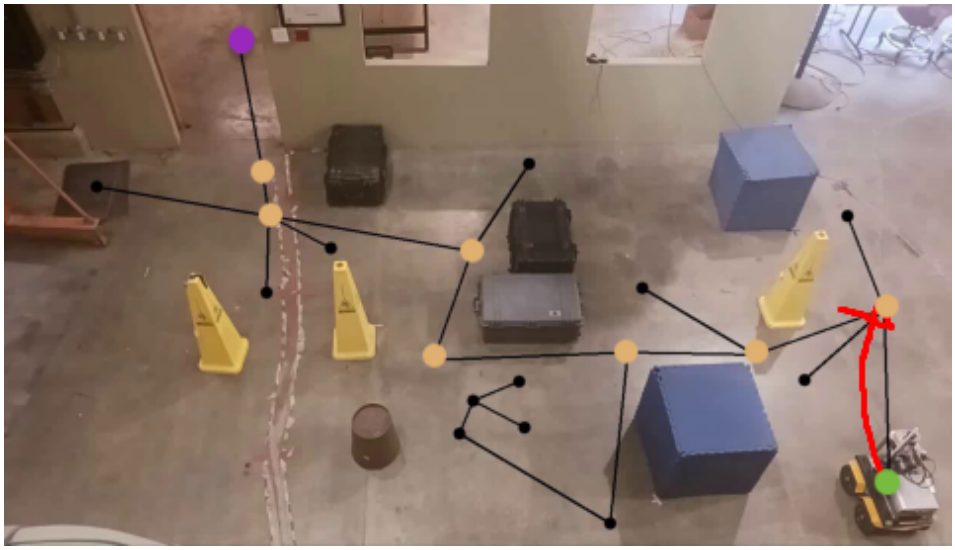


(b) Environment with rooms

Figure 8.2: (a) First and (b) second simulation environment experiments. Tree generated by `C-CLF-CBF-RRT` (black), waypoints of the returned path (dark yellow) and trajectory followed by the robot using the controller from (8.19) (red). The starting point is the green dot and the end goal is the purple dot. In each environment, the robot successfully visits the waypoints while avoiding collisions with obstacles.



(a) C-CLF-CBF-RRT



(b) GEOM-RRT

Figure 8.3: Execution of (a) C-CLF-CBF-RRT and (b) GEOM-RRT in the hardware experiment. In both plots, tree generated by the corresponding algorithm (black), waypoints of the returned path (dark yellow), and trajectory followed by the robot (red) using the controller from (8.19) (red). The starting point is the green dot and the end goal is the purple dot. The trajectory executed by the robot under C-CLF-CBF-RRT reaches its goal safely, whereas it fails under GEOM-RRT because it quickly encounters a point where the optimization problem (8.19) is infeasible.

Part III

Learning in Safety-Critical Systems under Uncertainty

Chapter 9

Feasibility and Regularity Analysis of Safe Stabilizing Controllers under Uncertainty

In this chapter we study the problem of safe stabilization of control-affine systems under uncertainty. Our starting point is the availability of worst-case or probabilistic error descriptions for the dynamics, along with a CBF and a CLF. These descriptions give rise to second-order cone constraints (SOCCs) whose simultaneous satisfaction guarantees safe stabilization. We study the feasibility of such SOCCs and the regularity properties of various controllers satisfying them.

9.1 Problem Statement

We consider a control-affine system of the form (3.1), as well as a CBF h of a safe set $\mathcal{C}$ (with $\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x}) \neq 0$ for all $x \in \partial\mathcal{C}$), and a CLF V. We are interested in the design of controllers that ensure stability and safety in the presence of uncertainty. We assume that the maps f, g in (3.1) and the CBF h and its gradient ∇h are unknown. We also assume that a CLF V for the true system is unknown. Instead, estimates of f, g, h, ∇h, V, and ∇V (denoted $\hat{f}$, $\hat{g}$, $\hat{h}$, $\widehat{\nabla h}$, $\hat{V}$, and $\widehat{\nabla V}$ resp.) are available. Even if these estimates are available, note that since the true values of f, g, and h are unknown, a safe controller is not easily computable through [23,

Theorem 2].

Remark 9.1.1. (Lyapunov function search under uncertainty): We assume that f, g and h are only approximately known because, in practice, the dynamic model and safety constraints are often obtained using noisy sensor data and simplified models, which leads to estimation errors. The construction of CLFs for these approximations in turn leads to approximations of the CLF for the true system. However, there are techniques to find CLFs for uncertain systems including sum-of-squares [220], which is limited to polynomial systems but provides known error bounds, [221], which describes a method that only requires knowledge of the degree of actuation, and [222], which uses ideas from distributionally robust optimization. All these works seek to find a CLF that is valid for all systems compatible with the given uncertainty. In our treatment, we only require $\hat{V}$ and $\widehat{\nabla V}$ to be within some error bounds of a true CLF and its gradient, respectively, but if a true CLF is known (by using for instance the techniques in the given references), these error bounds can be taken as identically zero. •

We consider two types of models for the errors between the estimates and the true quantities. First, for $\mathbf{x} \in \mathbb{R}^n$, consider worst-case error bounds as follows:

$$\begin{aligned}
\left\| f(\mathbf{x}) - \hat{f}(\mathbf{x}) \right\| \leq e_f(\mathbf{x}),\ \left\| g(\mathbf{x}) - \hat{g}(\mathbf{x}) \right\| \leq e_g(\mathbf{x}), \\
\left| h(\mathbf{x}) - \hat{h}(\mathbf{x}) \right| \leq e_h(\mathbf{x}),\ \left\| \nabla h(\mathbf{x}) - \widehat{\nabla h}(\mathbf{x}) \right\| \leq e_{\nabla h}(\mathbf{x}), \\
\left| V(\mathbf{x}) - \hat{V}(\mathbf{x}) \right| \leq e_V(\mathbf{x}),\ \left\| \nabla V(\mathbf{x}) - \widehat{\nabla V}(\mathbf{x}) \right\| \leq e_{\nabla V}(\mathbf{x}).
\end{aligned}$$

Since the exact dynamics, the CBF and CLF are unknown, one can not certify the inequalities (2.5) and (2.7) directly. Instead, using the error bounds above, define

$$\begin{aligned}
a_V(\mathbf{x}) &= e_{\nabla V}(\mathbf{x}) e_g(\mathbf{x}) + e_{\nabla V}(\mathbf{x}) \left\| \hat{g}(\mathbf{x}) \right\| + \left\| \widehat{\nabla V}(\mathbf{x}) \right\| e_g(\mathbf{x}), \\
b_V(\mathbf{x}) &= -\widehat{\nabla V}(\mathbf{x})^\top \hat{g}(\mathbf{x}), \\
c_V(\mathbf{x}) &= -e_{\nabla V}(\mathbf{x}) e_f(\mathbf{x}) - e_{\nabla V}(\mathbf{x}) \left\| \hat{f}(\mathbf{x}) \right\| - \left\| \widehat{\nabla V}(\mathbf{x}) \right\| e_f(\mathbf{x}) - \widehat{\nabla V}(\mathbf{x})^\top \hat{f}(\mathbf{x}) - W(\mathbf{x}), \\
a_h(\mathbf{x}) &= e_{\nabla h}(\mathbf{x}) e_g(\mathbf{x}) + e_{\nabla h}(\mathbf{x}) \left\| \hat{g}(\mathbf{x}) \right\| + \left\| \widehat{\nabla h}(\mathbf{x}) \right\| e_g(\mathbf{x}), \\
b_h(\mathbf{x}) &= \widehat{\nabla h}(\mathbf{x})^\top \hat{g}(\mathbf{x}), \\
c_h(\mathbf{x}) &= -e_{\nabla h}(\mathbf{x}) e_f(\mathbf{x}) - e_{\nabla h}(\mathbf{x}) \left\| \hat{f}(\mathbf{x}) \right\| - \left\| \widehat{\nabla h}(\mathbf{x}) \right\| e_f(\mathbf{x}) + \widehat{\nabla h}(\mathbf{x})^\top \hat{f}(\mathbf{x}) + \\
&\quad \alpha(\hat{h}(\mathbf{x}) - e_h(\mathbf{x})).
\end{aligned}$$

According to [41, Proposition V.I], if the two (state-dependent) SOCCs (in $\mathbf{u}$):

$$a_V(\mathbf{x})\,\|\mathbf{u}\| \le b_V(\mathbf{x})\mathbf{u} + c_V(\mathbf{x}), \tag{9.1a}$$

$$a_h(\mathbf{x})\,\|\mathbf{u}\| \le b_h(\mathbf{x})\mathbf{u} + c_h(\mathbf{x}), \tag{9.1b}$$

are satisfied for all $\mathbf{x} \in \mathcal{C}$, then (2.5) and (2.7) hold for all $\mathbf{x} \in \mathcal{C}$. This result provides a way of designing controllers that simultaneously satisfy (2.5) and (2.7).

Second, suppose that GP estimates are available for the following quantities [38]:

$$\Delta_V(\mathbf{x},\mathbf{u}) = L_f V(\mathbf{x}) + L_g V(\mathbf{x})\mathbf{u} - \widehat{\nabla V}(\mathbf{x})^\top(\hat{f}(\mathbf{x}) + \hat{g}(\mathbf{x})\mathbf{u}),$$
$$\Delta_h(\mathbf{x},\mathbf{u}) = L_f h(\mathbf{x}) + L_g h(\mathbf{x})\mathbf{u} + \alpha(h(\mathbf{x})) - \widehat{\nabla h}(\mathbf{x})^\top \hat{f}(\mathbf{x}) - \widehat{\nabla h}(\mathbf{x})^T \hat{g}(\mathbf{x})\mathbf{u} - \alpha(\hat{h}(\mathbf{x})).$$

We further assume that if $\mathcal{H}$ is the Reproducing Kernel Hilbert Space (RKHS, [223, Section 2.1]) with respect to which the GP estimates of Δ_V and Δ_h have been derived, then Δ_V and Δ_h have bounded RKHS norm with respect to $\mathcal{H}$. Let $\mu_V(\mathbf{x},\mathbf{u})$ and $s_V^2(\mathbf{x},\mathbf{u})$ denote the mean and variance, resp., of the GP prediction of Δ_V, which we assume affine and quadratic in $\mathbf{u}$, resp. Therefore, there exist $\gamma_V(\mathbf{x}) : \mathbb{R}^n \to \mathbb{R}^{m+1}$ and $G_V(\mathbf{x}) \in \mathbb{R}^{(m+1)\times(m+1)}$ such that

$$\mu_V(\mathbf{x},\mathbf{u}) = \gamma_V(\mathbf{x})^\top \begin{bmatrix} 1 \\ \mathbf{u} \end{bmatrix}, \quad s_V(\mathbf{x},\mathbf{u}) = \left\| G_V(\mathbf{x}) \begin{bmatrix} 1 \\ \mathbf{u} \end{bmatrix} \right\|_2.$$

For the GP prediction of Δ_h, let $\gamma_h(\mathbf{x})$, and $G_h(\mathbf{x})$ be defined analogously. Since the exact dynamics, the CBF and CLF are unknown, one cannot certify the inequalities (2.5) and (2.7). However, for $\delta \in (0,1)$, and using the GP predictions, define

$$\begin{aligned}
Q_V(\mathbf{x}) &= \beta(\delta) G_{V,2:(m+1)}(\mathbf{x}) \in \mathbb{R}^{(m+1)\times m}, \\
r_V(\mathbf{x}) &= \beta(\delta) G_{V,1}(\mathbf{x}) \in \mathbb{R}^{(m+1)\times 1}, \\
b_V(\mathbf{x}) &= -\widehat{\nabla V}(\mathbf{x})^\top \hat{g}(\mathbf{x}) - \gamma_{V,2:(m+1)}^\top(\mathbf{x}) \in \mathbb{R}^{1\times m}, \\
c_V(\mathbf{x}) &= -\widehat{\nabla V}(\mathbf{x})^\top \hat{f}(\mathbf{x}) - W(\mathbf{x}) - \gamma_{V,1}(\mathbf{x}) \in \mathbb{R},
\end{aligned}$$

and similarly Q_h, r_h, b_h and c_h (the exact form of $\beta(\delta)$ is given in [39, Theorem 2]).

Then, according to [38, Section IV], if the two SOCCs

$$\|Q_V(\mathbf{x})\mathbf{u} + r_V(\mathbf{x})\| \leq b_V(\mathbf{x})\mathbf{u} + c_V(\mathbf{x}), \tag{9.2a}$$

$$\|Q_h(\mathbf{x})\mathbf{u} + r_h(\mathbf{x})\| \leq b_h(\mathbf{x})\mathbf{u} + c_h(\mathbf{x}), \tag{9.2b}$$

are satisfied for all $\mathbf{x} \in \mathcal{C}$, then (2.5) and (2.7) each hold for all $\mathbf{x} \in \mathcal{C}$ with probability at least $1 - \delta$.

Remark 9.1.2. (General form of SOCCs): By taking

$$Q_V(\mathbf{x}) = a_V(\mathbf{x}) \begin{pmatrix} \mathbf{I}_m \\ \mathbf{0}_m^\top \end{pmatrix}, \; r_V(\mathbf{x}) = \mathbf{0}_{m+1}$$

in (9.2a), we obtain (9.1a). Hence, in the following, we derive the results for SOCCs of the most general form (9.2). •

In the rest of the chapter, we suppose that either worst-case or probabilistic descriptions of the dynamics, the CBF and the CLF are available. Given this setup, our goals are to (i) derive conditions that ensure the feasibility of the pair of robust stability (9.1a) and safety-(9.1b) (resp., probabilistic stability (9.2a) and safety (9.2b)) inequalities and, building on this, (ii) design controllers that jointly satisfy the inequalities pointwise in $\mathcal{C}$ and characterize their regularity properties. The latter is motivated by both theoretical (guarantee the existence and uniqueness of solutions to the closed-loop system) and practical (ease of implementation of feedback control on digital platforms and avoidance of chattering behavior) considerations.

9.2 Compatibility of Pairs of Second-Order Cone Constraints

In this section, we derive sufficient conditions that guarantee the feasibility of the pairs of inequalities in (9.1) and in (9.2), resp. The next definition extends the notion of compatibility between a CLF and a CBF (cf. Definition 2.5.7) to any set of inequalities.

Definition 9.2.1. (Compatibility of a set of inequalities): *Given functions* $q_i : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ *for* $i \in [p]$*, the inequalities* $q_i(\mathbf{x}, \mathbf{u}) \leq 0$*,* $i \in [p]$ *are (strictly) compatible at a point* $\mathbf{x} \in \mathbb{R}^n$ *if there exists a corresponding* $\mathbf{u} \in \mathbb{R}^m$ *satisfying all inequalities (strictly). The same inequalities are (strictly) compatible on a set* $\mathcal{G}$ *if they are (strictly) compatible at every* $\mathbf{x} \in \mathcal{G}$*.*

As the estimation errors (resp. the variances) approach zero, the inequalities in (9.1) (resp. (9.2)) approach (2.5) and (2.7). If (2.15) and (2.16) are compatible, the next result provides explicit bounds for the estimation errors such that (9.1a)-(9.1b) and (9.2a)-(9.2b) are strictly compatible.

Proposition 9.2.2. (Sufficient condition for compatibility given upper bound on the norm of a safe stabilizing controller): *Let* h *be an* η*-robust CBF. Let* $\tilde{\mathcal{C}}$ *be a set containing* $\mathcal{C}$ *such that* (2.15) *and* (2.16) *are compatible on* $\tilde{\mathcal{C}}$*. Let* $B : \mathbb{R}^n \to \mathbb{R}$ *be an upper bound on the norm of a control satisfying both inequalities. Suppose* α *in* (2.16) *is Lipschitz with constant* K_α*. Let* $\mathbf{x} \in \mathcal{C}$*.*

(1) If

$$\begin{aligned} &\left\|\widehat{\nabla V}(\mathbf{x})\right\| (e_f(\mathbf{x}) + e_g(\mathbf{x})B(\mathbf{x})) + e_{\nabla V}(\mathbf{x})\Big(\left\|\hat{f}(\mathbf{x})\right\| + \\ &e_f(\mathbf{x}) + (\|\hat{g}(\mathbf{x})\| + e_g(\mathbf{x}))B(\mathbf{x})\Big) < \frac{1}{2}S(\mathbf{x}), \end{aligned} \tag{9.3a}$$

$$\begin{aligned} &(e_{\nabla h}(\mathbf{x}) + \left\|\widehat{\nabla h}(\mathbf{x})\right\|)(e_f(\mathbf{x}) + e_g(\mathbf{x})B(\mathbf{x})) + K_\alpha e_h(\mathbf{x}) \\ &+ e_{\nabla h}(\mathbf{x})(\left\|\hat{f}(\mathbf{x})\right\| + \|\hat{g}(\mathbf{x})\| B(\mathbf{x})) < \frac{1}{2}(\eta + \zeta(h(\mathbf{x}))), \end{aligned} \tag{9.3b}$$

then (9.1a) *and* (9.1b) *are strictly compatible in a neighborhood of* $\mathbf{x}$*;*

(2) If

$$\sigma_{\max}(G_V(\mathbf{x})) < \frac{S(\mathbf{x})}{2\beta(\delta)\sqrt{1 + B^2(\mathbf{x})}}, \tag{9.4a}$$

$$\sigma_{\max}(G_h(\mathbf{x})) < \frac{\eta + \zeta(h(\mathbf{x}))}{2\beta(\delta)\sqrt{1 + B^2(\mathbf{x})}}, \tag{9.4b}$$

then (9.2a) *and* (9.2b) *are strictly compatible in a neighborhood of* $\mathbf{x}$ *with probability at least* $1 - 2\delta$*.*

Proof. 1) Since the inequalities (9.3) are strict, there exists a neighborhood $\mathcal{W}_{\mathbf{x}}$ of $\mathbf{x}$ such that (9.3) holds for all points in $\mathcal{W}_{\mathbf{x}}$. The proof follows by applying the definition of $e_f, e_g, e_h, e_{\nabla h}$, $e_{\nabla V}$ given in Section 9.1.

2) First note that since the inequalities in (9.4) are satisfied at $\mathbf{x}$, there exists a neighborhood $\mathcal{W}_{\mathbf{x}}$ of $\mathbf{x}$ such that (9.4) hold for all points in $\mathcal{W}_{\mathbf{x}}$. Note that (9.2a) can be equivalently written as

$$\beta(\delta)\left\|G_V(\mathbf{x})\begin{bmatrix}1\\ \mathbf{u}\end{bmatrix}\right\|_2 \leq -\widehat{\nabla V}(\mathbf{x})^\top \hat{f}(\mathbf{x}) - \gamma_{V,1}(\mathbf{x}) - W(\mathbf{x}) - (\widehat{\nabla V}(\mathbf{x})^\top \hat{g}(\mathbf{x}) + \gamma_{V,2:(m+1)}^T(\mathbf{x}))\mathbf{u},$$

and similarly for (9.2b). Now, note that $-\widehat{\nabla V}(\mathbf{x})^\top(\hat{f}(\mathbf{x}) + \hat{g}(\mathbf{x})\mathbf{u}) - \gamma_{V,1}(\mathbf{x}) - \gamma_{V,2:(m+1)}^\top(\mathbf{x})\mathbf{u} = -L_fV(\mathbf{x}) - L_gV(\mathbf{x})\mathbf{u} + \Delta_V(\mathbf{x},\mathbf{u}) - \gamma_{V,1}(\mathbf{x}) - \gamma_{V,2:(m+1)}^T(\mathbf{x})\mathbf{u}$, and similarly for the safety constraint. Define then the events

$$\mathcal{E}_V = \{|\gamma_V(\mathbf{y})^\top\begin{bmatrix}1\\ \mathbf{u}\end{bmatrix} - \Delta_V(\mathbf{y},\mathbf{u})| \leq \beta s_V(\mathbf{y},\mathbf{u}),\ \forall \mathbf{y}\in\mathcal{W}_{\mathbf{x}}, \mathbf{u}\in\mathbb{R}^m\},$$

$$\mathcal{E}_h = \{|\gamma_h(\mathbf{y})^\top\begin{bmatrix}1\\ \mathbf{u}\end{bmatrix} - \Delta_h(\mathbf{y},\mathbf{u})| \leq \beta(\delta) s_h(\mathbf{y},\mathbf{u}),\ \forall\ \mathbf{y}\in\mathcal{W}_{\mathbf{x}}, \mathbf{u}\in\mathbb{R}^m\}.$$

By [223, Theorem 6], $\mathbb{P}(\mathcal{E}_V)\geq 1-\delta$ and $\mathbb{P}(\mathcal{E}_h)\geq 1-\delta$. Therefore, $\mathbb{P}(\mathcal{E}_V\cap\mathcal{E}_h) = \mathbb{P}(\mathcal{E}_V)+\mathbb{P}(\mathcal{E}_h)-\mathbb{P}(\mathcal{E}_V\cup\mathcal{E}_h)\geq 1-2\delta$. Hence, if for all $\mathbf{y}\in\mathcal{W}_{\mathbf{x}}$ we can find $\mathbf{u}\in\mathbb{R}^m$ satisfying

$$L_fh(\mathbf{y}) + L_gh(\mathbf{y})\mathbf{u} + \alpha(h(\mathbf{y})) \geq 2\beta(\delta)s_h(\mathbf{y},\mathbf{u}), \tag{9.5a}$$

$$-L_fV(\mathbf{y}) - L_gV(\mathbf{y})\mathbf{u} - W(\mathbf{y}) \geq 2\beta(\delta)s_V(\mathbf{y},\mathbf{u}), \tag{9.5b}$$

then (9.2a), (9.2b) are compatible at $\mathcal{W}_{\mathbf{x}}$ with probability at least $1-2\delta$. Let $u^*(\mathbf{x})$ be a control satisfying (2.15)-(2.16) with $\|u^*(\mathbf{x})\|\leq B(\mathbf{x})$. Let us show that $u^*(\mathbf{y})$ satisfies (9.5) for all $\mathbf{y}\in\mathcal{W}_{\mathbf{x}}$. By using the characterization of the matrix norm induced by the Euclidean norm in [115, Example 5.6.6], we get $\left\|G_V(\mathbf{y})\begin{bmatrix}1\\ u^*(\mathbf{y})\end{bmatrix}\right\|_2 \leq \sigma_{\max}(G_V(\mathbf{y}))\sqrt{1+B^2(\mathbf{y})}$ and similarly for the safety constraint. Using now (9.4), we deduce that $u^*(\mathbf{y})$ satisfies (9.5) for all $\mathbf{y}\in\mathcal{W}_{\mathbf{x}}$. □

Remark 9.2.3. (Tightness of conditions for SOCC compatibility): The assumption that h is an η-robust CBF makes it possible for (9.3b) and (9.4b) to be satisfied at $\partial\mathcal{C}$. If the estimation errors (resp. the variances s_V^2, s_h^2) are zero, then (9.3) (resp. (9.4)) is trivially satisfied. Larger values of $S(\mathbf{x})$ and $\zeta(h(\mathbf{x}))$, and smaller values of $B(\mathbf{x})$, lead to conditions that are easier to satisfy. Closer to the origin, $S(\mathbf{x})$ becomes smaller, thus making (9.3a) and (9.4a) harder to satisfy. In fact, (9.3a) and (9.4a) can only be satisfied near the origin if knowledge of ∇V is exact near it, cf. Remark 9.1.1. If $\zeta(h(\mathbf{x}))$ is unknown, a known lower bound for it (e.g., 0) can be used at the expense of more conservativeness. •

Remark 9.2.4. (Computation of upper bound of safe stabilizing controller): One can obtain B in Proposition 9.2.2 by relying on the expression for a safe stabilizing controller provided in [4], together with upper and lower bounds on the norms of f, g, h, ∇h, V, and ∇V. •

We next provide a sufficient condition for the compatibility of (9.2) which does not require knowledge of an upper bound on the norm of a safe stabilizing controller. To do so, we first introduce some useful notation. Given (9.2), define $\hat{A} : \mathbb{R} \to \mathbb{R}^{m\times m}$, $\hat{B} : \mathbb{R} \to \mathbb{R}^m$ by (note we have dropped the state-dependency in $\mathbf{x}$ for brevity)

$$\begin{aligned}\hat{A}(\lambda) &:= 2(Q_V^T Q_V - b_V^T b_V) + 2\lambda(Q_h^T Q_h - b_h^T b_h),\\ \hat{B}(\lambda) &:= 2(Q_V^T r_V - b_V^T c_V) + 2\lambda(Q_h^T r_h - b_h^T c_h),\end{aligned}$$

and the set $\mathcal{F}_0 := \{\lambda \in \mathbb{R} : \det(\hat{A}(\lambda)) \neq 0\}$. Let $A : \mathcal{F}_0 \to \mathbb{R}^{m\times m}$ and $d, \alpha_h, \alpha_V : \mathcal{F}_0 \to \mathbb{R}$ be given by

$$\begin{aligned}A(\lambda) &:= \hat{A}(\lambda)^{-1},\\ d(\lambda) &:= b_h A(\lambda) b_h^T b_V A(\lambda) b_V^T - (b_h A(\lambda) b_V^T)^2,\\ \alpha_h(\lambda) &:= b_h A(\lambda)\hat{B}(\lambda) - c_h,\\ \alpha_V(\lambda) &:= b_V A(\lambda)\hat{B}(\lambda) - c_V.\end{aligned}$$

Further let

$$\mathcal{F}_1 := \{\lambda \in \mathbb{R} : \det(\hat{A}(\lambda)) \neq 0,\ d(\lambda) \neq 0\},$$
$$\mathcal{F}_2 := \{\lambda \in \mathbb{R} : \det(\hat{A}(\lambda)) \neq 0,\ b_V A(\lambda) b_V^\top \neq 0\},$$
$$\mathcal{F}_3 := \{\lambda \in \mathbb{R} : \det(\hat{A}(\lambda)) \neq 0,\ b_h A(\lambda) b_h^\top \neq 0\},$$

and define $\lambda_{2,0} : \mathbb{R} \to \mathbb{R}$, $\{\lambda_{2,i} : \mathcal{F}_i \to \mathbb{R}\}_{i=1}^3$, $\lambda_{3,0} : \mathbb{R} \to \mathbb{R}$, $\{\lambda_{3,i} : \mathcal{F}_i \to \mathbb{R}\}_{i=1}^3$, and $u_i^* : \mathcal{F}_i \to \mathbb{R}^m$ for $i \in \{0,1,2,3\}$ as follows:

$$\lambda_{2,i}(\lambda) := \begin{cases} 0 & \text{if } i = 0, \\ \frac{1}{d(\lambda)} b_V A(\lambda)(b_V^T \alpha_h(\lambda) - b_h^\top \alpha_V(\lambda)) & \text{if } i = 1, \\ 0 & \text{if } i = 2, \\ \frac{\alpha_h(\lambda)}{b_h A(\lambda) b_h^\top} & \text{if } i = 3, \end{cases}$$

$$\lambda_{3,i}(\lambda) := \begin{cases} 0 & \text{if } i = 0, \\ \frac{1}{d(\lambda)}(-b_V \alpha_h(\lambda) + b_h \alpha_V(\lambda)) A(\lambda) b_h^\top & \text{if } i = 1, \\ \frac{\alpha_V(\lambda)}{b_V A(\lambda) b_V^\top} & \text{if } i = 2, \\ 0 & \text{if } i = 3, \end{cases}$$

$$u_i^*(\lambda) := A(\lambda)(\lambda_{2,i}(\lambda) b_h^\top + \lambda_{3,i}(\lambda) b_V^\top - \hat{B}(\lambda)).$$

We are now ready to state the result.

Proposition 9.2.5. (Sufficient condition for compatibility without knowledge of upper bound on the norm of a safe stabilizing controller): *Let the functions $g_h, g_V : \mathbb{R}^m \to \mathbb{R}$ be given by*

$$g_h(\mathbf{u}) = \mathbf{u}^\top (Q_h^\top Q_h - b_h^\top b_h)\mathbf{u} + 2(r_h^\top Q_h - b_h c_h)\mathbf{u} + \|r_h\|^2 - c_h^2,$$
$$g_V(\mathbf{u}) = \mathbf{u}^T (Q_V^\top Q_V - b_V^\top b_V)\mathbf{u} + 2(r_V^\top Q_V - b_V c_V)\mathbf{u} + \|r_V\|^2 - c_V^2,$$

and define the functions $\{\eta_i : \mathcal{F}_i \to \mathbb{R}\}_{i=0}^3$ by $\eta_i(\lambda) = \lambda g_h(u_i^*(\lambda))$. Further consider the constraints

$$g_h(\mathbf{u}) \leq 0, \quad -b_h \mathbf{u} - c_h \leq 0, \quad -b_V \mathbf{u} - c_V \leq 0. \tag{9.6}$$

Then, (9.2) *are compatible if there is* $i \in \{0,1,2,3\}$ *such that there exists a non-negative root* $\lambda_i^* \in \mathcal{F}_i$ *of* η_i *such that* $\lambda_{2,i}(\lambda_i^*) \geq 0$, $\lambda_{3,i}(\lambda_i^*) \geq 0$, $g_V(u_i^*(\lambda_i^*)) \leq 0$, $g_h(u_i^*(\lambda_i^*)) \leq 0$, *the constraints in* (9.6) *at* $u_i^*(\lambda_i^*)$ *are satisfied, and the gradients of the active constraints in* (9.6) *are linearly independent.*

Proof. Let

$$\begin{aligned} \sigma \coloneqq \min_{\mathbf{u}\in\mathbb{R}^m} & \; g_V(\mathbf{u}) \\ \text{s.t. } & g_h(\mathbf{u}) \leq 0, \quad -b_h\mathbf{u} - c_h \leq 0, \quad -b_V\mathbf{u} - c_V \leq 0. \end{aligned} \tag{9.7}$$

By [38], (9.2) are compatible if and only if $\sigma \leq 0$. The result now follows by applying the KKT conditions to Problem (9.7). The condition that the gradients of the active constraints in (9.6) are linearly independent guarantees that Linear Independence Constraint Qualification (cf. [99, Definition 2.4]) holds at the optimizer of (9.7). Hence, the optimizer of (9.7) satisfies the KKT conditions of (9.7), cf. [178, Theorem 5.33]. Let then $\mathcal{L}(\mathbf{u},\lambda_1,\lambda_2,\lambda_3) = g_V(\mathbf{u}) + \lambda_1 g_h(\mathbf{u}) + \lambda_2(-b_h\mathbf{u} - c_h) + \lambda_3(-b_V\mathbf{u} - c_V)$ be the Lagrangian of (9.7). The stationarity condition $\nabla_{\mathbf{u}}\mathcal{L}(\mathbf{u},\lambda_1,\lambda_2,\lambda_3) = 0$ implies that any solution $u^*, \lambda_1^*, \lambda_2^*, \lambda_3^*$ of the KKT conditions with $\lambda_1^* \in \mathcal{F}_0$ satisfies

$$u^* = A(\lambda_1^*)(\lambda_2^* b_h^\top + \lambda_3^* b_V^\top - \hat{B}(\lambda_1^*)).$$

Now the four different cases in the statement arise by applying the rest of the KKT conditions depending on whether the constraints $-b_h\mathbf{u} - c_h \leq 0$, $-b_V\mathbf{u} - c_V \leq 0$ are active at the optimizer. The case $i = 0$ corresponds to both constraints being inactive, the case $i = 1$ to both constraints being active, the case $i = 2$ to only the constraint $-b_V\mathbf{u} - c_V \leq 0$ being active, and $i = 3$ to only the constraint $-b_h\mathbf{u} - c_h \leq 0$ being active. □

Remark 9.2.6. (Applicability of Proposition 9.2.5): Although the problem of knowing whether a nonlinear equation has any roots is undecidable in general, cf. [224], if a root satisfying either of the specific conditions in Proposition 9.2.5 can be rapidly found, this result provides a quick test for the compatibility of the two SOCCs in (9.2). A simple setting in which this holds is the following.

Recall that η_1 is a function of $\mathbf{x}$ and suppose that a root $\lambda^*_{\mathbf{x}_0}$ of η_1 has been found at a point $\mathbf{x}_0$. Moreover, suppose that the inequalities $\lambda_{2,1}(\lambda^*_{\mathbf{x}_0}) > 0$, $\lambda_{3,1}(\lambda^*_{\mathbf{x}_0}) > 0$, $g_V(u_1^*(\lambda^*_{\mathbf{x}_0})) < 0$ and $g_h(u_1^*(\lambda^*_{\mathbf{x}_0})) < 0$ are satisfied strictly. Then, under the assumptions of the Implicit Function Theorem [225, Theorem 2-12], there exists a neighborhood $\mathcal{V}$ of $\mathbf{x}_0$ such that for all $\mathbf{x} \in \mathcal{V}$, there exists a root $\lambda^*_{\mathbf{x}}$ of η_1 that is close to $\lambda^*_{\mathbf{x}_0}$. Therefore, we can limit the search of the root to a neighborhood of $\lambda^*_{\mathbf{x}_0}$ and we should expect to find a solution satisfying the conditions in Proposition 9.2.5 fast. Analogous observations are valid for $i \in \{0, 2, 3\}$. •

Remark 9.2.7. (Necessity of Proposition 9.2.5): Proposition 9.2.5 is close to being a necessary and sufficient condition for compatibility. The gap arises from not including the cases where $\lambda_i^* \notin \mathcal{F}_i$ for $i \in \{0, 1, 2, 3\}$ or where the gradients of the active constraints in (9.6) at the optimizer of (9.7) are linearly dependent. In these cases, a condition that ensures compatibility of the SOCCs can still be given on the basis of the KKT conditions of (9.7), but its statement becomes quite involved and we have not included it in Proposition 9.2.5 for simplicity. •

Remark 9.2.8. (Practical significance of sufficient conditions): Propositions 9.2.2 and 9.2.5 are complementary to each other. Proposition 9.2.2 requires the knowledge of the upper bound B, but is computationally cheap. Proposition 9.2.5 requires less restrictive assumptions but involves finding a root of a nonlinear scalar equation, which can be more computationally expensive. Their practical usage is threefold, both in online and offline settings. First, if they are not met (which does not mean that the corresponding pair of SOCCs is not compatible), this can be taken as an indication that the estimates of the dynamics, CLF, and CBF need to be improved. Therefore, in settings where data is gathered online and the uncertainty models are updated on the fly, Propositions 9.2.2 and 9.2.5 pave the way for the design of active learning strategies that leverage them to decide when more data needs to be collected. Second, these sufficient conditions can be used to identify the regions of the state space where compatibility might fail, and design control strategies that avoid them in order to guarantee recursive feasibility. This is particularly relevant in settings where uncertainty models are not updated online and plans that avoid regions of high model uncertainty have to be designed offline.

Third, given that in general, state-of-the-art SOCP solvers provide infeasibility and optimality certificates with the same time complexity, cf. [226, Section A], our sufficient conditions can be used before solving the SOCP to save computation time in the case where the problem is unfeasible. This latter point is illustrated in more detail in our simulations below, cf. Section 9.4. •

9.3 Design and Regularity Analysis of Controllers Satisfying SOCCs

In this section, we study the existence and regularity properties of controllers satisfying sets of SOCCs. Our first result establishes that, if a set of state-dependent SOCCs are strictly compatible, then there exists a smooth controller satisfying all of them simultaneously.

Proposition 9.3.1. (Existence of a smooth controller satisfying a finite number of SOCCs): *For $i \in [p]$, let $Q_i : \mathbb{R}^n \to \mathbb{R}^{(m+1)\times m}, r_i : \mathbb{R}^n \to \mathbb{R}^{m+1}, b_i : \mathbb{R}^n \to \mathbb{R}^m, c_i : \mathbb{R}^n \to \mathbb{R}$ be continuous functions on an open set $\mathcal{G} \subset \mathbb{R}^n$. If the p SOCC inequalities $\|Q_i(\mathbf{x})\mathbf{u} + r_i(\mathbf{x})\| \leq b_i(\mathbf{x})\mathbf{u} + c_i$, $i \in [p]$, are strictly compatible on $\mathcal{G}$, then there exists a $\mathcal{C}^\infty(\mathcal{G})$ function $k : \mathcal{G} \to \mathbb{R}^m$ such that $\|Q_i(\mathbf{x})k(\mathbf{x}) + r_i(\mathbf{x})\| \leq b_i(\mathbf{x})k(\mathbf{x}) + c_i(\mathbf{x})$ for all $i \in [p]$ and all $\mathbf{x} \in \mathcal{G}$.*

This result is an extension of [227, Proposition 4.2.1] to a finite set of SOCCs. Since SOCCs define convex sets, the proof follows an identical argument and we omit it for space reasons. The combination of Propositions 9.2.2 and 9.3.1 guarantees the smooth safe stabilization of (3.1) under either worst-case or probabilistic uncertainty.

Corollary 9.3.2. (Smooth safe stabilization under uncertainty): *Let $\tilde{\mathcal{C}}$ be a neighborhood of $\mathcal{C}$, h be an η-robust CBF, and assume* (2.15) *and* (2.16) *are compatible on $\tilde{\mathcal{C}}$. Let $\mathcal{V}$ be a neighborhood of the origin and $\tilde{\mathcal{V}}$ be the smallest sublevel set of V containing $\mathcal{V}$.*

(1) (Local smooth safe control): *Suppose that* (9.3) *(resp.* (9.4)*) holds at $\mathbf{x}_0 \in \mathcal{C}\backslash\mathcal{V}$ and* (9.1) *(resp.* (9.2)*) is continuous at $\mathbf{x}_0$. Then, there exists a neighborhood*

$\mathcal{W}_{\mathbf{x}_0}$ of $\mathbf{x}_0$, a smooth controller $k_{\mathbf{x}_0} : \mathcal{W}_{\mathbf{x}_0} \to \mathbb{R}^m$, and a time $t_{\mathbf{x}_0} > 0$ such that the flow map of $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k_{\mathbf{x}_0}(\mathbf{x})$, denoted by $\Psi_t(\mathbf{x})$, is such that $\Psi_t(\mathbf{x}_0) \in \mathcal{C}$ and $\frac{d}{dt}V(\Psi_t(\mathbf{x}_0)) < 0$ for all $t \in [0, t_{\mathbf{x}_0})$ (resp. with probability at least $1 - 2\delta$);

(2) (Global smooth safe stabilization): *Let $\hat{\mathcal{C}}$ be open with $\mathcal{C} \subseteq \hat{\mathcal{C}} \subseteq \tilde{\mathcal{C}}$. If* (9.3) *(resp.* (9.4)*) holds for all $\mathbf{x} \in \hat{\mathcal{C}} \backslash \mathcal{V}$ and* (9.1) *(resp.* (9.2)*) is continuous on $\hat{\mathcal{C}} \backslash \mathcal{V}$, then there exists a smooth controller $k : int(\hat{\mathcal{C}} \backslash \mathcal{V}) \to \mathbb{R}^m$ such that all trajectories of $\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x})$ starting at $\mathcal{C}$ remain in $\mathcal{C}$ and asymptotically converge to $\tilde{\mathcal{V}}$ (resp. with probability at least $1 - 2\delta$);*

Remark 9.3.3. (Asymptotic stability): If conditions (9.3) and (9.4) hold for all points in $\tilde{\mathcal{C}} \backslash \{0\}$ (not only for all points in $\tilde{\mathcal{C}} \backslash \mathcal{V}$), then Corollary 9.3.2(ii) implies that the origin is asymptotically stable. This can only be the case if knowledge of ∇V near the origin is exact, cf. Remark 9.1.1. •

Note that the set $\mathcal{C}$ is unknown and hence checking the conditions (9.3) and (9.4) for all $x \in \mathcal{C} \backslash \mathcal{V}$ may not be practical. This is the reason why we introduce the set $\hat{\mathcal{C}}$ in Corollary 9.3.2(ii). Corollary 9.3.2 establishes the existence of a smooth safe stabilizing controller under uncertainty, but does not provide an explicit closed-form design that can be used for implementation. In what follows, we provide controller designs that are explicit but have weaker regularity properties. Let

$$\begin{aligned} u^*(\mathbf{x}) = \arg\min_{\mathbf{u} \in \mathbb{R}^m} \frac{1}{2} \|\mathbf{u}\|^2, \\ \text{s.t.} \quad \|Q_i(\mathbf{x})\mathbf{u} + r_i(\mathbf{x})\| \leq b_i(\mathbf{x})\mathbf{u} + c_i(\mathbf{x}), \ i \in [p]. \end{aligned} \tag{9.8}$$

Note that this program can be written as a second-order convex program (SOCP), as shown in [228, Section 2.2]. If the constraints in (9.8) are either (9.1) or (9.2), we refer to (9.8) as CLF-CBF-SOCP. The following result establishes different conditions under which u^* is point-Lipschitz (cf. [8, Definition 2.1]) and locally Lipschitz.

Proposition 9.3.4. (Lipschitzness of SOCP solution): *Let $\{Q_i, r_i, b_i, c_i\}_{i=1}^p$ be twice continuously differentiable at a point $\mathbf{x} \in \mathbb{R}^n$ and assume the constraints*

in (9.8) *are strictly compatible at* x*. Then* u^* *is point-Lipschitz at* x*. Further, for* $i \in [p]$*, let*

$$\begin{aligned} g_i(\mathbf{x},\mathbf{u}) &= \|Q_i(\mathbf{x})\mathbf{u} + r_i(\mathbf{x})\| - b_i(\mathbf{x})\mathbf{u} - c_i(\mathbf{x}), \\ g_{i,1}(\mathbf{x},\mathbf{u}) &= \mathbf{u}^T(Q_i(\mathbf{x})^\top Q_i(\mathbf{x}) - b_i(\mathbf{x})b_i(\mathbf{x})^T)\mathbf{u} + r_i(\mathbf{x})^2 \\ &\quad + 2(Q_i(\mathbf{x})^\top r_i(\mathbf{x}) - c_i(\mathbf{x})b_i(\mathbf{x}))^\top \mathbf{u} - c_i(\mathbf{x})^2, \\ g_{i,2}(\mathbf{x},\mathbf{u}) &= -b_i(\mathbf{x})^\top \mathbf{u} - c_i(\mathbf{x}), \end{aligned}$$

and define

$$\begin{aligned} \mathcal{A}(\mathbf{x}) &:= \{i \in [p] : \|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| \neq 0,\ g_i(\mathbf{x}) = 0\}, \\ \mathcal{A}_1(\mathbf{x}) &:= \{i \in [p] : \|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| = 0,\ g_{i,1}(\mathbf{x}) = 0\}, \\ \mathcal{A}_2(\mathbf{x}) &:= \{i \in [p] : \|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| = 0,\ g_{i,2}(\mathbf{x}) = 0\}. \end{aligned}$$

Suppose that the vectors

$$\{\nabla_{\mathbf{u}} g_i(\mathbf{x}, u^*(\mathbf{x}))\}_{i\in\mathcal{A}(\mathbf{x})} \cup \{\nabla_{\mathbf{u}} g_{i,1}(\mathbf{x}, u^*(\mathbf{x}))\}_{i\in\mathcal{A}_1(\mathbf{x})} \cup \{\nabla_{\mathbf{u}} g_{i,2}(\mathbf{x}, u^*(\mathbf{x}))\}_{i\in\mathcal{A}_2(\mathbf{x})} \tag{9.9}$$

are linearly independent. Then, u^* *is locally Lipschitz at* x*.*

Proof. First consider the points $\mathbf{x} \in \mathcal{G}$ where $\|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| \neq 0$ for all $i \in [p]$. At these points, the constraints of (9.8) are twice continuously differentiable in $\mathbf{x}$ and $\mathbf{u}$ in a neighborhood of the optimizer. Moreover, since the constraints in (9.8) are strictly compatible, for any $\epsilon > 0$ there exists $\hat{u}_\epsilon^{\mathbf{x}}$ satisfying them strictly and such that $\|u^*(\mathbf{x}) - \hat{\mathbf{u}}_\epsilon^{\mathbf{x}}\| < \epsilon$. Since none of the constraints are active at $\hat{\mathbf{u}}_\epsilon^{\mathbf{x}}$, the Mangasarian-Fromovitz Constraint Qualification (MFCQ) holds at $\hat{\mathbf{u}}_\epsilon^{\mathbf{x}}$. By [99, Lemma 6.1] this implies that MFCQ also holds at $u^*(\mathbf{x})$. Furthermore, since the objective function in (9.8) is strongly convex and the constraints are convex, the second-order condition (SOC2) [99, Definition 6.1] holds and by [99, Theorem 6.4], u^* is point-Lipschitz at $\mathbf{x}$. Next, consider any point $\mathbf{x} \in \mathcal{G}$ where $\mathcal{I}_{\mathbf{x}} = \{i \in [p] : \|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| = 0\}$ is nonempty. Since the constraint $\|Q_i(\mathbf{x})\mathbf{u} + r_i(\mathbf{x})\| \leq b_i(\mathbf{x})\mathbf{u} + c_i(\mathbf{x})$ is not differentiable at those points, we square the SOCCs in (9.8) associated to $\mathcal{I}_{\mathbf{x}}$ to obtain the equivalent formulation

with twice-continuously differentiable constraints:

$$
\begin{aligned}
u^*(\mathbf{x}) = \arg\min_{\mathbf{u}\in\mathbb{R}^m} \frac{1}{2}\|\mathbf{u}\|^2, \qquad (9.10)\\
\text{s.t.} \quad g_{i,1}(\mathbf{x},\mathbf{u}) \le 0,\ g_{i,2}(\mathbf{x},\mathbf{u}) \le 0,\ i \in \mathcal{I}_{\mathbf{x}},\\
\|Q_i(\mathbf{x})\mathbf{u} + r_i(\mathbf{x})\| \le b_i(\mathbf{x})\mathbf{u} + c_i(\mathbf{x}),\ i \in [p]\backslash\mathcal{I}_{\mathbf{x}},
\end{aligned}
$$

Strict compatibility of the constraints in (9.8) implies the strict compatibility of the constraints in (9.10) and, by the same argument as before, MFCQ holds at the optimizer. To show that SOC2 also holds for (9.10), note that the constraints $g_{i,1}(\mathbf{x},\mathbf{u}) \le 0$ for $i \in \mathcal{I}_{\mathbf{x}}$ cannot be active at the optimizer (otherwise, that would imply that $b_i(\mathbf{x})u^*(\mathbf{x})+c_i(\mathbf{x}) = 0$, implying that MFCQ is violated at the optimizer, reaching a contradiction). Thus, by the strict complementarity condition, the Lagrange multipliers associated with the constraints $g_{i,1}(\mathbf{x},\mathbf{u}), i \in \mathcal{I}_{\mathbf{x}}$ are zero and the Hessian of the Lagrangian $\mathcal{L}$ of (9.10) at the optimizer takes the form

$$
\nabla^2_{\mathbf{u}}\mathcal{L}(u^*(\mathbf{x}), \{\lambda_i(\mathbf{x})\}_{i\in\mathcal{A}}) = \mathbf{I}_m + \sum_{i\in\mathcal{A}(\mathbf{x})} \lambda_i(\mathbf{x})\nabla^2_{\mathbf{u}} g_i(\mathbf{x}, u^*(\mathbf{x})),
$$

where λ_i is the Lagrange multiplier associated with the constraint $g_i(\mathbf{x},\mathbf{u}) \le 0$ for $i \notin \mathcal{I}_{\mathbf{x}}$. Since $\|Q_i(\mathbf{x})u^*(\mathbf{x}) + r_i(\mathbf{x})\| \neq 0$ for the active constraints, their Hessian is well-defined and is positive semidefinite due to their convexity, making $\nabla^2_{\mathbf{u}}\mathcal{L}(u^*(\mathbf{x}), \{\lambda_i(\mathbf{x})\}_{i\in\mathcal{A}})$ positive definite. Hence, SOC2 holds for (9.10) at the optimizer and, by [99, Theorem 6.4], u^* is point-Lipschitz at $\mathbf{x}$. Moreover, the assumption that the vectors in (9.9) are linearly independent implies that the gradients of the active constraints are linearly independent. By the same argument used to show that the SOC2 condition holds, the strong second-order sufficient condition also holds. This shows by [171, Theorem 4.1] that u^* is *strongly regular* at $\mathbf{x}$, which by [171, Corollary 2.1] implies that u^* is locally Lipschitz at $\mathbf{x}$. □

Note that the reformulation (9.10) in the proof of Proposition 9.3.4 by squaring the constraints is done purely for analysis purposes and does not have to be done in practice when solving (9.8).

Remark 9.3.5. (Not-locally Lipschitz example without independence of gradients): [165] introduces an example of a parametric quadratic program with strongly

convex objective function, smooth objective function and constraints, and for which Slater's condition holds for all values of the parameter. Moreover, the parametric optimizer of this problem is shown to be not locally Lipschitz. Since the parametric QP presented by Robinson is a particular case of (9.8), it also provides an example as to why the extra condition on the set (9.9) being linearly independent is necessary in order to guarantee local Lipschitzness of u^*. Our recent note [8] explores in detail the regularity properties of parametric optimization problems satisfying conditions similar to those of Robinson's counterexample and shows that such conditions guarantee point-Lipschitzness of the optimizer. This property ensures existence (but not uniqueness) of solutions of the closed-loop system. •

As a consequence of Proposition 9.3.4, we conclude that if the estimates $\hat{f}$, $\hat{g}$, $\hat{h}$, $\widehat{\nabla h}$, $\hat{V}$, $\widehat{\nabla V}$ and worst-case error bounds (resp. means and variances) that appear in (9.1) (resp. (9.2)) are twice continuously differentiable and the conditions (9.3) (resp. (9.4)) hold, then the corresponding CLF-CBF-SOCP controller is point-Lipschitz. We also note that the condition that the vectors in (9.9) are linearly independent corresponds to the Linear Independence Constraint Qualification (LICQ) [99, Definition 2.4] for problem (9.10).

Next we provide a formula, inspired by Sontag's universal formula [29], for a smooth controller satisfying a single SOCC defined by smooth functions.

Proposition 9.3.6. (Universal formula for a controller satisfying one SOCC): *Let $l \in \mathbb{Z}_{>0}$ and assume $Q : \mathbb{R}^n \to \mathbb{R}^{(m+1)\times m}$, $r : \mathbb{R}^n \to \mathbb{R}^{m+1}$, $b : \mathbb{R}^n \to \mathbb{R}^m$, and $c : \mathbb{R}^n \to \mathbb{R}$ are l-continuously differentiable on an open set $\mathcal{G} \subseteq \mathbb{R}^n$. Suppose that the SOCC $\|Q(\mathbf{x})\mathbf{u} + r(\mathbf{x})\| \leq b(\mathbf{x})\mathbf{u} + c(\mathbf{x})$ is strictly feasible on $\mathcal{G}$ and $Q(\mathbf{x})^\top Q(\mathbf{x})$ is invertible for all $\mathbf{x} \in \mathcal{G}$. Let $\tilde{b}(\mathbf{x}) = b(\mathbf{x})(Q^\top(\mathbf{x})Q(\mathbf{x}))^{-1}Q^\top(\mathbf{x})$, $\tilde{c}(\mathbf{x}) = c(\mathbf{x}) - \tilde{b}(\mathbf{x})r(\mathbf{x})$, $\bar{b}(\mathbf{x}) = (\|\tilde{b}(\mathbf{x})\| - 1)\|\tilde{b}(\mathbf{x})\|$, and*

$$v_s(\mathbf{x}) = \begin{cases} 0 & \text{if } \|\tilde{b}(\mathbf{x})\| \leq 1, \\ \frac{-\tilde{c}(\mathbf{x}) + \sqrt{\tilde{c}(\mathbf{x})^2 + \bar{b}(\mathbf{x})^2}}{\bar{b}(\mathbf{x})}\tilde{b}(\mathbf{x}) & \text{if } \|\tilde{b}(\mathbf{x})\| > 1. \end{cases} \tag{9.11}$$

Further assume $v_s(\mathbf{x}) - r(\mathbf{x}) \in Im(Q(\mathbf{x}))$ for all $\mathbf{x} \in \mathcal{G}$. Then

$$u_s(\mathbf{x}) := (Q^\top(\mathbf{x})Q(\mathbf{x}))^{-1}Q^\top(\mathbf{x})(v_s(\mathbf{x}) - r(\mathbf{x})),$$

is l-continuously differentiable for all $\mathbf{x} \in \mathcal{G}$. Moreover, $\|Q(\mathbf{x})u_s(\mathbf{x}) + r(\mathbf{x})\| \leq b(\mathbf{x})u_s(\mathbf{x}) + c(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{G}$.

Proof. Let $\mathbf{v} = Q(\mathbf{x})\mathbf{u} + r(\mathbf{x})$. Since $Q^T(\mathbf{x})Q(\mathbf{x})$ is invertible and $\|Q(\mathbf{x})\mathbf{u} + r(\mathbf{x})\| \leq b(\mathbf{x})\mathbf{u} + c(\mathbf{x})$ is strictly feasible on $\mathcal{G}$, the resulting SOCC $\|\mathbf{v}\| \leq \tilde{b}(\mathbf{x})\mathbf{v} + \tilde{c}(\mathbf{x})$ is also strictly feasible on $\mathcal{G}$. Moreover, v_s satisfies it. Indeed, if $\left\|\tilde{b}(\mathbf{x})\right\| \leq 1$, since the SOCC is feasible there exists v^* such that $\|v^*\| \leq \tilde{b}(\mathbf{x})v^* + \tilde{c}(\mathbf{x})$ and it follows that $\tilde{c}(\mathbf{x}) \geq 0$. The case $\left\|\tilde{b}(\mathbf{x})\right\| > 1$ follows from a direct calculation. If $\left\|\tilde{b}(\mathbf{x})\right\| \neq 1$, v_s is $\mathcal{C}^l$ at $\mathbf{x}$ because $\tilde{b}$ and $\tilde{c}$ are $\mathcal{C}^l$ at $\mathbf{x}$. If $\left\|\tilde{b}(\mathbf{x})\right\| = 1$, then $\tilde{c}(\mathbf{x}) \neq 0$ (otherwise, if $\tilde{c}(\mathbf{x}) = 0$, since the SOCC $\|\mathbf{v}\| \leq \tilde{b}(\mathbf{x})\mathbf{v} + \tilde{c}(\mathbf{x})$ is strictly compatible, there would exist $\hat{\mathbf{v}}$ such that $\|\hat{\mathbf{v}}\| < \tilde{b}(\mathbf{x})\hat{\mathbf{v}} \leq \|\hat{\mathbf{v}}\|$, which is a contradiction). Now, from the proof of [29, Theorem 1], the function $\phi : \mathbb{R}^2 \to \mathbb{R}$ defined as

$$\phi(c, \alpha) := \begin{cases} 0 & \text{if } \alpha \leq 0, \\ \frac{-c+\sqrt{c^2+\alpha^2}}{\alpha} & \text{else,} \end{cases}$$

is analytic at points of the form $(c, 0)$, with $c \neq 0$, so $\mathbf{v}_s$ is $\mathcal{C}^l$ for all $x \in \mathcal{G}$. Moreover, since $\mathbf{v}_s(\mathbf{x}) - r(\mathbf{x}) \in \mathrm{Im}(Q(\mathbf{x}))$ for all $\mathbf{x} \in \mathcal{G}$, it also follows that $\|Q(\mathbf{x})u_s(\mathbf{x}) + r(\mathbf{x})\| \leq b(\mathbf{x})u_s(\mathbf{x}) + c(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{G}$ and u_s is $\mathcal{C}^l$ for all $\mathbf{x} \in \mathcal{G}$. □

From the proof of Proposition 9.3.6, we observe that in the case where the SOCC takes the form (9.1), a simpler expression is available for a controller satisfying it. As a result of Proposition 9.3.6, the proposed formula can be used to guarantee safety or stability under the worst-case or probabilistic uncertainties described in Section 9.1.

Remark 9.3.7. (Using the universal formula to filter a nominal controller): The universal formula in Proposition 9.3.6 can also be used to render an existing nominal controller safe or stable. Indeed, let $u_{\mathrm{nom}} : \mathbb{R}^n \to \mathbb{R}^m$ be a nominal controller and define $\tilde{f} : \mathbb{R}^n \to \mathbb{R}^n$ as $\tilde{f}(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x})u_{\mathrm{nom}}(\mathbf{x})$ and the modified dynamics

$$\dot{\mathbf{x}} = \tilde{f}(\mathbf{x}) + g(\mathbf{x})\tilde{\mathbf{u}}, \tag{9.12}$$

with $\tilde{\mathbf{u}} \in \mathbb{R}^m$. By leveraging the estimates of f, g, V, and h either in the worst-case or probabilistic case, we can formulate SOCCs similar to (9.1) and (9.2),

respectively, for the modified system (9.12). Depending on which SOCC we choose, this allows us to use the universal formula in Proposition 9.3.6 to obtain a safe or a stable controller $\tilde{u}_s : \mathbb{R}^n \to \mathbb{R}^m$, which in turn results in $u_{\text{fi-nom}}(\mathbf{x}) = u_{\text{nom}}(\mathbf{x}) + \tilde{u}_s(\mathbf{x})$ being a safe or a stable controller for (3.1). We refer to this controller $u_{\text{fi-nom}}$ as the filtered version of the nominal controller u_{nom}. This generalizes the safe filtering of a nominal controller in the uncertainty-free case, cf. [36, 23]. •

9.4 Simulations

In this section we illustrate our results in an example. For simplicity, we focus on the case of worst-case error estimates. Consider a control-affine planar system of the form (3.1) with $f(x,y) = (-x, -(x^2+5)y)$ and $g(x,y) = (1, 0.1)$. We consider the CBF $h(x,y) = x^2 + (y-4)^2 - 4$.

From data to estimates and error bounds: We obtain here worst-case error models, cf. Section 9.1, from data. For simplicity, we assume that the CLF $V(x,y) = \frac{1}{2}(x^2+y^2)$ is known, so that $\widehat{\nabla V} = \nabla V$ and $\hat{V} = V$. We also assume that the obstacle is known to be a circle with center at $(0,4)$, but its radius is uncertain, so that $\hat{h}(x,y) = x^2 + (y-4)^2 - 3.8$, and $\widehat{\nabla h} = \nabla h$, $e_h = 0.4$, $e_{\nabla h} = 0$. We have access to an oracle that, given a query point $(x,y) \in \mathcal{C}$, returns noiseless measurements $(f(x,y), g(x,y))$ of the functions in (3.1) (the noisy case can be considered without major modifications). Given a set of N measurements $\mathcal{D} = \{(x_i,y_i), f(x_i,y_i), g(x_i,y_i)\}_{i=1}^N$ obtained by querying the oracle, we estimate f at $(x,y) \in \mathbb{R}^2$ as $\hat{f}(x,y) = f(p_{\text{cl}}(x,y))$, where $p_{\text{cl}}(x,y)$ is the closest datapoint to (x,y). Prior knowledge of (not necessarily tight) Lipschitz constants of f and g in a compact region containing the origin, the initial conditions and $\{(x_i,y_i)\}_{i=1}^N$ ($K_f = 28.0$ and $K_g = 3.2$ respectively) is also available. We compute the corresponding worst-case error bounds as $e_f(x,y) \coloneqq K_f \|(x,y) - p_{\text{cl}}(x,y)\|$. We do similarly for $\hat{g}$ and e_g.

Performance dependency on error estimates: Here we illustrate how smaller estimation errors lead to improved performance. We use different datasets with different number of data points N to generate $\hat{f}$, $\hat{g}$, e_f, and e_g. We solve the

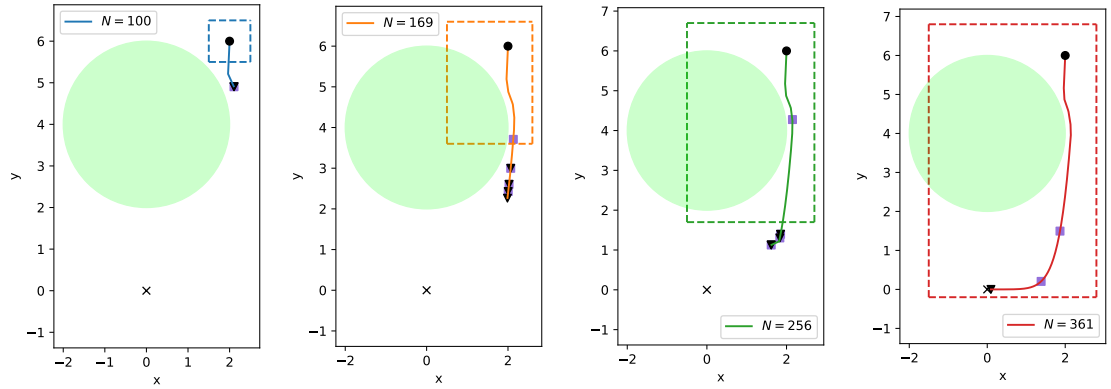


Figure 9.1: Safe stabilization of a planar system with worst-case uncertainty error bounds. The green ball is the unsafe set and black dots denote initial conditions. Dashed lines enclose the region where data is located for different N. Solid lines show the evolution under the corresponding CLF-CBF-SOCP controller in (9.8). Black triangles indicate points where the sufficient conditions for feasibility (9.3) in Proposition 9.2.2 do not hold. Purple squares denote points where the root-finding method (`fsolve` from Python's `SCIPY` library) did not return a solution satisfying the sufficient condition of Proposition 9.2.5.

resulting CLF-CBF-SOCP every 0.01s with initial condition at $(2.0, 6.0)$ and plot the trajectories until it becomes unfeasible. We compare the results for different N in Figure 9.1. Larger datasets with data from a neighborhood of the origin allow trajectories to converge closer to the origin before the problem becomes unfeasible. This illustrates one of the critical points of the paper: optimization-based control formulations that take uncertainty into account in order to ensure safety or stability might be unfeasible depending on the specific system and the magnitude of the errors in the employed approximations. Our results here provide quantifiable conditions to determine whether the accuracy of the approximations is sufficient or, instead, they need to be refined in order to guarantee feasibility. In the plot, we observe that the sufficient conditions in Propositions 9.2.2 and 9.2.5 serve as a good indicator of when the SOCP actually becomes unfeasible, hence illustrating how they can be used to infer when the available estimates are insufficient to guarantee that the controller is well defined.

Online safe stabilization: We illustrate also the case where data is collected online. We start from an initial set of 150 measurements of f, g and h near the initial condition obtained by querying the oracle. Given an initial condition, at

every 0.01s we check whether the conditions in (9.3) hold. If this is the case, we find the CLF-CBF-SOCP controller and execute it. If during the execution the conditions in (9.3) stop being satisfied at some point $\bar{\mathbf{x}}$, we query the oracle to obtain measurements of f and g at $\bar{\mathbf{x}}$ (making it feasible) and a small neighborhood around it (for improved performance). Figure 9.2 illustrates executions of this procedure for three different initial conditions. As trajectories approach the origin, more measurements need to be taken because the conditions in (9.3) become harder to satisfy.

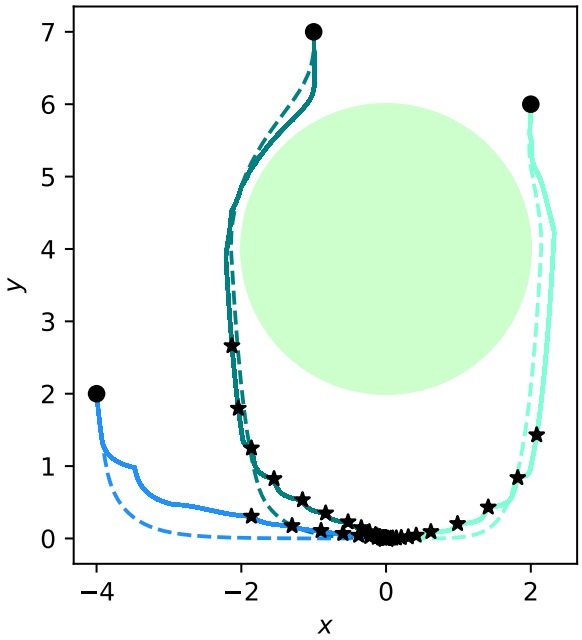


Figure 9.2: Safe stabilization of a planar system with worst-case uncertainty error bounds. The green ball is the unsafe set and black dots denote initial conditions. The solid lines display the evolution of the controller obtained by solving the CLF-CBF-SOCP (9.8). Black stars denote points where measurements have been taken. All trajectories asymptotically converge to a ball around the origin of radius 0.01. For reference, the dashed lines display the evolution of a min-norm controller with perfect knowledge of the dynamics, CBF and CLF (CLF-CBF QP) [1], for which the trajectories stay safe and asymptotically converge to the origin.

Time complexity: We show here the computational savings of checking the sufficient conditions in Propositions 9.2.2 and 9.2.5 as compared to directly solving the SOCP using the Embedded Conic Solver from the Python library CVXPY. Figure 9.3 shows that the time complexity of using the SOCP solver is higher than

the time complexity of checking the sufficient condition in Proposition 9.2.5, which is in turn higher than the time complexity of checking the sufficient condition of Proposition 9.2.2. Since, in general, state-of-the-art SOCP solvers provide infeasibility and optimality certificates with the same time complexity, cf. [226, Section A], our sufficient conditions can be used to save computation time in the case where the problem is unfeasible, cf. Remark 9.2.8.

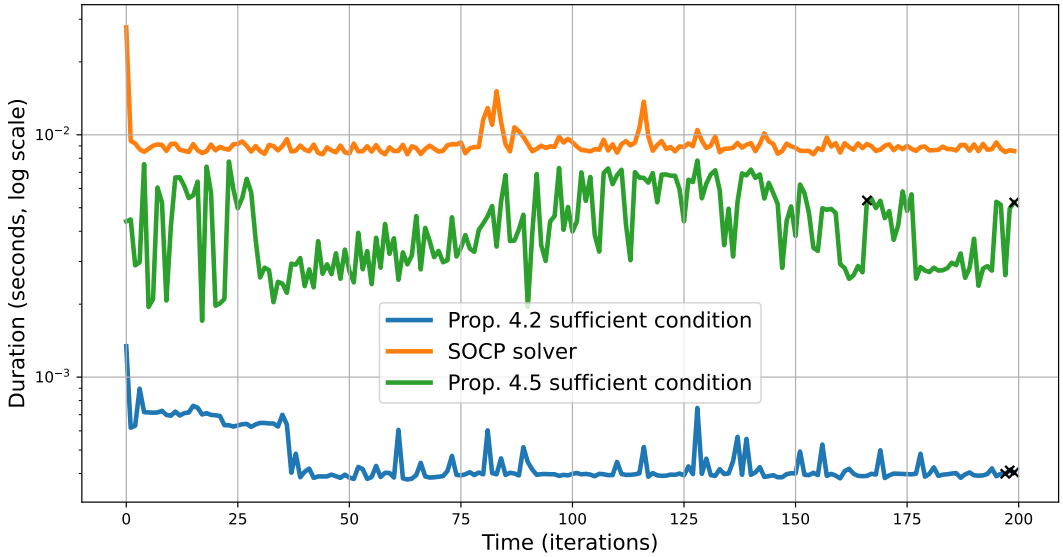


Figure 9.3: Time complexity comparison of evaluating the sufficient conditions in Proposition 4.2 (blue), Proposition 4.5 (green) and using an SOCP solver (orange) along the trajectory with $N = 361$ in Figure 9.1. Note that the trajectory is plotted until the CLF-CBF-SOCP becomes unfeasible. Therefore, the SOCP is feasible at all points in the trajectory. The black crosses denote points where the sufficient conditions do not hold. On average, the sufficient conditions in Proposition 4.2 is 50 times faster to evaluate than directly solving the SOCP.

Chapter 10

Feasibility Analysis and Regularity Characterization of Distributionally Robust Safe Stabilizing Controllers

Similarly to the Chapter 9, this chapter also studies the well-posedness and regularity of safe stabilizing optimization-based controllers for control-affine systems in the presence of model uncertainty. However, here we assume that the system dynamics contain unknown parameters, and we leverage a finite number of samples of such parameters to formulate a distributionally robust version of the CBF and CLF constraints. Control synthesis with such distributionally robust constraints can again be achieved by solving a (convex) SOCP. We provide one necessary and two sufficient conditions to check the feasibility of such optimization problems, characterize their computational complexity and numerically show that they are significantly faster to check than direct use of SOCP solvers. Finally, we also analyze the regularity of the resulting control laws.

10.1 Problem Statement

Consider a nominal system F and a linear combination of k perturbations:

$$\dot{\mathbf{x}} = \big(F(\mathbf{x}) + \sum_{j=1}^{k} W_j(\mathbf{x})\xi_j\big)\underline{\mathbf{u}} \tag{10.1}$$

where for $1 \le j \le k$, $W_j(\mathbf{x}) \in \mathbb{R}^{n\times(m+1)}$ denotes known model perturbations, and $\xi_j \in \mathbb{R}$ denotes the corresponding unknown weight, and $\underline{\mathbf{u}} = [1; \mathbf{u}] \in \underline{\mathcal{U}} := \{1\} \times \mathbb{R}^m$. We let $\boldsymbol{\xi} = [\xi_1, \xi_2, \cdots, \xi_k]^\top \in \Xi \subseteq \mathbb{R}^k$. We assume that $\boldsymbol{\xi}$ follows an unknown distribution $\mathbb{P}^*$ but a set of samples $\{\boldsymbol{\xi}_i\}_{i=1}^N$ is available. Note that as shown in [43, Section IV], the CBF condition for a system of the form (10.1) and a function $h : \mathbb{R}^n \to \mathbb{R}$ reads as $\mathrm{CBC}(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}) := \underline{\mathbf{u}}^\top q_h(\mathbf{x}) + \underline{\mathbf{u}}^\top R_h(\mathbf{x})\boldsymbol{\xi} \ge 0$, where the exact forms of q_h and R_h are given in [43, Section IV] and depends on h and its gradient. Now, since $\boldsymbol{\xi}$ follows a distribution $\mathbb{P}^*$, we extend the definition of CBF by requiring that for all $\mathbf{x}$ in the safe set, there exist $\underline{\mathbf{u}} \in \underline{\mathcal{U}}$ such that

$$\mathbb{P}^*(\mathrm{CBC}(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}) \ge 0) \ge 1 - \epsilon. \tag{10.2}$$

The CLF condition for (10.1) takes a similar form and is written as $\mathrm{CLC}(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}) \le 0$ (cf. [43, Section IV]). As shown in Section 2.9, CVaR can be used as a convex approximation of (10.2). Hence, we introduce the following definitions.

Definition 10.1.1. (Control Lyapunov Function for Systems with Distributional Uncertainty): *Let $\epsilon \in (0,1)$. Given a set $\Gamma \subset \mathbb{R}^n$, with $\mathbf{0}_n \in \Gamma$, a continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ is a CLF on Γ for (10.1) if it is proper in Γ, positive definite, and for each $\mathbf{x} \in \Gamma\backslash\{\mathbf{0}_n\}$, there exists a control $\underline{\mathbf{u}} \in \underline{\mathcal{U}}$ satisfying*

$$\mathrm{CVaR}^{\mathbb{P}^*}_{1-\epsilon}(\mathrm{CLC}(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi})) \le 0.$$

Definition 10.1.2. (Control Barrier Function for Systems with Distributional Uncertainty): *Let $\epsilon \in (0,1)$, $\mathcal{C} \subset \mathbb{R}^n$ and $h : \mathbb{R}^n \to \mathbb{R}$ continuously differentiable such that (2.6) holds. The function h is a CBF for (10.1) if there is a $\mathcal{K}_\infty$ function α such that for all $\mathbf{x} \in \mathcal{C}$, there exists $\underline{\mathbf{u}} \in \underline{\mathcal{U}}$ with*

$$\mathrm{CVaR}^{\mathbb{P}^*}_{1-\epsilon}(\mathrm{CBC}(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi})) \ge 0.$$

The existence of a CLF (resp. a CBF) for (10.1) implies the existence of a controller that makes the CLC (resp. the CBC) condition hold at every point with probability at least $1-\epsilon$. paving the way for the design of controllers that make the system stable (resp. safe) with arbitrarily high probability.

Consider the system model in (10.1) with distributional uncertainty, meaning that the true distribution $\mathbb{P}^*$ of the parameter $\boldsymbol{\xi}$ is unknown. Assume the system admits a CLF and a CBF, as specified in Definitions 10.1.1 and 10.1.2, respectively. Given a nominal controller specified by a smooth function $\underline{k}:\mathbb{R}^n\to\underline{\mathcal{U}}$, we would like to synthesize a controller closest to it that respects safety and stability constraints. Using (2.20), this problem can be written in general form as

$$\begin{aligned}&\min_{\underline{\mathbf{u}}\in\underline{\mathcal{U}}} \|\underline{\mathbf{u}}-\underline{k}(\mathbf{x})\|^2 \\ &\text{s.t.} \sup_{\mathbb{P}\in\mathcal{M}_N^r} \inf_{t\in\mathbb{R}} [\epsilon^{-1}\mathbb{E}_{\mathbb{P}}[(G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi})+t)_+]-t]\le 0,\ \forall l\in[M],\end{aligned} \tag{10.3}$$

where $M\in\mathbb{Z}_{>0}$ and each $G_l:\mathbb{R}^n\times\underline{\mathcal{U}}\times\Xi\to\mathbb{R}$ is an affine function in $\underline{\mathbf{u}}$ and $\boldsymbol{\xi}$, $G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi})=\underline{\mathbf{u}}^\top q_l(\mathbf{x})+\underline{\mathbf{u}}^\top R_l(\mathbf{x})\boldsymbol{\xi}$, for smooth functions $q_l:\mathbb{R}^n\to\mathbb{R}^{m+1}$ and $R_l:\mathbb{R}^n\to\mathbb{R}^{(m+1)\times k}$. With $M=2$ and constraints corresponding to CBC and CLC, this corresponds to a stable and safe control synthesis problem. The case $M=1$ with the constraint CBC corresponds to a distributionally robust version of a safety filter of $\underline{k}$.

Although the constraints in (10.3) are convex, the program is intractable due to the search of suprema over the Wasserstein set. Fortunately, [43, Proposition IV.1] shows that when $\Xi=\mathbb{R}^k$ and $p=1$, the following SOCP is equivalent to (10.3):

$$\min_{\underline{\mathbf{u}}\in\underline{\mathcal{U}},y\in\mathbb{R},t\in\mathbb{R},s_i\in\mathbb{R}} y \tag{10.4a}$$

$$\text{s.t.}\quad r\,\|R_l^\top(\mathbf{x})\underline{\mathbf{u}}\|+\frac{1}{N}\sum_{i=1}^N s_i-t\epsilon\le 0,\ \forall l\in[M], \tag{10.4b}$$

$$s_i\ge G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi}_i)+t,\ \forall i\in[N],\ \forall l\in[M], \tag{10.4c}$$

$$s_i\ge 0,\ \forall i\in[N], \tag{10.4d}$$

$$y+1\ge\sqrt{\|2(\underline{\mathbf{u}}-\underline{k}(\mathbf{x}))\|^2+(y-1)^2}\ . \tag{10.4e}$$

We refer to (10.4) as the DRO-SOCP and take $\Xi=\mathbb{R}^k$ and $p=1$ Wasserstein distance throughout the paper.

A critical observation about problem (10.4) is that, in general, it might be infeasible, leading to controllers that are undefined. Furthermore, even if the problem is feasible, the controller obtained from it might not be continuous, hence resulting in implementation problems (it might induce chattering behavior when implemented on physical systems) and theoretical problems (lack of existence of solutions of the closed-loop system). Hence, our goal in this paper is twofold. First, we want to derive conditions to ensure the feasibility of (10.4). Given the complexity of obtaining characterizations for the feasibility of such problems, we focus on identifying conditions that are easy to evaluate computationally as opposed to directly attempting to solve the optimization problem: either sufficient conditions, to quickly ensure feasibility, or necessary, to quickly discard it. Second, assuming that the problem (10.4) is feasible, we want to characterize the regularity properties of the resulting controller.

10.2 Feasibility Analysis

In this section, we study the feasibility properties of (10.4). We start by giving a necessary condition for its feasibility.

Proposition 10.2.1. (Necessary condition for feasibility of DRO-SOCP): *Let* $\epsilon \in (0, \frac{1}{N}]$ *and* $r > 0$. *For* $\mathbf{x} \in \mathbb{R}^n$, *let*

$$\begin{aligned}
&\bar{Q}_l(\mathbf{x}) = rR_l(\mathbf{x})_{2:(m+1)} \in \mathbb{R}^{m\times k},\ \bar{r}_l(\mathbf{x}) = rR_l(\mathbf{x})_1 \in \mathbb{R}^{1\times k},\\
&\bar{w}_{l,i}(\mathbf{x}) = (-\epsilon q_l(\mathbf{x}) - \epsilon R_l(\mathbf{x})\boldsymbol{\xi}_i)_{2:(m+1)} \in \mathbb{R}^m,\\
&\bar{v}_{l,i}(\mathbf{x}) = (-\epsilon q_l(\mathbf{x}) - \epsilon R_l(\mathbf{x})\boldsymbol{\xi}_i)_1 \in \mathbb{R},\\
&\bar{F}_{l,i}(\mathbf{x}) = \bar{Q}_l(\mathbf{x})\bar{Q}_l(\mathbf{x})^\top - \bar{w}_{l,i}(\mathbf{x})\bar{w}_{l,i}(\mathbf{x})^\top \in \mathbb{R}^{m\times m},
\end{aligned}$$

for $l \in [M]$ *and* $i \in [N]$. *Let* $\bar{\lambda}_{l,i}(\mathbf{x})$ *be the minimum eigenvalue of* $\bar{F}_{l,i}(\mathbf{x})$ *and suppose* $\bar{Q}_l(\mathbf{x})\bar{Q}_l(\mathbf{x})^\top$ *is invertible for all* $l \in [M]$. *If* (10.4) *is feasible, then for each* $l \in [M]$, *there exists* $i \in [N]$ *such that one of the following holds:*

(1) $\bar{\lambda}_{l,i}(\mathbf{x}) < 0$,

(2) $\bar{\lambda}_{l,i}(\mathbf{x}) > 0$ *and* $\left(\bar{v}_{l,i} - \bar{w}_{l,i}^\top \bar{F}_{l,i}^{-1}(\bar{Q}_l\bar{r}_l^\top - \bar{w}_{l,i}\bar{v}_{l,i})\right)(\mathbf{x}) \geq 0$,

(3) $\bar{\lambda}_{l,i}(\mathbf{x}) = 0$, *and* $\left(\bar{v}_{l,i} - \bar{w}_{l,i}^\top(\bar{Q}_l\bar{Q}_l^\top)^{-1}\bar{Q}_l\bar{r}_l^\top\right)(\mathbf{x}) > 0$.

Proof. Note that (10.3) (and hence (10.4)) is equivalent to

$$\begin{aligned} &\min_{\underline{\mathbf{u}}\in\underline{\mathcal{U}}} \left\|\underline{\mathbf{u}} - \underline{k}(\mathbf{x})\right\|^2 \\ &\text{s.t. } r\left\|R_l^\top(\mathbf{x})\underline{\mathbf{u}}\right\| + \inf_{t\in\mathbb{R}}\Big[\frac{1}{N}\sum_{i=1}^{N}(G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi}_i)+t)_+ - t\epsilon\Big] \le 0, \end{aligned} \tag{10.5}$$

for $l \in \{1,\dots,M\}$, cf. [43, Proposition IV.1]. For $(\mathbf{x},\underline{\mathbf{u}}) \in \mathbb{R}^n \times \underline{\mathcal{U}}$, the function $A^l_{\mathbf{x},\underline{\mathbf{u}}}(t) = \frac{1}{N}\sum_{i=1}^{N}(G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi}_i)+t)_+ - t\epsilon$ is a piecewise linear function in t. Since $\epsilon \le \frac{1}{N}$, it is decreasing for $t < t_l^*(x,\underline{\mathbf{u}}) := \min_{i\in[N]} -G_l(\mathbf{x},\underline{\mathbf{u}},\boldsymbol{\xi}_i)$ and increasing for $t > t_l^*(\mathbf{x},\underline{\mathbf{u}})$. Hence, it achieves its minimum at $t_l^*(\mathbf{x},\underline{\mathbf{u}})$. Thus, (10.4) is feasible if and only if for all $l \in [M]$ the following inequalities are simultaneously feasible:

$$r\left\|R_l^\top(\mathbf{x})\underline{\mathbf{u}}\right\| + \epsilon\underline{\mathbf{u}}^\top q_l(\mathbf{x}) + \epsilon\max_{i\in[N]}\underline{\mathbf{u}}^\top R_l(\mathbf{x})\boldsymbol{\xi}_i \le 0. \tag{10.6}$$

Note that, if for some $l \in [M]$, the constraint $r\left\|R_l^\top(\mathbf{x})\underline{\mathbf{u}}\right\| + \epsilon\underline{\mathbf{u}}^\top q_l(\mathbf{x}) + \epsilon\underline{\mathbf{u}}^\top R_l(\mathbf{x})\boldsymbol{\xi}_i \le 0$ is infeasible for all $i \in [N]$, then (10.4) is infeasible. The result now follows from [38, Theorem 2], which gives a characterization for the feasibility of a single second-order cone constraint. □

The following observation explains how Proposition 10.2.1 can be used to check for the infeasibility of (10.4) efficiently.

Remark 10.2.2. (Computational complexity of necessary condition): *A commonly used algorithm for solving SOCPs is the method in [229]. For an SOCP with r_S constraints and optimization variable of dimension n_S it requires solving $\sqrt{r_S}$ linear systems of dimension n_S and hence has complexity $\mathcal{O}(\sqrt{r_S}n_S^3)$ (cf. [230]). Therefore,* (10.4) *has complexity $\mathcal{O}(\sqrt{MN}(m+N)^3)$. Instead, since checking the positive definiteness of a symmetric matrix of dimension n_P can be done by checking if its Cholesky factorization exists (which has complexity $\mathcal{O}(n_P^3)$), the complexity of checking the condition in Proposition 10.2.1 is $\mathcal{O}(NMm^3)$. Hence, for large N, it is much more efficient than solving the SOCP* (10.4) *directly. We also note that the scaling in M for the complexity of the SOCP solver is more favorable than that of checking the necessary condition.* •

Next, we state a sufficient condition for the feasibility of (10.4) in the case $M = 1$.

Proposition 10.2.3. (Sufficient condition for feasibility of DRO-SOCP with one constraint): *Let $r > 0$, $M = 1$, and $0 < \epsilon \leq \frac{1}{N}$. Given $\mathbf{x} \in \mathbb{R}^n$, define*

$$\begin{aligned}
\hat{Q}(\mathbf{x}) &= (r + \epsilon \max_{i\in[N]} \|\boldsymbol{\xi}_i\|) R_1(\mathbf{x})_{2:(m+1)} \in \mathbb{R}^{m\times k},\\
\hat{r}(\mathbf{x}) &= (r + \epsilon \max_{i\in[N]} \|\boldsymbol{\xi}_i\|) R_1(\mathbf{x})_1 \in \mathbb{R}^{1\times k},\\
\hat{w}(\mathbf{x}) &= -\epsilon q_1(\mathbf{x})_{2:(m+1)} \in \mathbb{R}^m,\ \hat{v}(\mathbf{x}) = -\epsilon q_1(\mathbf{x})_1 \in \mathbb{R},\\
\hat{F}(\mathbf{x}) &= Q(\mathbf{x})Q(\mathbf{x})^\top - w(\mathbf{x})w(\mathbf{x})^\top \in \mathbb{R}^{m\times m}.
\end{aligned}$$

Let $\hat{\lambda}(\mathbf{x})$ be the minimum eigenvalue of $\hat{F}(\mathbf{x})$. Suppose that $Q(\mathbf{x})Q(\mathbf{x})^\top$ is invertible and one of the following holds:

(1) $\hat{\lambda}(\mathbf{x}) < 0$,

(2) $\hat{\lambda}(\mathbf{x}) > 0$ *and* $\left(\hat{v} - \hat{w}^\top \hat{F}^{-1}(\hat{Q}\hat{r}^\top - \hat{w}\hat{v})\right)(\mathbf{x}) \geq 0$,

(3) $\hat{\lambda}(\mathbf{x}) = 0$ *and* $\left(\hat{v} - \hat{w}^\top (\hat{Q}\hat{Q}^\top)^{-1}\hat{Q}\hat{r}^\top\right)(\mathbf{x}) > 0$.

Then, (10.4) *is feasible at* $\mathbf{x}$.

Proof. By repeating an argument similar to the one in the proof of Proposition 10.2.1, (10.4) is feasible in the case $M = 1$ if and only if the following inequality is feasible:

$$r\,\|R(\mathbf{x})^\top \underline{\mathbf{u}}\| + \epsilon \underline{\mathbf{u}}^\top q(\mathbf{x}) + \epsilon \max_{i\in[N]} \underline{\mathbf{u}}^\top R(\mathbf{x})\boldsymbol{\xi}_i \leq 0. \tag{10.7}$$

Using the Cauchy-Schwartz inequality, the following inequality being feasible implies that (10.7) is feasible,

$$(r + \epsilon \max_{i\in[N]} \|\boldsymbol{\xi}_i\|)\,\|R(\mathbf{x})^\top \underline{\mathbf{u}}\| + \epsilon \underline{\mathbf{u}}^\top q(\mathbf{x}) \leq 0. \tag{10.8}$$

Indeed, if (10.8) is feasible, there exists $\hat{\underline{\mathbf{u}}}$ such that $r\,\|\hat{\underline{\mathbf{u}}}^\top R(\mathbf{x})\| + \epsilon \hat{\underline{\mathbf{u}}}^\top q(\mathbf{x}) + \epsilon \hat{\underline{\mathbf{u}}}^\top R(\mathbf{x})\boldsymbol{\xi}_i \leq 0$ for all $i \in [N]$, and hence $\hat{\underline{\mathbf{u}}}$ satisfies (10.7). The result follows by [38, Thm. 2]. □

Remark 10.2.4. (Computational complexity of the sufficient condition): *The complexity of checking the sufficient condition in Proposition 10.2.3 reduces to finding a maximum of N numbers (which has complexity linear in N) and checking the positive definiteness of a symmetric matrix of dimension m. Hence, its complexity is $\mathcal{O}(N + m^3)$, which is more efficient than solving the SOCP* (10.4)*, which has complexity $\mathcal{O}(\sqrt{N}(m+N)^3)$, cf. Remark 10.2.2.* •

Remark 10.2.5. (More data leads to better feasibility guarantees): *For a fixed r, the addition of new data points (larger N) implies that there are more chances that either of (i)-(iii) in Proposition 10.2.1 are satisfied for each $l \in \{1, \ldots, M\}$. Moreover, if $\mathbb{P}^*$ is light-tailed, $r_N(\bar{\epsilon})$ decreases with N. The choice $r = r_N(\bar{\epsilon})$ means that for each fixed $i \in [N]$ and $l \in [M]$, the feasible set of the inequality $r \|R_l(\mathbf{x})^\top \underline{\mathbf{u}}\| + \epsilon \underline{\mathbf{u}}^\top q_l(\mathbf{x}) + \epsilon \underline{\mathbf{u}}^\top R_l(\mathbf{x}) \boldsymbol{\xi}_i \leq 0$ increases, which from the proof of Proposition 10.2.1, also means that there are more chances that either of (i)-(iii) are met. Similarly, under the assumption that the norm of additional samples is upper bounded by $\max_{i \in [N]} \|\boldsymbol{\xi}_i\|$, the choice $r = r_N(\bar{\epsilon})$ also leads to a larger feasible set of* (10.8) *and thus the sufficient condition in Proposition 10.2.3 has more chances of being satisfied.* •

Next, we provide a sufficient condition to ensure the feasibility of (10.4) for an arbitrary number of constraints.

Proposition 10.2.6. (Sufficient condition for feasibility of DRO-SOCP): *Let $r > 0$, $\epsilon \in (0,1)$ and $\bar{\epsilon} \in (0,1)$. Suppose that there exists a controller $\hat{k} : \mathbb{R}^n \to \underline{\mathcal{U}}$ and non-negative functions $S_l : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ for $l \in [M]$ satisfying*

$$\mathrm{CVaR}^{\mathbb{P}^*}_{1-\epsilon}(G_l(\mathbf{x}, \hat{k}(\mathbf{x}), \boldsymbol{\xi})) \leq -S_l(\mathbf{x}), \quad \forall l \in [M]. \tag{10.9}$$

Moreover, suppose that $\mathbb{P}^*$ is light-tailed and let $r_N(\bar{\epsilon})$ be defined as in (2.24)*. Let $\mathbf{x} \in \mathbb{R}^n$ be such that $\|R_l(\mathbf{x})\| \neq 0$ for all $l \in [M]$, and let $B : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be an upper bound on the norm of $\hat{k}$. Then, if*

$$r_N(\bar{\epsilon}) < \min_{l \in [M]} \frac{\epsilon S_l(\mathbf{x})}{2 \|R_l(\mathbf{x})\| B(\mathbf{x})}, \tag{10.10}$$

(10.4) *is strictly feasible at x with probability at least $1 - \bar{\epsilon}$ for any $r \leq r_N(\bar{\epsilon})$.*

Proof. Note that by definition, the first component of $\hat{k}(\mathbf{x})$ is 1 for all $\mathbf{x} \in \mathbb{R}^n$. Hence, $B(\mathbf{x}) \geq \left\|\hat{k}(\mathbf{x})\right\| \geq 1$ for all $\mathbf{x} \in \mathbb{R}^n$ so (10.10) is well-defined. Let $t_1^* \in \mathbb{R}$ be such that

$$\mathrm{CVaR}_{1-\epsilon}^{\mathbb{P}^*}(G_1(\mathbf{x}, \underline{u}, \boldsymbol{\xi})) = \frac{1}{\epsilon}\mathbb{E}_{\mathbb{P}^*}[(G_1(\mathbf{x}, \underline{u}, \boldsymbol{\xi}) + t_1^*)_+] - t_1^*,$$

and define $\hat{G}(\mathbf{x}, \boldsymbol{\xi}) = \frac{1}{\epsilon}(G_1(\mathbf{x}, \hat{k}(\mathbf{x}), \boldsymbol{\xi}) + t_1^*)_+ - t_1^*$. Note that for any $\boldsymbol{\xi}, \boldsymbol{\xi}' \in \mathbb{R}^k$,

$$|\hat{G}(\mathbf{x}, \boldsymbol{\xi}) - \hat{G}(\mathbf{x}, \boldsymbol{\xi}')| \leq \frac{1}{\epsilon}\left\|R_1(x)\right\| \cdot \left\|\hat{k}(\mathbf{x})\right\| \cdot \left\|\boldsymbol{\xi} - \boldsymbol{\xi}'\right\|, \tag{10.11}$$

where we have used the fact that the operator $(\cdot)_+$ is Lipschitz with constant 1. Using (10.11) in [110, Theorem 3.2], we conclude that for any $\hat{\mathbb{P}} \in \mathcal{P}_p(\Xi)$,

$$|\mathbb{E}_{\mathbb{P}^*}(\hat{G}(\mathbf{x}, \boldsymbol{\xi})) - \mathbb{E}_{\hat{\mathbb{P}}}(\hat{G}(\mathbf{x}, \boldsymbol{\xi}))| \leq \frac{1}{\epsilon}\left\|R_1(\mathbf{x})\right\| \cdot \left\|\hat{k}(\mathbf{x})\right\| \cdot W_1(\mathbb{P}^*, \hat{\mathbb{P}}).$$

From condition (10.10), together with the fact that $\mathcal{M}_N^{r_N(\bar{\epsilon})}$ contains $\mathbb{P}^*$ with probability at least $1-\bar{\epsilon}$ (cf. Remark 2.9.1) and since the maximum Wasserstein distance between two distributions in $\mathcal{M}_N^{r_N(\bar{\epsilon})}$ is $2r_N(\bar{\epsilon})$, this means that with probability at least $1-\bar{\epsilon}$,

$$|\mathrm{CVaR}_{1-\epsilon}^{\mathbb{P}^*}(G_1(\mathbf{x}, \hat{k}(\mathbf{x}), \boldsymbol{\xi})) - \mathbb{E}_{\hat{\mathbb{P}}}(\hat{G}(\mathbf{x}, \boldsymbol{\xi}))| < S_1(\mathbf{x}). \tag{10.12}$$

for any $\hat{\mathbb{P}} \in \mathcal{M}_N^{r_N(\bar{\epsilon})}$. By definition of CVaR, cf. (2.20), for any $\hat{\mathbb{P}} \in \mathcal{P}_p(\Xi)$,

$$\mathrm{CVaR}_{1-\epsilon}^{\hat{\mathbb{P}}}(G_1(\mathbf{x}, \hat{k}(\mathbf{x}), \boldsymbol{\xi})) \leq \mathbb{E}_{\hat{\mathbb{P}}}(\hat{G}(\mathbf{x}, \boldsymbol{\xi})).$$

Combining this with (10.12) and (10.9), we get that with probability at least $1-\bar{\epsilon}$, $\mathrm{CVaR}_{1-\epsilon}^{\hat{\mathbb{P}}}(G_1(\mathbf{x}, \hat{k}(\mathbf{x}), \boldsymbol{\xi})) < 0$ for all $\hat{\mathbb{P}} \in \mathcal{M}_N^{r_N(\bar{\epsilon})}$. This argument holds for $l \in \{2, \cdots, N\}$, implying that $\hat{k}(\mathbf{x})$ is strictly feasible for (10.3) (and hence, (10.4)) with probability at least $1-\bar{\epsilon}$ for any $r \leq r_N(\bar{\epsilon})$. □

Remark 10.2.7. (Dependency of sufficient condition on slack terms): *Condition* (10.9) *on the controller* $\hat{k}$ *corresponds to the satisfaction of the constraints in* (10.3) *with a slack term* $S_l(\mathbf{x})$ *on the righthand side. Larger values of these slack terms mean that fewer samples are needed to satisfy* (10.10). •

Remark 10.2.8. (Applicability of the sufficient condition): *Checking condition* (10.10) *does not require precise knowledge of* $\hat{k}$*, just an upper bound of its norm. In particular, if bounds on the control norm are included as constraints in* (10.4)*, those can be used to construct* B*. Moreover, unlike Proposition 10.2.3, condition* (10.10) *is agnostic to the samples* $\{\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_N\}$ *and instead solely depends on its number* N*. Note that for each* $\mathbf{x} \in \mathbb{R}^n$ *with* $\|R_l(\mathbf{x})\| \neq 0$ *for all* $l \in [M]$*, if* $S_l(\mathbf{x}) > 0$ *for all* $l \in [M]$*, there exists* $\hat{N}_{\mathbf{x}}$ *such that condition* (10.10) *holds for all* $N \geq \hat{N}_{\mathbf{x}}$*. This is because* $r_N(\bar{\epsilon})$ *is decreasing in* N *and* $\lim_{N\to\infty} r_N(\bar{\epsilon}) = 0$*. The value* $\hat{N}_{\mathbf{x}}$ *is state-dependent and is larger for smaller values of* ϵ*,* $S_l(\mathbf{x})$*, and larger values of* $B(\mathbf{x})$*. Note also that the complexity of checking the conditions in Proposition 10.2.6 is constant in* N *and* m*, and is linear in* M *due to the minimum in* (10.10). •

Given CBF and CLF constraints, according to Remark 2.6.4 we can find functions S_l as required in Proposition 10.2.6, even without knowledge of $\hat{k}$. Proposition 10.2.1 provides necessary conditions for feasibility. If the conditions are not met, it is advisable to gather more data for feasibility verification without directly solving the program. Moreover, Propositions 10.2.3 and 10.2.6 give sufficient conditions for feasibility. If the conditions are not met (which does not mean that (10.4) is infeasible), this may be an indication that more data is needed to certify feasibility, cf. Remarks 10.2.5 and 10.2.8.

10.3 Regularity Analysis

In this section, we show that the controller obtained by solving (10.4) is point-Lipschitz (cf. [8, Definition 2.1]).

Proposition 10.3.1. (Point-Lipschitzness of SOCP DRO): *Let* $r > 0$*,* $0 < \epsilon \leq \frac{1}{N}$ *and suppose* R_l *and* q_l *are twice continuously differentiable for all* $l \in [M]$*. Let* $\underline{\mathbf{u}}^* : \mathbb{R}^n \to \mathbb{R}^m$ *be the function mapping* $\mathbf{x} \in \mathbb{R}^n$ *to the solution of* (10.4) *in* $\underline{\mathbf{u}}$ *at* $\mathbf{x}$*. If* (10.3) *is strictly feasible at* $\mathbf{x}_0 \in \mathbb{R}^n$ *(i.e., there exists a solution satisfying all the constraints strictly), then* $\underline{\mathbf{u}}^*$ *is point-Lipschitz at* $\mathbf{x}_0$*.*

Proof. We first show the result for $M = 1$. Let

$$\mathcal{I} := \arg\max_{i\in[N]} G_1(\mathbf{x}_0, \underline{\mathbf{u}}^*(\mathbf{x}_0), \boldsymbol{\xi}_i). \tag{10.13}$$

Note that the set $\mathcal{I}$ is dependent on $\mathbf{x}_0$, but we omit this dependency to simplify the notation. Note also that since $G_1(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}_i)$ is continuous in $\mathbf{x}$ and $\underline{\mathbf{u}}$ for all $i \in [N]$, there exists a neighborhood $\mathcal{N} = \mathcal{N}_{\mathbf{x}} \times \mathcal{N}_{\underline{\mathbf{u}}} \subset \mathbb{R}^n \times \underline{\mathcal{U}}$ of $(\mathbf{x}_0, \underline{\mathbf{u}}^*(\mathbf{x}_0))$ such that for all $(\hat{\mathbf{x}}, \hat{\underline{\mathbf{u}}}) \in \mathcal{N}$, there exists $i_{\hat{\mathbf{x}},\hat{\underline{\mathbf{u}}}} \in \mathcal{I}$ such that $i_{\hat{\mathbf{x}},\hat{\underline{\mathbf{u}}}} \in \arg\max_{i\in[N]} G_1(\hat{\mathbf{x}}, \hat{\underline{\mathbf{u}}}, \boldsymbol{\xi}_i)$.

Recall from the proof of Proposition 10.2.1 that, for any $\mathbf{x}, \underline{\mathbf{u}} \in \mathbb{R}^n \times \underline{\mathcal{U}}$, the function $A_{\mathbf{x},\underline{\mathbf{u}}}(t) := \frac{1}{N}\sum_{i=1}^{N}(G_1(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}_i) + t)_+ - t\epsilon$ attains its minimum at $t^*(\mathbf{x}, \underline{\mathbf{u}}) := \max_{i\in[N]} G_1(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}_i)$. Therefore, for $(\hat{\mathbf{x}}, \hat{\underline{\mathbf{u}}}) \in \mathcal{N}$, $t^*(\hat{\mathbf{x}}, \hat{\underline{\mathbf{u}}}) = G_1(\hat{\mathbf{x}}, \hat{\underline{\mathbf{u}}}, \boldsymbol{\xi}_{i_{\hat{\mathbf{x}},\hat{\underline{\mathbf{u}}}}})$.

For each $i \in \mathcal{I}$, let $\underline{\mathbf{u}}_i^* : \mathbb{R}^n \to \mathbb{R}^m$ be defined as:

$$\begin{aligned} \underline{\mathbf{u}}_i(x) := \min_{\underline{\mathbf{u}}\in\underline{\mathcal{U}}} \|\underline{\mathbf{u}} - \underline{k}(\mathbf{x})\|^2 \\ \text{s.t. } r\|R_1(\mathbf{x})^\top \underline{\mathbf{u}}\| + \epsilon G_1(\mathbf{x}, \underline{\mathbf{u}}, \boldsymbol{\xi}_i) \le 0. \end{aligned} \tag{10.14}$$

Note that since (10.3) is strictly feasible at $\mathbf{x}_0$, there exists $\tilde{\underline{\mathbf{u}}} \in \underline{\mathcal{U}}$ such that $r\|R_1(\mathbf{x}_0)^\top \tilde{\underline{\mathbf{u}}}\| + \max_{i\in[N]} \epsilon G_1(\mathbf{x}_0, \tilde{\underline{\mathbf{u}}}, \boldsymbol{\xi}_i) < 0$. By continuity of R_1 and G_1 in $\mathbf{x}$, there exists a neighborhood $\tilde{\mathcal{N}}_{\mathbf{x}} \subset \mathcal{N}_{\mathbf{x}}$ of $\mathbf{x}_0$ such that $r\|R_1(\mathbf{x})^T \tilde{\underline{\mathbf{u}}}\| + \epsilon G_1(\mathbf{x}, \tilde{\underline{\mathbf{u}}}, \boldsymbol{\xi}_i) < 0$ for all $\mathbf{x} \in \tilde{\mathcal{N}}_{\mathbf{x}}$ and $i \in \mathcal{I}$. This implies that (10.14) is strictly feasible for any $\mathbf{x} \in \tilde{\mathcal{N}}_x$. Hence, by [12, Proposition 5.4], $\underline{u}_i^*$ is point-Lipschitz at $\mathbf{x}_0$ for each $i \in \mathcal{I}$. Now, since for all $\mathbf{y} \in \mathcal{N}_x$ there exists $i \in \mathcal{I}$ such that $\underline{u}^*(\mathbf{y}) = \underline{u}_i^*(\mathbf{y})$, and $\tilde{\mathcal{N}}_{\mathbf{x}} \subset \mathcal{N}_{\mathbf{x}}$, it follows that $\|\underline{u}^*(\mathbf{y}) - \underline{u}^*(\mathbf{x}_0)\| = \|\underline{u}_i^*(\mathbf{y}) - \underline{u}_i^*(\mathbf{x}_0)\| \le l_i \|\mathbf{y} - \mathbf{x}_0\|$ for some $l_i > 0$. Now, by taking $l := \max_{i\in\mathcal{I}} l_i$, it follows that $\|\underline{u}^*(\mathbf{y}) - \underline{u}^*(\mathbf{x}_0)\| \le l\|\mathbf{y} - \mathbf{x}_0\|$ for all $\mathbf{y} \in \mathcal{N}_{\mathbf{x}}$ and hence $\underline{u}^*$ is point-Lipschitz at $\mathbf{x}_0$. The argument if $M > 1$ proceeds analogously by defining a set $\mathcal{I}_l$ similar to $\mathcal{I}$ for each $l \in [M]$. □

Proposition 10.3.1 implies in particular that u^* is continuous at x_0. Note also that the strict feasibility assumption in Proposition 10.3.1 is satisfied with a prescribed probability if the hypothesis of Proposition 10.2.6 are satisfied.

10.4 Simulations

In this section, we evaluate our results in a ground-robot navigation example. We model the robot motion using unicycle kinematics and take a small distance

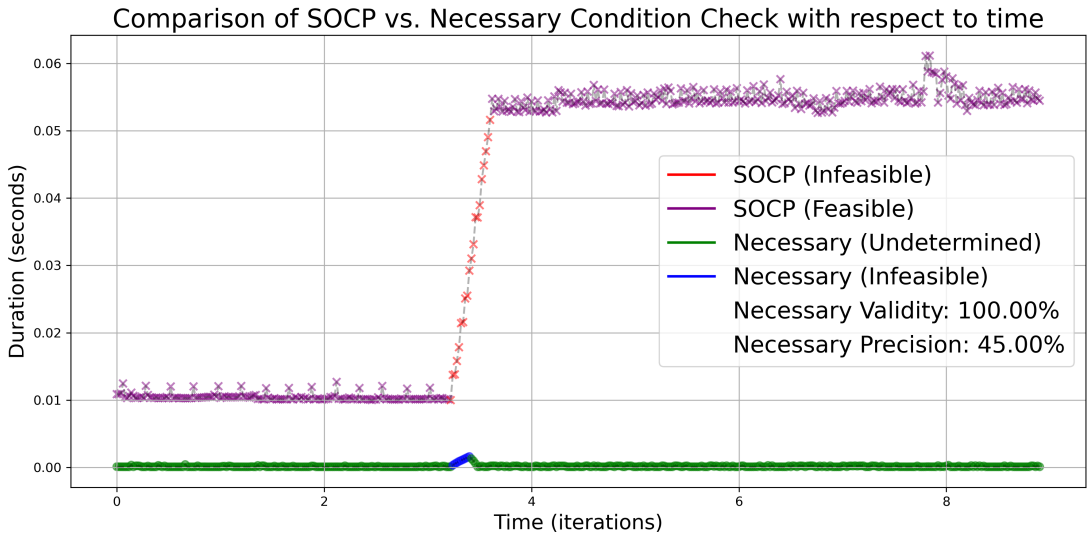


Figure 10.1: Time complexity comparison between necessary condition verification (cf. Proposition 10.2.1) and SOCP solver along the robot trajectory. The label "undetermined" means that the necessary condition is met, from which we could not know if the problem is feasible or not.

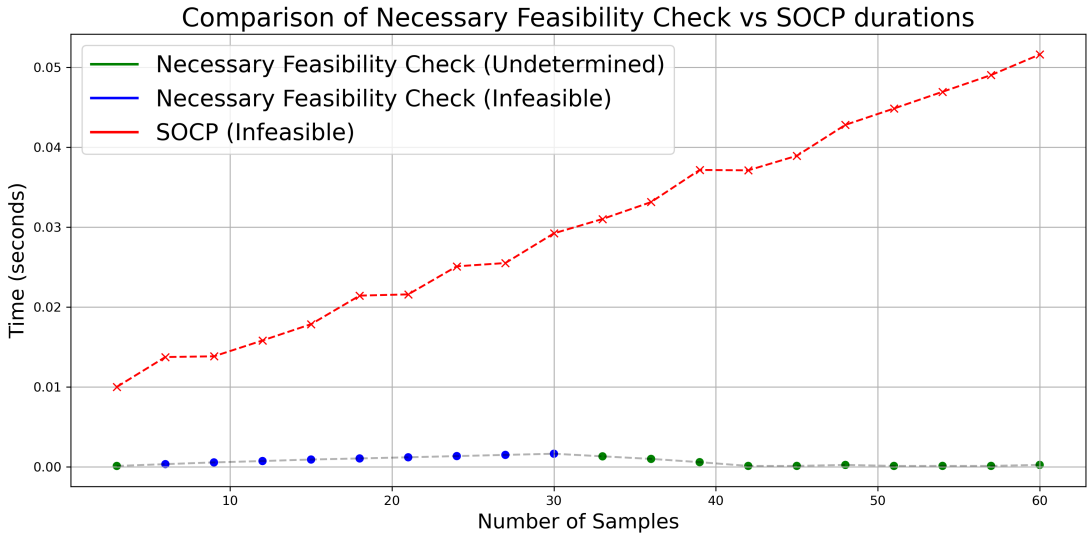


Figure 10.2: Time complexity of necessary condition verification and SOCP solver with increasing uncertainty samples (constraints).

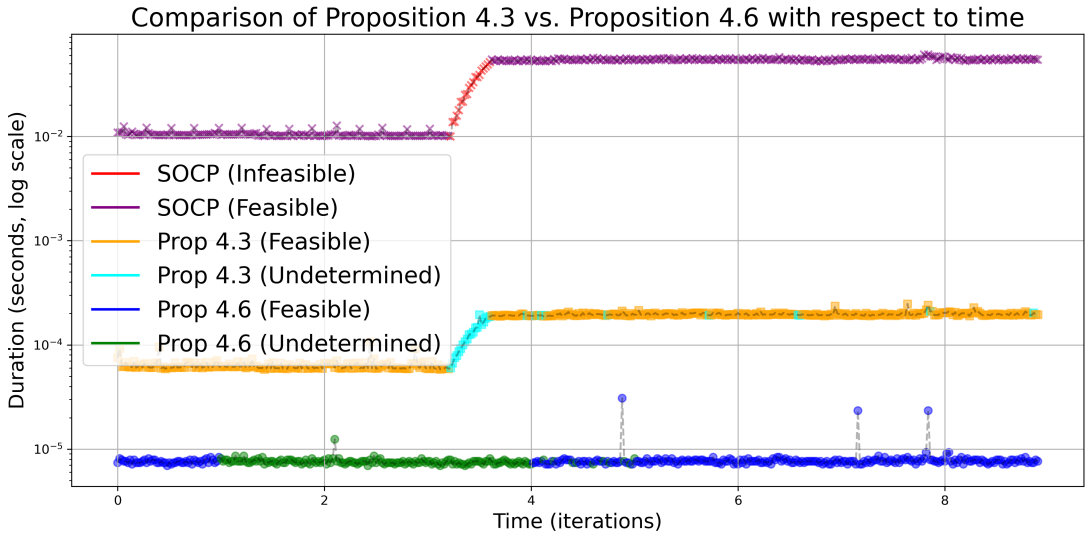


Figure 10.3: Log-scaled time complexity comparison of two sufficient conditions (cf. Proposition 10.2.3 and Proposition 10.2.6) with the SOCP solver along the robot trajectory.

$a = 0.05$ off the wheel axis, cf.[231] to obtain a relative-degree-one model:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{\theta} \end{bmatrix} = \left(\begin{bmatrix} 0 & \cos(\theta) & -a\sin(\theta) \\ 0 & \sin(\theta) & a\cos(\theta) \\ 0 & 0 & 1 \end{bmatrix} + \sum_{j=1}^{3} W_j(x_1, x_2, \theta)\xi_j \right) \begin{bmatrix} 1 \\ v \\ \omega \end{bmatrix},$$

where v, ω are the linear and angular velocity, and

$$W_1(x_1, x_2, \theta) = \begin{bmatrix} 0.02 & 0 & 0 \\ 0.02 & 0 & 0 \\ 0.01 & 0 & 0 \end{bmatrix}, W_2(x_1, x_2, \theta) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -0.02 \end{bmatrix},$$

$$W_3(x_1, x_2, \theta) = \begin{bmatrix} 0 & 0.02\cos(\theta) & -0.02a\sin(\theta) \\ 0 & 0.02\sin(\theta) & 0.02a\cos(\theta) \\ 0 & 0 & 0 \end{bmatrix},$$

represent the model perturbations in the drift, angular velocity, and orientation. We consider uncertainty samples from the following distributions: $\xi_1 \sim \mathcal{N}(0.5, 1)$, $\xi_2 \sim \mathcal{U}(-1, 1)$, and $\xi_3 \sim \mathcal{B}(2, 0.2)$, where $\mathcal{N}$, $\mathcal{U}$, $\mathcal{B}$ denote normal, uniform, and beta distributions, respectively. The optimization programs are solved using the Embedded Conic Solver in CVXPY [232] with an Intel i7 9700K CPU.

We first consider the problem of stabilizing the uncertain unicycle system to a goal position $[x_1^\star, x_2^\star] = [7, 7]$ with initial state $[0, 0, 0]$, so we take $M = 1$ in (10.3).

At the initial state, the robot is assumed to have access to 3 samples $\{\boldsymbol{\xi}_i\}_{i=1}^3$ and initial Wasserstein radius $r = 0.5$ with risk tolerance $\epsilon = 0.01$. As the robot moves in the environment, each unsuccessful solver attempt prompts the collection of additional uncertainty samples and a corresponding reduction in the ambiguity radius as prescribed by (2.24).

The time complexity, validity, and precision of Proposition 10.2.1 are explored in Fig. 10.1 and Fig. 10.2. Fig. 10.1 compares the time complexity of checking the necessary condition in Proposition 10.2.1 and solving the corresponding SOCP along the robot trajectory. Notably, the SOCP becomes infeasible at around $t = 3$ s and more uncertainty samples are given until feasibility is regained. As expected, when Proposition 10.2.1 predicts the program is infeasible, such inference is consistently mirrored by the solver. Fig. 10.2 specifically emphasizes the time complexity during data collection stages. As the number of samples increases, the SOCP's time complexity escalates at a much faster rate than the necessary condition verification, in agreement with Remark 10.2.2.

Fig. 10.3 compares the time complexity of solving the SOCP and of checking the sufficient conditions in Propositions 10.2.3 and 10.2.6. As expected, feasibility validation by either result ensures the actual feasibility of the program by the solver. Checking Proposition 10.2.3 is more time-consuming than checking Proposition 10.2.6, cf. Remark 10.2.4, but has greater accuracy in validating feasibility. Notably, both checks are significantly more efficient than solving the SOCP problem.

We also consider the safe stabilizing problem of the unicycle system. The stabilization goal is $[x_1^*, x_2^*] = [5, 5]$ while the safety goal is to avoid a circular obstacle centered at $[3, 2]$ with radius 1. Fig. 10.4 compares the time complexity and conservativeness of Proposition 10.2.1 and Proposition 10.2.6 for the case $M = 2$ in (10.3). Proposition 10.2.1 is valid and requires significantly less time than solving the SOCP, while Proposition 10.2.6 is also valid and even more efficient.

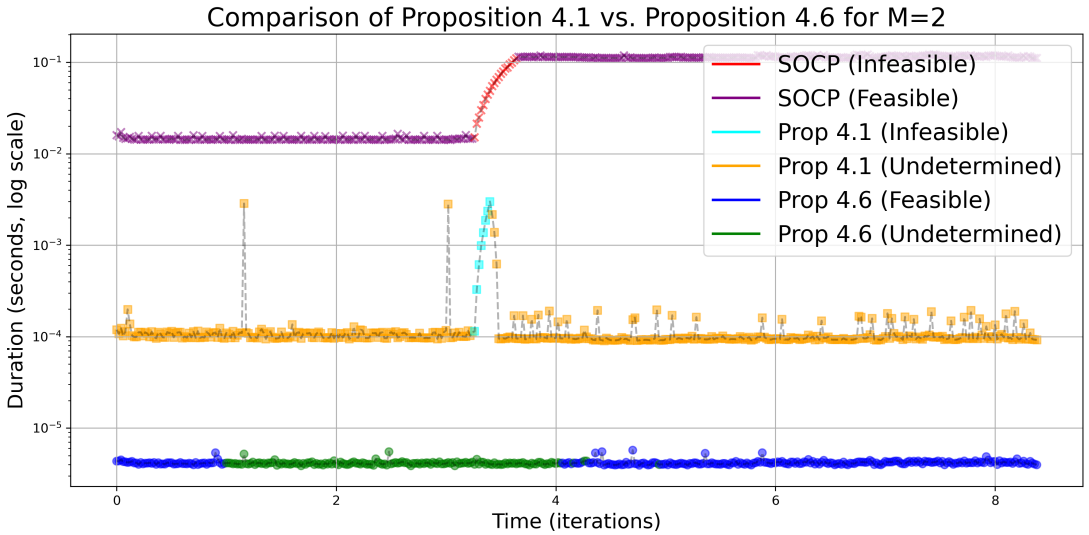


Figure 10.4: Time complexity comparison of necessary (cf. Proposition 10.2.1) and sufficient (cf. Proposition 10.2.6) conditions.

Chapter 11

Anytime Safe Reinforcement Learning

This chapter considers the problem of solving constrained reinforcement learning (RL) problems with anytime guarantees, which means that the algorithmic solution yields a policy that satisfies the constraints of the problem at every iteration. To this end, first we introduce a continuous-time algorithm for constrained optimization called the *Robust Safe Gradient Flow* (RSGF), which is a variation of the recently introduced *Safe Gradient Flow*. Next, we leverage the RSGF to introduce RL-SGF, an off-policy algorithm for constrained RL which employs estimates of the value functions and their respective gradients, and updates the policy parameters by solving a convex quadratically constrained quadratic program. By studying the statistical properties of such estimates, we show that if the estimates are computed with a sufficiently large number of episodes (which we explicitly quantify), safe policies are updated to safe policies with an arbitrarily high probability. We also show that the iterates of the algorithm asymptotically converge to a KKT point with high probability, and we provide an explicit rate of convergence. Various simulations illustrate our results.

11.1 Problem Statement

In this section we formalize the problem of solving constrained reinforcement learning (RL) problems in an anytime fashion. Given a CMDP defined by $\mathcal{M} = (\mathcal{S}, \mathcal{A}, P, R_0, \{R_j\}_{j=1}^q)$, the goal is to maximize the cumulative reward while keeping the cumulative costs below a certain threshold. We consider a parametric class of policies indexed by a vector $\boldsymbol{\theta} \in \mathbb{R}^d$. We denote the policy associated with $\boldsymbol{\theta}$ as $\pi_{\boldsymbol{\theta}}$. Given a distribution η of initial states, a discount factor $\gamma \in (0,1)$, and a time horizon $T \in \mathbb{Z}_{>0}$, we consider the following problem:

$$\begin{aligned} \min_{\boldsymbol{\theta}\in\mathbb{R}^d} \; & V_0(\boldsymbol{\theta}) = \mathbb{E}_{\substack{a\sim\pi_{\boldsymbol{\theta}}(\cdot|s)\\ s_0\sim\eta}}\left[\sum_{k=0}^{T} -\gamma^k R_0(s_k, a_k, s_{k+1})\right] \\ \text{s.t.} \quad & V_j(\boldsymbol{\theta}) = \mathbb{E}_{\substack{a\sim\pi_{\boldsymbol{\theta}}(\cdot|s)\\ s_0\sim\eta}}\left[\sum_{k=0}^{T} \gamma^k R_j(s_k, a_k, s_{k+1})\right] \leq 0, \;\; j \in [q]. \end{aligned} \tag{11.1}$$

Problem (11.1) seeks to find the policy $\pi_{\boldsymbol{\theta}}$ that maximizes the expected cumulative reward given by R_0 (note that, for convenience, we have changed the sign of R_0 to turn (11.1) into a minimization problem) over T time steps and also maintains the expected cumulative costs given by R_j for all $j \in [q]$ over T time steps below zero. Throughout the paper, we refer to the functions $V_0, \cdots, V_q$ as *value functions*. The discount factor γ determines how much future rewards are valued compared to immediate rewards.

Remark 11.1.1. (Ensuring safety of state trajectories): Throughout the paper, the notion of *safety* refers to the satisfaction of the constraints in (11.1), and therefore pertains the policy parameter θ. Interestingly, with an appropriate selection of the cost function R_j, this safety guarantee implies the forward invariance of a desired set $\mathcal{C}_j \subset \mathcal{S}$ with a prescribed confidence. In fact, let

$$R_j(s_t) = 1 - \mathbb{1}_{\mathcal{C}_j}(s_t) + \frac{\gamma^T \delta_j}{\sum_{t=0}^{T-1} \gamma^t},$$

where $0 < \delta_j < 1$, for all $j \in [q]$, are prescribed confidence levels. According to [89, Theorems 1 and 2], the satisfaction of the cumulative constraints in (11.1) implies that

$$\mathbb{P}\Big(\bigcap_{t=0}^{T-1} \{s_t \in \mathcal{C}_j\}\Big) \geq 1 - \delta_j, \quad \forall j \in [q],$$

i.e., the probability that the states remain within $\mathcal{C}_j$ in the next T timesteps is at least $1 - \delta_j$. •

The functions $\{V_i\}_{i=0}^q$ are in general non-convex, and this makes solving (11.1) NP-hard. Therefore, we aim to find local minimizers (or, more generally, KKT points) of (11.1). Additionally, because of their definition, the values of $V_0, \cdots, V_q$ and their gradients at arbitrary $\boldsymbol{\theta} \in \mathbb{R}^d$ are not readily available, and instead need to be estimated through episodic data (i.e., trajectories generated by the policy $\pi_{\boldsymbol{\theta}}$) of the CMDP.

Formally, we seek to solve the following problem.

Problem 3. *Develop an RL algorithm that,*

- *converges to a KKT point of* (11.1)*;*
- *is anytime, meaning that at every iteration, the constraints of* (11.1) *are satisfied.*

Due to the probabilistic nature of the CMDP dynamics, Problem 3 can only be solved in a probabilistic sense, i.e., given a finite number of available episodes, one can only expect to obtain convergence and constraint satisfaction results that hold in probability. As the number of available episodes grows, one can also expect that the convergence and constraint satisfaction guarantees hold with arbitrarily high probability.

11.2 The Robust Safe Gradient Flow

In this section, we introduce the Robust Safe Gradient Flow (RSGF), a continuous-time anytime algorithm for constrained optimization that is a variation of the *Safe Gradient Flow* [98]. We later rely on the RSGF to design our proposed solution to Problem 3. Even though our proposed RL algorithm will eventually be defined in discrete time, the properties of the continuous-time flow established here are key, as we will leverage them using the theory of stochastic approximation, cf. [233, 234].

Let $V_0, \cdots, V_{\tilde{q}} : \mathbb{R}^d \to \mathbb{R}$ be continuously differentiable functions and consider the constrained optimization problem

$$\begin{aligned} &\min_{\boldsymbol{\theta} \in \mathbb{R}^d} \; V_0(\boldsymbol{\theta}) \\ &\text{s.t.} \quad V_j(\boldsymbol{\theta}) \leq 0, \; j \in [\tilde{q}]. \end{aligned} \tag{11.2}$$

We let $\mathcal{C} = \{\boldsymbol{\theta} \in \mathbb{R}^d : V_j(\boldsymbol{\theta}) \leq 0, \; \forall j \in [\tilde{q}]\}$ denote the feasible set. Given $\alpha > 0$ and a continuously differentiable function $\beta : \mathbb{R}^d \to \mathbb{R}_{>0}$, consider the map $\mathcal{R}_{\alpha,\beta} : \mathbb{R}^d \to \mathbb{R}^d$ defined by

$$\begin{aligned} \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) = \arg\min_{\xi \in \mathbb{R}^d} \frac{1}{2} \left\| \xi + \nabla V_0(\boldsymbol{\theta}) \right\|^2 \\ \text{s.t. } \alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \xi + \frac{\beta(\boldsymbol{\theta})}{2} \left\| \xi \right\|^2 \leq 0, \; j \in [\tilde{q}]. \end{aligned} \tag{11.3}$$

We note that if $\beta \equiv 0$, this definition recovers the Safe Gradient Flow [98]. We are interested in studying the dynamical properties of the flow

$$\dot{\boldsymbol{\theta}} = \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}), \tag{11.4}$$

which we refer to as the Robust Safe Gradient Flow (RSGF). In particular, we seek to determine conditions under which the dynamics is well-posed and characterize the transient and asymptotic behavior of its trajectories.

11.2.1 Well-Posedness and Regularity Properties

We start by introducing some regularity and constraint qualification assumptions regarding the optimization problem (11.2).

Assumption 10. (Regularity): *The functions $V_0, \cdots, V_{\tilde{q}} : \mathbb{R}^d \to \mathbb{R}$, and $\beta : \mathbb{R} \to \mathbb{R}$ are twice continuously differentiable.*

Assumption 11. (Constraint qualifications in the feasible set): *For all $\boldsymbol{\theta} \in \mathcal{C}$,* (11.2) *satisfies MFCQ. Additionally, for each $\boldsymbol{\theta} \in \mathcal{C}$, the parametric problem* (11.3) *satisfies CRC at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$.*

Assumption 12. (Constraint qualifications outside the feasible set): *For all $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$, Slater's condition holds for* (11.3) *and the parametric problem* (11.3) *satisfies CRC at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$.*

Assumption 10 is standard in the literature [235] and is satisfied by considering smooth policies π_θ. MFCQ and CRC in Assumptions 11, 12 are standard constraint qualification conditions for constrained optimization problems such as (11.2) and (11.3), and ensure that $\mathcal{R}_{\alpha,\beta}$ enjoys good regularity properties, as we establish in the sequel. Lemma 11.7.1 provides conditions under which Slater's condition holds for (11.3) for each $\theta \in \mathbb{R}^d \backslash \mathcal{C}$, and Lemma 11.7.2 provides conditions under which CRC holds for (11.3) at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$ for some $\boldsymbol{\theta} \in \mathcal{C}$.

The next result provides a closed-form expression for $\mathcal{R}_{\alpha,\beta}$ in terms of the Lagrange multipliers of (11.3).

Lemma 11.2.1. (Alternative expression for RSGF): *Let $u_j : \mathbb{R}^d \to \mathbb{R}$ map $\boldsymbol{\theta} \in \mathbb{R}^d$ to the Lagrange multiplier associated with the j-th constraint of* (11.3)*. If MFCQ holds for* (11.2) *at $\boldsymbol{\theta} \in \mathcal{C}$, then*

$$\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) = -\frac{\nabla V_0(\boldsymbol{\theta}) + \sum_{j=1}^{\tilde{q}} u_j(\boldsymbol{\theta}) \nabla V_j(\boldsymbol{\theta})}{1 + \beta(\boldsymbol{\theta}) \sum_{j=1}^{\tilde{q}} u_j(\boldsymbol{\theta})}. \tag{11.5}$$

Proof. Note that since $\theta \in \mathcal{C}$, $[\tilde{q}] = I_0(\theta) \cup I_-(\theta)$. Since MFCQ holds for (11.2) at $\boldsymbol{\theta}$, there exists $\xi \in \mathbb{R}^d$ such that $\nabla V_j(\boldsymbol{\theta})^\top \xi < 0$ for all $j \in I_0(\boldsymbol{\theta})$. Hence, by taking $\epsilon_j < \frac{2|\nabla V_j(\boldsymbol{\theta})^\top \xi|}{\beta(\boldsymbol{\theta})\|\xi\|^2}$ and $\hat{\xi} = \epsilon\xi$ with $\epsilon \in (0, \min_{j \in I_0(\boldsymbol{\theta})} \epsilon_j)$,

$$\alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \hat{\xi} + \frac{\beta(\boldsymbol{\theta})}{2} \left\|\hat{\xi}\right\|^2 < 0, \quad \forall j \in I_0(\boldsymbol{\theta}).$$

On the other hand, for every $j \in I_-(\boldsymbol{\theta})$, let ϵ_j be sufficiently small so that

$$\alpha V_j(\boldsymbol{\theta}) + \epsilon_j \nabla V_j(\boldsymbol{\theta})^\top \hat{\xi} + \epsilon_j^2 \frac{\beta(\boldsymbol{\theta})}{2} \left\|\hat{\xi}\right\|^2 < 0.$$

Now, taking $\epsilon \in (0, \min_{j \in [\tilde{q}]} \epsilon_j)$ and $\tilde{\xi} = \epsilon\xi$, we conclude $\alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \tilde{\xi} + \frac{\beta(\boldsymbol{\theta})}{2} \left\|\tilde{\xi}\right\|^2 < 0$, for all $j \in [\tilde{q}]$, and hence Slater's condition holds for (11.3). Since (11.3) is convex, this means that $\mathcal{R}_{\alpha,\beta}$ satisfies the KKT equations associated to (11.3). Hence,

$$\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) + \nabla V_0(\boldsymbol{\theta}) + \sum_{j=1}^{\tilde{q}} u_j(\boldsymbol{\theta}) \Big(\nabla V_i(\boldsymbol{\theta}) + \beta(\boldsymbol{\theta}) \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) \Big) = 0,$$

from where the expression (11.5) follows. □

The next result provides conditions under which (11.3) is feasible and locally Lipschitz.

Lemma 11.2.2. (Feasibility and Lipschitzness): *Suppose that Assumption 10 holds. Then,*

(1) under Assumption 11, $\mathcal{R}_{\alpha,\beta}$ is well-defined and locally Lipschitz on an open neighborhood containing $\mathcal{C}$;

(2) under Assumptions 11 and 12, $\mathcal{R}_{\alpha,\beta}$ is well-defined and locally Lipschitz on $\mathbb{R}^d$.

Proof. 1: By the argument employed in the proof of Lemma 11.2.1, Slater's condition holds for (11.3) at any $\boldsymbol{\theta} \in \mathcal{C}$. This means that there exists $\xi \in \mathbb{R}^d$ such that $\alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \xi + \frac{\beta(\boldsymbol{\theta})}{2} \|\xi\|^2 < 0$ for all $j \in [q]$. Since $V_j, \nabla V_j$ and β are continuous, there exists a neighborhood $U_{\boldsymbol{\theta}}$ of $\boldsymbol{\theta}$ such that $\alpha V_j(\bar{\boldsymbol{\theta}}) + \nabla V_j(\bar{\boldsymbol{\theta}})^\top \xi + \frac{\beta(\bar{\boldsymbol{\theta}})}{2} \|\xi\|^2 < 0$ for all $\bar{\boldsymbol{\theta}} \in U_{\boldsymbol{\theta}}$. In particular, the constraints in the definition of $\mathcal{R}_{\alpha,\beta}$ are feasible at all points in $U_{\boldsymbol{\theta}}$ and hence $\mathcal{R}_{\alpha,\beta}$ is well-defined at all points in $U_{\boldsymbol{\theta}}$. Hence $\mathcal{R}_{\alpha,\beta}$ is well-defined in the open set $\cup_{\boldsymbol{\theta} \in \mathcal{C}} U_{\boldsymbol{\theta}}$ containing $\mathcal{C}$. Since SC implies MFCQ for convex problems [178, Proposition 5.39], the functions $V_0, \cdots, V_q$, and β are twice continuously differentiable, and for each $\theta \in \mathcal{C}$, (11.3) satisfies CRC at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$, $\mathcal{R}_{\alpha,\beta}$ is locally Lipschitz on an open neighborhood of $\mathcal{C}$, invoking [172, Theorem 3.6].

2: by assumption, for any $\boldsymbol{\theta} \in \mathbb{R}^d$, we have that Slater's condition holds for (11.3) and CRC holds at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$ for (11.3). Therefore, by [172, Theorem 3.6], $\mathcal{R}_{\alpha,\beta}$ is locally Lipschitz at $\boldsymbol{\theta}$. □

The local Lipschitzness of $\mathcal{R}_{\alpha,\beta}$ on a neighborhood of $\mathcal{C}$, cf. Lemma 11.2.21 (resp., in all of $\mathbb{R}^d$, cf. Lemma 11.2.22) ensures that (11.4) is well-defined and has a unique solution for any initial condition in a neighborhood of $\mathcal{C}$ (resp., in all of $\mathbb{R}^d$). We refer the reader to [8] for a survey of other conditions that guarantee local Lipschitzness of parametric optimization problems such as (11.3).

11.2.2 Equilibria, Forward Invariance, and Stability

Next we establish the equivalence between the equilibrium points of (11.4) and the KKT points of (11.2).

Proposition 11.2.3. (Equivalence between equilibria and KKT points): *Let* (11.3) *be feasible at* $\boldsymbol{\theta}^* \in \mathbb{R}^d$. *If* $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) = 0$, *then* $\boldsymbol{\theta}^* \in \mathcal{C}$. *If MFCQ holds for* (11.2) *at* $\boldsymbol{\theta}^* \in \mathbb{R}^d$, *then* $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) = 0$ *if and only if* $\boldsymbol{\theta}^*$ *is a KKT point of* (11.2).

Proof. If (11.3) is feasible at $\boldsymbol{\theta}^* \in \mathbb{R}^d$ and $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) = 0$, then $\alpha V_j(\boldsymbol{\theta}^*) + \nabla V_j(\boldsymbol{\theta}^*)^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) + \frac{\beta(\boldsymbol{\theta}^*)}{2} \left\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*)\right\|^2 = \alpha V_j(\boldsymbol{\theta}^*) \leq 0$, for all $j \in [\tilde{q}]$, and therefore $\boldsymbol{\theta}^* \in \mathcal{C}$. Next, suppose that MFCQ holds for (11.2) at $\boldsymbol{\theta}^* \in \mathbb{R}^d$ and $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) = 0$. As shown in the proof of Lemma 11.2.1(i), Slater's condition holds for (11.3). Hence, since $\mathcal{R}_{\alpha,\beta}$ is the local minimizer of the optimization problem (11.3), it satisfies the KKT equations for (11.3). Enforcing that the solution is $\xi = 0$, these read exactly as the KKT equations for (11.2). Since MFCQ holds for (11.2), it follows that $\boldsymbol{\theta}^*$ is a KKT point of (11.2). Conversely, if θ^* is a KKT point of (11.2), then there exist a Lagrange multiplier vector $u \in \mathbb{R}^{\tilde{q}}$ satisfying the KKT equations. Since the solution of (11.3) is unique because the problem is strongly convex, we conclude that $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}^*) = 0$. □

The next result shows that $\mathcal{C}$ is forward invariant under (11.4).

Proposition 11.2.4. (Safety of RSGF): *Suppose that Assumptions 10 and 11 hold. Then,* $\mathcal{C}$ *is forward invariant under* (11.4).

Proof. By Lemma 11.2.2(i), every solution of (11.4) with initial condition in $\mathcal{C}$ is unique and well-defined as long as it stays in a neighborhood of $\mathcal{C}$. Furthermore, due to the constraints in (11.3),

$$\nabla V_j(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) \leq -\alpha V_j(\boldsymbol{\theta}) - \frac{\beta(\boldsymbol{\theta})}{2} \left\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\right\|^2, \tag{11.6}$$

which implies that $\nabla V_j(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) \leq 0$ whenever $V_j(\boldsymbol{\theta}) = 0$, for all $i \in [\tilde{q}]$. The result then follows from Nagumo's Theorem [126]. □

The final result of this section characterizes the convergence properties of (11.4).

Proposition 11.2.5. (Convergence of RSGF): *Suppose that Assumptions 10 and 11 hold. Then,*

(1) every bounded trajectory of (11.4) *starting in* $\mathcal{C}$ *converges to the set of KKT points of* (11.2).

(2) if Assumption 12 holds, then every bounded trajectory of (11.4) *converges to the set of KKT points of* (11.2).

In either case, if every KKT point is isolated, convergence is to a point.

Proof. 1: From the proof of Lemma 11.2.1(i), we have that $\mathcal{R}_{\alpha,\beta}(\theta)$ satisfies the KKT equations for (11.3),

$$u_j(\boldsymbol{\theta})\big(\alpha V_j(\boldsymbol{\theta})+\nabla V_j(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})+\tfrac{\beta(\boldsymbol{\theta})}{2}\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\|^2\big)=0,$$
$$u_j(\boldsymbol{\theta})\geq 0,\ \alpha V_j(\theta)+\nabla V_j(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})+\tfrac{\beta(\boldsymbol{\theta})}{2}\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\|^2\leq 0.$$

Hence,

$$\begin{aligned}\frac{d}{dt}V_0(\theta) &= \nabla V_0(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) = \\ &-\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})^\top\Big(\big(1+\beta(\boldsymbol{\theta})\sum_{j=1}^q u_j(\boldsymbol{\theta})\big)\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})+\sum_{j=1}^q u_j(\boldsymbol{\theta})\nabla V_j(\boldsymbol{\theta})\Big)\\ &=-\Big(1+\tfrac{\beta(\boldsymbol{\theta})}{2}\sum_{j=1}^q u_j(\boldsymbol{\theta})\Big)\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\|^2+\sum_{j=1}^q \alpha u_j(\boldsymbol{\theta})V_j(\boldsymbol{\theta}),\end{aligned} \tag{11.7}$$

where in the second equality we have used (11.5) and in the third we have used the KKT equations above. Now, since $u_j(\boldsymbol{\theta})\geq 0$ for all $j\in[q]$, and $V_j(\boldsymbol{\theta})\leq 0$ for all $j\in[q]$ if $\boldsymbol{\theta}\in\mathcal{C}$, we deduce that $\frac{d}{dt}V_0(\boldsymbol{\theta})\leq 0$ for all $\boldsymbol{\theta}\in\mathcal{C}$, with equality if and only if $\boldsymbol{\theta}$ is a KKT point of (11.2) by Proposition 11.2.3. The fact that all bounded trajectories converge to the set of KKT points follows then from [124, Proposition 5.3] using V_0 as a LaSalle function. Convergence to a point when the KKT points are isolated follows from [124, Corollary 5.2].

2: Let $\epsilon>0$ and consider the function $V_{\epsilon_*}:\mathbb{R}^d\to\mathbb{R}$ defined by

$$V_{\epsilon_*}(\boldsymbol{\theta})=V_0(\boldsymbol{\theta})+\frac{1}{\epsilon_*}\sum_{j=1}^q[V_j(\boldsymbol{\theta})]_+.$$

From [236, Proposition 3], V_{ϵ_*} is directionally differentiable and its directional derivative in the direction $\xi\in\mathbb{R}^n$ is

$$\begin{aligned}V'_{\epsilon_*}(\boldsymbol{\theta};\xi)=\nabla V_0(\boldsymbol{\theta})^\top\xi&+\frac{1}{\epsilon_*}\sum_{j\in I_+(\boldsymbol{\theta})}\nabla V_j(\boldsymbol{\theta})^\top\xi\\ &+\frac{1}{\epsilon_*}\sum_{j\in I_0(\boldsymbol{\theta})}[\nabla V_j(\boldsymbol{\theta})^\top\xi]_+,\end{aligned} \tag{11.8}$$

where $I_0(\boldsymbol{\theta})$ and $I_+(\theta)$ correspond to the optimization problem (11.2). From the KKT equations above, we have that $\nabla V_j(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) \leq -\alpha V_j(\boldsymbol{\theta})$ for all $j \in [q]$. Using (11.7) in (11.8) for $\xi = \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})$, we have

$$V'_{\epsilon_*}(\boldsymbol{\theta}; \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})) \leq -\Big(1 + \tfrac{\beta(\boldsymbol{\theta})}{2} \sum_{j=1}^{q} u_j(\boldsymbol{\theta})\Big) \|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\|^2 + \sum_{j=1}^{q} \alpha u_j(\boldsymbol{\theta}) V_j(\boldsymbol{\theta}) - \frac{1}{\epsilon_*} \sum_{j \in I_+(\boldsymbol{\theta})} \alpha V_j(\boldsymbol{\theta}).$$

Now, by an argument analogous to [98, Lemma D.1], for any compact set Ω, there exists $B_\Omega > 0$ such that $u_j(\theta) \leq B_\Omega$ for all $j \in [\tilde{q}]$ and $\boldsymbol{\theta} \in \Omega$. Then, for $\epsilon \in (0, \frac{1}{B_\Omega})$, and since $u_j(\boldsymbol{\theta}) V_j(\boldsymbol{\theta}) \leq 0$ for all $j \in I_0(\boldsymbol{\theta}) \cup I_-(\theta)$, we have

$$V'_{\epsilon_*}(\boldsymbol{\theta}; \mathcal{R}_{\alpha,\beta}(\theta)) \leq -\Big(1 + \tfrac{\beta(\boldsymbol{\theta})}{2} \sum_{j=1}^{q} u_j(\boldsymbol{\theta})\Big) \|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})\|^2 \leq 0, \tag{11.9}$$

for all $\boldsymbol{\theta} \in \Omega$, where the last inequality is an equality if and only if $\boldsymbol{\theta}$ is a KKT point of (11.2) (cf. Proposition 11.2.3). Now the fact that all bounded trajectories in Ω converge to the set of KKT points of (11.2) follows from [124, Proposition 5.3] using V_{ϵ_*} as a LaSalle function. Convergence to a point when the KKT points are isolated follows from [124, Corollary 5.2]. □

Remark 11.2.6. (Boundedness of trajectories): Regarding Proposition 11.2.5(i), note that all trajectories of (11.4) starting in $\mathcal{C}$ remain in it by Proposition 11.2.4, and hence are bounded if this set is compact. Regarding Proposition 11.2.5(ii), if there is $i_* \in [\tilde{q}]$ and c such that $\Gamma = \{\boldsymbol{\theta} \in \mathbb{R}^d : V_{i_*}(\boldsymbol{\theta}) \leq c\}$ is compact, note that (11.6) implies that this set is forward invariant under (11.4). Therefore, all trajectories of (11.4) starting in Γ are bounded. In particular, this holds if V_{i_*} is radially unbounded, since all its sublevel sets are compact. •

Remark 11.2.7. (Robustness to error): The introduction of the strictly positive term β in the definition (11.3) strengthens the robustness against errors and disturbances of the robust safe gradient flow (as compared, for instance, with the safe gradient flow [98], which corresponds to $\beta \equiv 0$). An indication of this fact can be observed, for instance, in the contributions of the β term to the decrease of the LaSalle functions in the proof of Proposition 11.2.5, cf. (11.7) and (11.9). We quantify more precisely this robustness to model errors in Section 11.4 and exploit it to

handle imperfect knowledge of the functions $\{V_j\}_{j=0}^{\tilde{q}}$ and their gradients $\{\nabla V_j\}_{j=0}^{\tilde{q}}$ in the algorithm implementation. Interestingly, the use of quadratic constraints as in (11.3) has also been studied in the control barrier function literature [38, 12, 13] to robustify safe controllers against model uncertainty. •

Remark 11.2.8. (Discretization): We note that the forward-Euler discretization of (11.4) is equivalent to the discrete-time dynamics introduced in [3]. This follows by performing a change of variables ($\xi = \frac{y-\theta}{h}$ in the optimization problem (2) in [3], with the variables y and h as defined therein). This discrete-time dynamics is a special case of the Moving Balls Algorithm (MBA) [237]. Both [3] and [237] study the safety and convergence properties of the discrete-time dynamics directly, instead of their continuous-time counterpart (11.4), as we have done here. We leverage the latter in what follows the theory of stochastic approximation [233, 234]. •

11.3 Robust Safe Gradient Flow-Based Reinforcement Learning

In this section, we introduce our algorithmic solution to Problem 3. Consider the optimization problem (11.1) defining the optimal policy for the constrained Markov decision process $\mathcal{M}$. Instead of dealing directly with (11.1), we consider (11.2) with $\tilde{q} = q + 1$, and include the additional function $V_{q+1}(\boldsymbol{\theta}) = \|\boldsymbol{\theta}\|^2 - C$, where $C > 0$ is a design parameter. As we will justify later, this will have the effect of keeping the iterates of our proposed algorithm bounded.

Given $\alpha > 0$ and $\beta : \mathbb{R}^d \to \mathbb{R}_{>0}$, let $\mathcal{R}_{\alpha,\beta} : \mathbb{R}^d \to \mathbb{R}^d$ be defined by (11.3). To solve Problem 3, consider the forward-Euler discretization of the RSGF (11.4),

$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i + h_i \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i), \tag{11.10}$$

where $\{h_i\}_{i \in \mathbb{Z}_{>0}}$ is a sequence of stepsizes. Note that, since closed-from expressions for the value functions $V_0, \cdots, V_q$ are not readily available, one cannot directly implement this iteration. Instead, our strategy consists of relying on the robustness

properties of (11.10), when viewed as a discrete-time dynamical system, and employing estimates of $V_1, \cdots, V_q$, and $\nabla V_0, \cdots, \nabla V_q$ constructed with episodic data, as detailed next (note that V_{q+1} and ∇V_{q+1} are known and do not need to be estimated).

Episodic data available

Let Λ be a given set of policies for $\mathcal{M}$ and $\mathcal{I}_0$ a batch of episodes obtained offline with policies from Λ. Formally,

$$\mathcal{I}_0 = \{[s_0^n, a_0^n, s_1^n, a_1^n, \cdots, s_T^n, a_T^n, s_{T+1}^n]\}_{n \in [N_\zeta], \zeta \in \Lambda},$$

where N_ζ is the number of episodes obtained with policy ζ. Given $i \in \mathbb{Z}_{>0}$, let $\mathcal{I}_i$ be the collection of episodes at iteration i obtained using policy π_{θ_i}. Let $N_i = |\mathcal{I}_i|$ denote the number of episodes in $\mathcal{I}_i$.

At iteration i, we construct the estimates of the value functions and their gradients using episodes from $\cup_{j=0}^{i} \mathcal{I}_j$ as follows. Although one could potentially use all such episodes, for flexibility we assume that we only use a subset $\mathcal{J}_i \subset \cup_{j=0}^{i} \mathcal{I}_j$. We enumerate the episodes in $\mathcal{J}_i$ as

$$\mathcal{J}_i = \{[s_0^n, a_0^n, s_1^n, a_1^n, \cdots, s_T^n, a_T^n, s_{T+1}^n]\}_{n=1}^{|\mathcal{J}_i|}.$$

For each $n \in [|\mathcal{J}_i|]$, we denote by ζ_n the policy utilized to obtain the corresponding episode. We make the following assumption:

Assumption 13. *There exists $\nu > 0$ such that, for any $a \in \mathcal{A}$, $s \in \mathcal{S}$, $\boldsymbol{\theta} \in \mathbb{R}^d$ and $\zeta \in \Lambda$, it holds that $\pi_{\boldsymbol{\theta}}(a|s) > \nu$ and $\zeta(a|s) > \nu$.*

Assumption 13 is standard in the context of importance-sampling methods in RL [238, 239]. For any given state, it requires that any action has a positive probability lower bounded by ν for any policy in the parametric family $\{\pi_{\boldsymbol{\theta}}\}$ as well as in Λ.

Estimates of value functions and their gradients

For each $j \in [q] \cup \{0\}$, we consider the following estimate of the value function at iteration i,

$$\widehat{V}_j(\boldsymbol{\theta}_i) = \frac{\sigma_j}{|\mathcal{J}_i|}\left(\sum_{n=1}^{|\mathcal{J}_i|}\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\sum_{t=0}^{T}\gamma^t R_j(s_t^n, a_t^n, s_{t+1}^n)\right), \tag{11.11}$$

where $\sigma_0 = -1$, and $\sigma_j = 1$ for $j \in [q]$. Under Assumption 13, $\widehat{V}_j(\theta_i)$ is well defined, because the denominator in the ratio $\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}$ is strictly positive.

For any $a \in \mathcal{A}$ and $s \in \mathcal{S}$, define $\chi_{a,s} : \mathbb{R}^d \to \mathbb{R}$ as $\chi_{a,s}(\theta) = \log \pi_\theta(a|s)$. Note that $\chi_{a,s}$ is well-defined for all $\boldsymbol{\theta} \in \mathbb{R}^d$ under Assumption 13. Let $b : \mathcal{S} \to \mathbb{R}$ be a baseline function whose absolute value is bounded by $\hat{B} > 0$. For each $j \in [q] \cup \{0\}$, we consider the following estimates of the gradients of the value functions at iteration i,

$$\widehat{\nabla V_j}(\boldsymbol{\theta}_i) = \frac{\sigma_j}{|\mathcal{J}_i|}\left(\sum_{n=1}^{|\mathcal{J}_i|}\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\sum_{t=0}^{T}\gamma^t \nabla\chi_{a_t^n,s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n\right). \tag{11.12a}$$

where

$$D_{j,t}^n = \sum_{t'=t}^{T}\gamma^{t'-t} R_j(s_{t'}^n, a_{t'}^n, s_{t'+1}^n) - b(s_t^n). \tag{11.12b}$$

Under Assumption 13, $\widehat{\nabla V_j}(\boldsymbol{\theta}_i)$ is well defined.

Given these estimates, we define an approximated version of (11.3) as follows:

$$\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}) = \arg\min_{\xi\in\mathbb{R}^d}\frac{1}{2}\left\|\xi + \widehat{\nabla V_0}(\boldsymbol{\theta})\right\|^2 \tag{11.13a}$$

$$\text{s.t. } \alpha\widehat{V}_j(\boldsymbol{\theta}) + \widehat{\nabla V}_j(\boldsymbol{\theta})^\top\xi + \frac{\beta(\boldsymbol{\theta})}{2}\|\xi\|^2 \le 0,\ j \in [q], \tag{11.13b}$$

$$\alpha V_{q+1}(\boldsymbol{\theta}) + \nabla V_{q+1}(\boldsymbol{\theta})^\top\xi + \frac{\beta(\boldsymbol{\theta})}{2}\|\xi\|^2 \le 0. \tag{11.13c}$$

Note that this can be computed with the episodic data available to the agent.

Algorithm 3 presents the pseudocode for our proposal to solve Problem 3. We refer to it as Robust Safe Gradient Flow-based Reinforcement Learning (RSGF-RL).

In Algorithm 3, we do not detail a specific scheme to select the sets of episodes $\mathcal{J}_i$ from the available ones in $\cup_{j=0}^{i}\mathcal{I}_j$. Instead, in what follows, we study the properties of RSGF-RL for arbitrary sets $\mathcal{J}_i$ and provide conditions on these sets that guarantee a desired level of algorithmic performance.

Algorithm 3 RSGF-RL

Parameters: α, β, k, m, $\{h_i\}_{i=1}^k$ T, γ, $\mathcal{I}_0$, $\{N_i\}_{i=1}^k$

Initial Policy Parameter: $\boldsymbol{\theta}_1$

for $i \in [k]$ **do**

  Generate N_i episodes of length $T+1$ using π_{θ_i}

  Select the set $\mathcal{J}_i$ of episodes at iteration i

  Compute estimates $\{\widehat{V}_j(\boldsymbol{\theta}_i)\}_{j=0}^q$ using (11.11)

  Compute estimates $\{\widehat{\nabla V_j}(\boldsymbol{\theta}_i)\}_{j=0}^q$ using (11.12)

  Update policy according to

$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i + h_i \hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) \tag{11.14}$$

end for

return $\boldsymbol{\theta}_{k+1}$

11.4 Anytime Safety and Convergence Guarantees of RSGF-RL

In this section we present our technical analysis of RSGF-RL. We start by establishing different statistical properties of the value function and gradient estimates, and then characterize the safety and convergence properties of RSGF-RL.

11.4.1 Statistical Properties of Estimates

Here, we establish the statistical properties of the estimates (11.11) and (11.12) of the value functions and their gradients, resp. In our analysis, we make the following assumptions.

Assumption 14. (Boundedness of reward functions): *For each $j \in [q] \cup \{0\}$, there exist $B_j > 0$ such that $|R_j(s,a,s')| < B_j$, for all $s \in \mathcal{S}$, $a \in \mathcal{A}$, and $s' \in \mathcal{S}$.*

Assumption 15. (Differentiability and Lipschitzness of policy): *The function $\chi_{a,s}$*

is continuously differentiable and there exist $L > 0$ *and* $\tilde{B} > 0$ *such that*

$$\begin{aligned}\left\|\nabla\chi_{a,s}(\boldsymbol{\theta}) - \nabla\chi_{a,s}(\bar{\boldsymbol{\theta}})\right\| &\leq L\left\|\theta - \bar{\boldsymbol{\theta}}\right\|, \\ &\qquad \forall \boldsymbol{\theta}, \bar{\boldsymbol{\theta}} \in \mathbb{R}^d, a \in \mathcal{A}, s \in \mathcal{S}, \\ \left\|\nabla\chi_{a,s}(\boldsymbol{\theta})^{(l)}\right\| &\leq \tilde{B}, \ \forall \theta \in \mathbb{R}^d, l \in [d], a \in \mathcal{A}, s \in \mathcal{S}.\end{aligned}$$

Assumptions 14 and 15 are standard in the literature, cf. [235, 240]. By the Policy Gradient Theorem [241, Section 13.2], under Assumption 15, the functions $\{V_j\}_{j=0}^q$ in (11.1) are differentiable. Moreover, Lemma 11.6.1 ensures that, for all $j \in \{0\} \cup [q]$, ∇V_j is globally Lipschitz on $\mathbb{R}^d$ (we denote by L_j its Lipschitz constant). Additionally, we let $L_{q+1} = 2\sqrt{C}$ be the Lipschitz constant of V_{q+1} on $\theta = \{\theta \in \mathbb{R}^d : \|\theta\|^2 \leq C\}$.

In what follows, all expectations, variances and probabilities are taken with respect to $s_0 \sim \eta$, $a_t^n \sim \zeta_n(\cdot|s_t^n)$, for $t \in [T]$, and $n \in [|\mathcal{J}_i|]$. The following result characterizes the mean, variance, and probability of the tails of the value function estimates.

Proposition 11.4.1. (Value function estimates): *Suppose Assumptions 13 and 14 hold. Let* $i \in \mathbb{Z}_{>0}$ *and assume that* $\mathcal{J}_i$ *contains* $\bar{N}_i$ *episodes generated with* π_{θ_i} *(without loss of generality, we label them as the first* $\bar{N}_i$ *episodes in* $\mathcal{J}_i$*). Let*

$$\tilde{N}_i = |\mathcal{J}_i| - \bar{N}_i, \ \phi_j = \frac{B_j(1-\gamma^{T+1})}{1-\gamma}, \ \bar{\phi}_j = \frac{B_j(1-\gamma^{T+1})}{(1-\gamma)\nu^{T+1}}.$$

Then, for $j \in \{0\} \cup [q]$,

(1) $\mathbb{E}[\widehat{V}_j(\theta_i)] = V_j(\theta_i)$ *(unbiased function estimates);*

(2) $\mathrm{Var}[\widehat{V}_j(\boldsymbol{\theta}_i)] = \frac{\bar{N}_i\phi_j^2 + \tilde{N}_i\bar{\phi}_j^2}{|\mathcal{J}_i|^2}$*;*

(3) $\mathbb{P}(|\widehat{V}_j(\boldsymbol{\theta}_i) - V_j(\boldsymbol{\theta}_i)| \leq \epsilon) \geq 1 - 2\exp\big(-\frac{\epsilon^2|\mathcal{J}_i|^2}{2\bar{N}_i\phi_j^2 + 2\tilde{N}_i\bar{\phi}_j^2}\big)$.

Further assume that $\chi_{a,s}$ *is globally Lipschitz, uniformly in* a, s*, i.e., there exists* $\tilde{L} > 0$ *such that*

$$|\chi_{a,s}(\boldsymbol{\theta}) - \chi_{a,s}(\theta')| \leq \tilde{L}\left\|\boldsymbol{\theta} - \boldsymbol{\theta}'\right\|, \tag{11.15}$$

for all $\boldsymbol{\theta}, \boldsymbol{\theta}' \in \mathbb{R}^d$, $a \in \mathcal{A}$, *and* $s \in \mathcal{S}$, *and that the policies in* Λ *belong to* $\{\pi_{\boldsymbol{\theta}}\}$. *Let* $\{\bar{\boldsymbol{\theta}}_n\}_{n=1}^{|\mathcal{J}_i|}$ *denote the parameters that describe all the policies in* $\mathcal{J}_i$ *and define* $\tilde{\phi}_{i,j,n} = \phi_j \exp((T+1)\tilde{L}\left\|\boldsymbol{\theta}_i - \bar{\boldsymbol{\theta}}_n\right\|)$. *Then,*

(4) $\mathrm{VaR}[\widehat{V}_j(\boldsymbol{\theta}_i)] \leq \frac{\sum_{n=1}^{|\mathcal{J}_i|} \tilde{\phi}_{i,j,n}^2}{|\mathcal{J}_i|^2}$;

(5) $\mathbb{P}(|\widehat{V}_j(\boldsymbol{\theta}_i) - V_j(\boldsymbol{\theta}_i)| \leq \epsilon) \geq 1 - 2\exp\Big(-\frac{\epsilon^2|\mathcal{J}_i|^2}{2\sum_{n=1}^{|\mathcal{J}_i|}\tilde{\phi}_{i,j,n}^2}\Big)$.

Proof. 1: Let $d\Omega = \prod_{n=1}^{|\mathcal{J}_i|} ds_{T+1}^n \prod_{t=0}^{T} ds_t^n da_t^n$, where ds_t^n and da_t^n are the differential elements associated with the variables s_t^n and a_t^n, respectively. Define

$$E_{j,n} = \sum_{t'=0}^{T} \gamma^t R_j(s_t^n, a_t^n, s_{t+1}^n),$$
$$\Gamma = \mathcal{S}^{|\mathcal{J}_i|(T+2)} \times \mathcal{A}^{|\mathcal{J}_i|(T+1)},$$

for $j \in \{0\} \cup [q]$. Using (11.11), we have

$$\begin{aligned}\mathbb{E}[\widehat{V}_j(\boldsymbol{\theta}_i)] &= \frac{\sigma_j}{|\mathcal{J}_i|}\int_{\Gamma}\Bigg(\eta(s_0)\sum_{n=1}^{\bar{N}_i}\prod_{t=0}^{T}\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)E_{j,n} \\ &\qquad + \eta(s_0)\sum_{n=\bar{N}_i+1}^{|\mathcal{J}_i|}\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}E_{j,n}\zeta_n(a_t^n|s_t^n)\Bigg)d\Omega \\ &= \frac{1}{\bar{N}_i + \tilde{N}_i}(\bar{N}_i V_j(\boldsymbol{\theta}_i) + \tilde{N}_i V_j(\boldsymbol{\theta}_i)) = V_j(\boldsymbol{\theta}_i).\end{aligned}$$

2: By Assumption 13, $\zeta_n(a_t^n|s_t^n) > \nu$ for all $n \in [|\mathcal{J}_i|]$ and $t \in [T]$. This implies that, for each $n \in [\bar{N}_i : |\mathcal{J}_i|]$,

$$\left|\prod_{t=0}^{T}\frac{\pi_{\theta_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n, a_t^n, s_{t+1}^n)\right)\right| \leq B_j\frac{1-\gamma^{T+1}}{1-\gamma}\frac{1}{\nu^{T+1}} = \bar{\phi}_j \tag{11.16}$$

By Popovicius' inequality [242, Corollary 1], we have

$$\mathrm{VaR}\left[\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n, a_t^n, s_{t+1}^n)\right)\right] \leq \bar{\phi}_j^2.$$

Since the random variables

$$\left\{\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n, a_t^n, s_{t+1}^n)\right)\right\}_{n\in[\bar{N}_i:|\mathcal{J}_i|]}$$

are independent, it follows that

$$\mathrm{VaR}\left[\sum_{n=\bar{N}_i+1}^{|\mathcal{J}_i|}\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right)\right]\leq \tilde{N}_i\bar{\phi}_j^2.$$

On the other hand, note that

$$\left|\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right|\leq B_j\frac{1-\gamma^{T+1}}{1-\gamma}=\phi_j. \tag{11.17}$$

By Popovicius' inequality [242, Corollary 1],

$$\mathrm{VaR}\left[\sum_{\bar{n}=1}^{\bar{N}_i}\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right]\leq \bar{N}_i\phi_j^2,$$

from where the statement follows.

3: This follows from Hoeffding's inequality [243] using (11.16) and (11.17).

4: Under (11.15), we have

$$\frac{\pi_\theta(a|s)}{\pi_{\boldsymbol{\theta}'}(a|s)}\leq \exp\left(\tilde{L}\,\|\boldsymbol{\theta}-\boldsymbol{\theta}'\|\right),$$

for any $\boldsymbol{\theta},\boldsymbol{\theta}'\in\mathbb{R}^d$. Therefore,

$$\left|\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\pi_{\bar{\boldsymbol{\theta}}_n}(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right)\right| \leq B_j\frac{1-\gamma^{T+1}}{1-\gamma}\exp((T+1)\tilde{L}\left\|\boldsymbol{\theta}_i-\bar{\boldsymbol{\theta}}_n\right\|)=\tilde{\phi}_{i,j,n}. \tag{11.18}$$

By Popovicius' inequality [242, Corollary 1], this implies

$$\mathrm{VaR}\left[\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\pi_{\bar{\boldsymbol{\theta}}_n}(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right)\right]\leq\tilde{\phi}_{i,j,n}^2.$$

The result now follows by noting that the random variables

$$\left\{\prod_{t=0}^{T}\frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\pi_{\bar{\boldsymbol{\theta}}_n}(a_t^n|s_t^n)}\left(\sum_{t=0}^{T}\gamma^t R_j(s_t^n,a_t^n,s_{t+1}^n)\right)\right\}_{n\in[|\mathcal{J}_i|]}$$

are independent.

5: This follows from Hoeffding's inequality [243] using (11.18). □

In Proposition 11.4.1, the bounds in 4 and 5 derived under the additional assumption (11.15) are tighter than the ones derived in 2 and 3. This is because $\tilde{\phi}_{i,j,n}$, which appears in 4 and 5, depends on the difference between the policy parameters $\bar{\theta}_n$ and θ_i, so it takes advantage of their proximity. Instead, $\bar{\phi}_j$, which appears in 2 and 3, is insensitive to the proximity of the policy parameters to θ_i.

The next result states the same statistical properties for the gradients of the value functions.

Proposition 11.4.2. (Gradient of value function estimates): *Suppose Assumptions 13, 14, and 15 hold. Let $i \in \mathbb{Z}_{>0}$, $\bar{N}_i$ and $\tilde{N}_i$ as in Proposition 11.4.1, and*

$$\psi_j = \tilde{B} \sum_{t=0}^{T} \gamma^t \sum_{t'=t}^{T} (\gamma^{t'-t} B_j + \hat{B}),$$
$$\bar{\psi}_j = \frac{\tilde{B}}{\nu^{T+1}} \sum_{t=0}^{T} \gamma^t \sum_{t'=t}^{T} (\gamma^{t'-t} B_j + \hat{B}).$$

Then, for $j \in \{0\} \cup [q]$

(1) $\mathbb{E}[\widehat{\nabla V}_j(\boldsymbol{\theta}_i)] = \nabla V_j(\boldsymbol{\theta}_i)$ *(unbiased gradient estimates);*

(2) $\mathrm{VaR}[\widehat{\nabla V}_j(\boldsymbol{\theta}_i)^{(l)}] = \frac{\bar{N}_i \psi_j^2 + \tilde{N}_i \bar{\psi}_j^2}{|\mathcal{J}_i|^2}$, *for all $l \in [d]$;*

(3) $\mathbb{P}\big(\big\| \widehat{\nabla V}_j(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i) \big\| \le \epsilon \big) \ge 1 - 2d \exp\big(- \frac{\epsilon^2 |\mathcal{J}_i|^2}{2d(\bar{N}_i \psi_j^2 + \tilde{N}_i \bar{\psi}_j^2)} \big)$.

Further assume that $\chi_{a,s}$ is globally Lipschitz, uniformly in a, s, i.e., (11.15) *holds, and that the policies in Λ belong to $\{\pi_\theta\}$. Let $\{\bar{\boldsymbol{\theta}}_n\}_{n=1}^{|\mathcal{J}_i|}$ denote the parameters that describe all the policies in $\mathcal{J}_i$ and define $\tilde{\psi}_{i,j,n} = \exp((T+1)\tilde{L} \| \boldsymbol{\theta}_i - \bar{\boldsymbol{\theta}}_n \|) \psi_j$. Then,*

(4) $\mathrm{VaR}[\widehat{\nabla V}_j(\boldsymbol{\theta}_i)^{(l)}] \le \frac{\sum_{n=1}^{|\mathcal{J}_i|} \tilde{\psi}_{i,j,n}^2}{|\mathcal{J}_i|^2}$, *for all $l \in [d]$;*

(5) $\mathbb{P}\big(\big\| \widehat{\nabla V}_j(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i) \big\| \le \epsilon \big) \ge 1 - 2d \exp\big(- \frac{\epsilon^2 |\mathcal{J}_i|^2}{2 \sum_{n=1}^{|\mathcal{J}_i|} \tilde{\psi}_{i,j,n}^2} \big)$.

Proof. 1: Let $j \in [q] \cup \{0\}$. With the notation of (11.12), by the Policy Gradient Theorem with baseline (cf. [241, Section 13.4]), for each $n \in [\bar{N}_i]$, we have

$$\mathbb{E}\left[\sigma_j \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n \right] = \nabla V_j(\boldsymbol{\theta}_i).$$

On the other hand, for $n \in [\bar{N}_i : |\mathcal{J}_i|]$,

$$\begin{aligned}
&\mathbb{E}\left[\sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n\right] = \\
&\int_\Gamma \sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n \zeta_n(a_t^n|s_t^n) d\Omega \\
&= \int_\Gamma \sigma_j \eta(s_0) \prod_{t=0}^{T} \pi_{\theta_i}(a_t^n|s_t^n) \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\theta_i) D_{j,t}^n d\Omega \\
&= \nabla V_j(\boldsymbol{\theta}_i),
\end{aligned}$$

where $d\Omega$ and Γ are defined as in the proof of Proposition 11.4.1, and for the last equality we have also used the Policy Gradient Theorem with baseline (cf. [241, Section 13.4]). Therefore,

$$\mathbb{E}[\widehat{\nabla V}_j(\boldsymbol{\theta}_i)] = \frac{\bar{N}_i}{\bar{N}_i + \tilde{N}_i} \nabla V_j(\boldsymbol{\theta}_i) + \frac{\tilde{N}_i}{\bar{N}_i + \tilde{N}_i} \nabla V_j(\boldsymbol{\theta}_i) = \nabla V_j(\boldsymbol{\theta}_i).$$

2: Note that for each $l \in [d]$,

$$\begin{aligned}
&\left|\sigma_j \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i)^{(l)} \sum_{t'=t}^{T} \left(\gamma^{t'-t} R_j(s_{t'}^n, a_{t'}^n, s_{t'+1}^n) - b(s_t^n)\right)\right| \\
&\qquad \leq \tilde{B} \sum_{t=0}^{T} \gamma^t \sum_{t'=t}^{T} \left(\gamma^{t'-t} B_j + \hat{B}\right) = \psi_j. \quad (11.19)
\end{aligned}$$

By Popovicius' inequality [242, Corollary 1], this implies

$$\mathrm{VaR}\Big[\sigma_j \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i)^{(l)} D_{j,t}^n\Big] \leq \psi_j^2,$$

for $n \in [\bar{N}_i]$. On the other hand, for $n \in [\bar{N}_i : |\mathcal{J}_i|]$,

$$\begin{aligned}
&\left|\sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i)^{(l)} D_{j,t}^n\right| \leq \\
&\qquad \frac{\tilde{B}}{\nu^{T+1}} \sum_{t=0}^{T} \gamma^t \sum_{t'=t}^{T} \left(\gamma^{t'-t} B_j + \hat{B}\right) = \bar{\psi}_j. \quad (11.20)
\end{aligned}$$

Again, by Popoviciu's inequality [242, Corollary 1],

$$\mathrm{VaR}\left[\sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \frac{\partial}{\partial \boldsymbol{\theta}^{(l)}} \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n\right] \leq \bar{\psi}_j^2,$$

for $n \in [\bar{N}_i : |\mathcal{J}_i|]$. Since the random variables

$$\left\{ \sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\zeta_n(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \nabla \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i)^{(l)} D_{j,t}^n \right\}_{n \in [|\mathcal{J}_i|]}$$

are independent, it follows that

$$\mathrm{VaR}[\widehat{\nabla V_j}(\boldsymbol{\theta}_i)^{(l)}] \leq \frac{\bar{N}_i \psi_j^2 + \tilde{N}_i \bar{\psi}_j^2}{|\mathcal{J}_i|^2}, \quad \forall l \in [d].$$

3: From Hoeffding's inequality, using (11.19), (11.20), for any $\epsilon > 0$ and $l \in [d]$,

$$\mathbb{P}\Big(\Big| \widehat{\nabla V_j}(\boldsymbol{\theta}_i)^{(l)} - \nabla V_j(\boldsymbol{\theta}_i)^{(l)} \Big| \leq \frac{\epsilon}{\sqrt{d}} \Big) \geq 1 - 2\exp\Big\{ - \frac{\epsilon^2 |\mathcal{J}_i|^2}{2d\big(\bar{N}_i \psi_j^2 + 2\tilde{N}_i \bar{\psi}_j^2\big)} \Big\}.$$

Now, note that if $|\widehat{\nabla V_j}(\boldsymbol{\theta}_i)^{(l)} - \nabla V_j(\boldsymbol{\theta}_i)^{(l)}| \leq \frac{\epsilon}{\sqrt{d}}$ for all $l \in [d]$, then $\big\| \widehat{\nabla V_j}(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i) \big\| \leq \epsilon$, which means that

$$\mathbb{P}\Big(\big\| \widehat{\nabla V_q}(\boldsymbol{\theta}_i) - \nabla V_q(\boldsymbol{\theta}_i) \big\| \leq \epsilon \Big) \geq \mathbb{P}\Big(\bigcap_{l=1}^{d} \Big\{ |\widehat{\nabla V_q}(\boldsymbol{\theta}_i)^{(l)} - \nabla V_q(\boldsymbol{\theta}_i)^{(l)}| \leq \frac{\epsilon}{\sqrt{d}} \Big\} \Big).$$

Using Fréchet's Inequality [244],

$$\mathbb{P}\Big(\bigcap_{l=1}^{d} \Big\{ |\widehat{\nabla V_q}(\boldsymbol{\theta}_i)^{(l)} - \nabla V_q(\boldsymbol{\theta}_i)^{(l)}| \leq \frac{\epsilon}{\sqrt{d}} \Big\} \Big) \geq 1 - 2d\exp\Big\{ - \frac{\epsilon^2 |\mathcal{J}_i|^2}{2d\big(\bar{N}_i \psi_j^2 + \tilde{N}_i \bar{\psi}_j^2\big)} \Big\},$$

and the result follows.

4: Under the additional assumption (11.15), we have that for each $n \in [|\mathcal{J}_i|]$,

$$\left| \sigma_j \prod_{t=0}^{T} \frac{\pi_{\boldsymbol{\theta}_i}(a_t^n|s_t^n)}{\pi_{\bar{\theta}_n}(a_t^n|s_t^n)} \sum_{t=0}^{T} \gamma^t \frac{\partial}{\partial \boldsymbol{\theta}^{(l)}} \chi_{a_t^n, s_t^n}(\boldsymbol{\theta}_i) D_{j,t}^n \right| \leq \tag{11.21}$$

$$\tilde{B} \exp\Big\{ (T+1)\tilde{L} \big\| \boldsymbol{\theta}_i - \bar{\boldsymbol{\theta}}_n \big\| \Big\} \sum_{t=0}^{T} \gamma^t \sum_{t'=t}^{T} \Big(\gamma^{t'-t} B_j + \hat{B} \Big) = \tilde{\psi}_{i,j,n}.$$

Now the argument follows analogously to the one used in item 2.

5: This follows analogously to item 3 by using (11.21). □

Propositions 11.4.1 and 11.4.2 characterize the statistical properties of the estimates of the value functions and their gradients, generalizing to the on/off-policy case our previous result in [3, Lemma 2], which was limited to the on-policy case. These results show that, by increasing the number of episodes (either on-policy or off-policy) used, the distribution of the estimates of the value functions and their gradients concentrates around their true values, with the rate of concentration depending on the constants defined in Assumptions 13, 14, 15.

Remark 11.4.3. (Assumption on global Lipschitzness): Assumption (11.15) is standard in the literature (cf. [235, Assumption 3.1]). We note that, if the parameterized policy π_θ is globally Lipschitz uniformly in a and s, then (11.15) is satisfied. Indeed, using the Mean Value Theorem [245, Theorem 5.10], and under Assumption 13, we deduce

$$|\log \pi_{\boldsymbol{\theta}}(a|s) - \log \pi_{\boldsymbol{\theta}'}(a|s)| \leq \frac{1}{p^*}|\pi_{\boldsymbol{\theta}}(a|s) - \pi_{\boldsymbol{\theta}'}(a|s)|,$$

for some $p^* \in [\pi_{\boldsymbol{\theta}}(a|s), \pi_{\theta'}(a|s)]$. Note that such p^* is strictly positive because of Assumption 13. Hence, if π_θ is globally Lipschitz uniformly in a and s, it follows that (11.15) is satisfied. This is the case, for instance, for truncated Gaussian policies with compact state and action spaces (cf. [246, Section 6], [3, Section 5]). •

11.4.2 Safety Guarantees

In this section we study the safety guarantees of RSGF-RL.

Theorem 11.4.4. (Safety guarantees): *Suppose Assumptions 13, 14, and 15 hold. Let $i \in \mathbb{Z}_{>0}$, $\bar{N}_i$, $\tilde{N}_i$, ϕ_j, and $\bar{\phi}_j$ as in Proposition 11.4.1, and ψ_j, $\bar{\psi}_j$ as in Proposition 11.4.2. Suppose* (11.13) *is feasible at $\theta_i \in \mathbb{R}^d$ and that the stepsize satisfies*

$$h_i < \min\Big\{\frac{1}{\alpha}, \frac{\beta(\boldsymbol{\theta}_i)}{L_1}, \cdots, \frac{\beta(\boldsymbol{\theta}_i)}{L_q}, \frac{\beta(\boldsymbol{\theta}_i)}{L_{q+1}}\Big\}. \tag{11.22}$$

For $j \in [q]$, define

$$\hat{M}_{i,j} = \frac{-(1-\alpha h_i)\widehat{V}_j(\boldsymbol{\theta}_i) + \frac{h_i}{2}(\beta(\boldsymbol{\theta}_i) - L_j h_i)\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2}{1 + h_i\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|}.$$

Then, for any $\delta \in (0,1)$, under (11.14)

(1) if $\widehat{V}_j(\boldsymbol{\theta}_i) \leq 0$ and

$$\frac{|\mathcal{J}_i|^2}{\bar{N}_i\phi_j^2 + \tilde{N}_i\bar{\phi}_j^2} \geq -\frac{2}{\hat{M}_{i,j}^2}\log\frac{\delta}{2}, \tag{11.23a}$$

$$\frac{|\mathcal{J}_i|^2}{\bar{N}_i\psi_j^2 + \tilde{N}_i\bar{\psi}_j^2} \geq -\frac{2d}{\hat{M}_{i,j}^2}\log\frac{\delta}{2d}, \tag{11.23b}$$

then $\mathbb{P}(V_j(\boldsymbol{\theta}_{i+1}) \leq 0) \geq 1 - 2\delta$;

(2) if $\widehat{V}_j(\boldsymbol{\theta}_i) > 0$ *is such that* $\hat{M}_{i,j} > 0$*, and* (11.23) *holds, then,* $\mathbb{P}(V_j(\boldsymbol{\theta}_{i+1}) \leq 0) \geq 1 - 2\delta$*;*

(3) if for each $j \in [q]$ *such that* $\widehat{V}_j(\theta_i) > 0$*, it holds that* $\hat{M}_{i,j} > 0$*, and* (11.23) *holds for all* $j \in [q]$*, then* $\mathbb{P}(V_j(\boldsymbol{\theta}_{i+1}) \leq 0,\ \forall j \in [q]) \geq 1 - 2q\delta$*;*

(4) if $V_{q+1}(\boldsymbol{\theta}_i) \leq 0$*, then* $V_{q+1}(\boldsymbol{\theta}_{i+1}) \leq 0$*.*

Proof. 1: Since ∇V_j is Lipschitz with Lipschitz constant L_j, cf. Lemma 11.6.1, we invoke [247, Lemma 1.2.3] to deduce

$$V_j(\boldsymbol{\theta}_{i+1}) \leq V_j(\boldsymbol{\theta}_i) + \nabla V_j(\boldsymbol{\theta})^\top(\theta_{i+1} - \boldsymbol{\theta}_i) + \frac{L_j}{2}\left\|\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i\right\|^2. \tag{11.24}$$

This implies, using the Cauchy-Schwartz inequality, that

$$\begin{aligned} V_j(\boldsymbol{\theta}_{i+1}) \leq\ & V_j(\boldsymbol{\theta}_i) - \widehat{V}_j(\boldsymbol{\theta}_i) + \widehat{V}_j(\boldsymbol{\theta}_i) + \\ & \left\|\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V}_j(\boldsymbol{\theta}_i)\right\| \left\|\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i\right\| + \\ & \widehat{\nabla V}_j(\boldsymbol{\theta}_i)^\top(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \frac{L_j}{2}\left\|\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i\right\|^2. \end{aligned} \tag{11.25}$$

Since $\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i + h_i\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)$, and by using the constraints in (11.13), inequality (11.25) implies

$$\begin{aligned} V_j(\boldsymbol{\theta}_{i+1}) \leq\ & V_j(\boldsymbol{\theta}_i) - \widehat{V}_j(\boldsymbol{\theta}_i) + (1 - \alpha h_i)\widehat{V}_j(\boldsymbol{\theta}_i) + \\ & \left\|\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V}_j(\boldsymbol{\theta}_i)\right\| h_i\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i) \\ & - \frac{h_i}{2}(\beta(\boldsymbol{\theta}_i) - L_j h_i)\left\|\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2. \end{aligned} \tag{11.26}$$

Note that (11.22), together with the fact that $\widehat{V}_j(\boldsymbol{\theta}_i) \leq 0$, implies that $\hat{M}_{i,j} > 0$. Now, by Proposition 11.4.13, if $\frac{|\mathcal{J}_i|^2}{\bar{N}_i\phi_j^2 + \tilde{N}_i\bar{\phi}_j^2} \geq -\frac{2}{\hat{M}_{i,j}^2}\log\frac{\delta}{2}$, then $\mathbb{P}(|\widehat{V}_j(\boldsymbol{\theta}_i) - V_j(\boldsymbol{\theta}_i)| \leq \hat{M}_{i,j}) \geq 1 - \delta$. On the other hand, by Proposition 11.4.23, if $\frac{|\mathcal{J}_i|^2}{\bar{N}_i\psi_j^2 + \tilde{N}_i\bar{\psi}_j^2} \geq -\frac{2d}{\hat{M}_{i,j}^2}\log\frac{\delta}{2d}$, then $\mathbb{P}(\left\|\widehat{\nabla V}_j(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i)\right\| \leq \hat{M}_{i,j}) \geq 1 - \delta$. Using (11.26) and the definition of $\hat{M}_{i,j}$, we deduce that, if $|\widehat{V}_j(\boldsymbol{\theta}_i) - V_j(\boldsymbol{\theta}_i)| \leq \hat{M}_{i,j}$ and $\left\|\widehat{\nabla V}_j(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i)\right\| \leq \hat{M}_{i,j}$, then $V_j(\boldsymbol{\theta}_{i+1}) \leq 0$. Now, the result follows by Fréchet's inequality [244].

2: if $\hat{M}_{i,j} > 0$, $|\widehat{V}_j(\boldsymbol{\theta}_i) - V_j(\boldsymbol{\theta}_i)| \leq \hat{M}_{i,j}$, and $\left\|\widehat{\nabla V}_j(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i)\right\| \leq \hat{M}_{i,j}$, then $V_j(\boldsymbol{\theta}_{i+1}) \leq 0$, even if $\widehat{V}_j(\boldsymbol{\theta}_i) \geq 0$. The result follows by using a similar argument to 1.

3: this follows from 1, 2, and Fréchet's inequality [244].

4: this follows from employing (11.13c) in (11.24), combined with the hypothesis that $V_{q+1}(\boldsymbol{\theta}_i) \leq 0$. □

Theorem 11.4.41 shows that if the number of episodes utilized to estimate $V_j(\theta_i)$ is sufficiently large and $\widehat{V}_j(\theta_i) \leq 0$ (i.e., we estimate that the j-th safety constraint is satisfied at iteration i), then the next iterate of RSGF-RL satisfies the j-th safety constraint with arbitrarily high probability. Similarly, Theorem 11.4.42 provides such guarantees when $\widehat{V}_j(\boldsymbol{\theta}_i) \geq 0$ (i.e., we estimate that the j-th safety constraint is not satisfied at iteration i). We note that $\hat{M}_{i,j} > 0$ holds when $\widehat{V}_j(\boldsymbol{\theta}_i) \leq 0$ and $\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|$ is nonzero (which is a reasonable assumption if $\boldsymbol{\theta}_i$ is away from a KKT point). By continuity, this suggests that $\hat{M}_{i,j} > 0$ is also satisfied in a neighborhood of $\{\boldsymbol{\theta} \in \mathbb{R}^d : \widehat{V}_j(\boldsymbol{\theta}) \leq 0\}$ (again provided that $\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|$ is nonzero), and it becomes increasingly more difficult to satisfy with large $\widehat{V}_j(\theta_i)$. Intuitively, this means that safety can be ensured in the next iteration as long as safety violations in the current iteration are not too extreme.

Remark 11.4.5. (Feasibility): Since the estimates of the value functions and their estimates converge to their true values as the number of episodes increases, cf. Propositions 11.4.1 and 11.4.2, the requirement in Theorem 11.4.4 that (11.13) is feasible at θ_i is satisfied with high probability under Assumptions 11 and 12, cf. Lemma 11.2.2, provided that the number of episodes used in the estimates is sufficiently large. •

We state next a result that provides safety guarantees over a finite time horizon. Its proof follows from Theorem 11.4.4 and Fréchet's inequality [244]. We omit it for space reasons.

Corollary 11.4.6. (Safety guarantees over a finite time horizon): *Suppose Assumptions 13, 14 and 15 hold. Let $H \in \mathbb{Z}_{>0}$. If, for each $i \in [H]$, the assumptions in Theorem 11.4.43 hold, then under* (11.14),

$$\mathbb{P}\Big(\bigcap_{i=1}^{H+1} \{V_j(\boldsymbol{\theta}_i) \leq 0,\ \forall j \in [q]\} \Big) \geq 1 - 2qH\delta.$$

Corollary 11.4.6 provides conditions under which consecutive iterates of RSGF-RL probabilistically satisfy the constraints. Since δ is a design parameter, this guarantee can be ensured with arbitrarily high probability. Smaller values of δ, however, require a larger number of episodes, as reflected in (11.23).

11.4.3 Convergence Guarantees

In this section we provide convergence guarantees for RSGF-RL.

Theorem 11.4.7. (Almost sure convergence): *Suppose Assumptions 10, 11, 13, 14, 15 hold. Further suppose that:*

(1) $V_{q+1}(\boldsymbol{\theta}_0) \leq 0$*;*

(2) for all $\boldsymbol{\theta} \in \Theta \backslash \mathcal{C}$*, Slater's condition holds for* (11.3) *and CRC holds for* (11.3) *at* $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$*;*

(3) (11.13) *is feasible for all* $i \in \mathbb{Z}_{>0}$*;*

(4) $\lim_{i\to\infty} \left\| \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i) - \hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) \right\| = 0$ *with probability one;*

(5) $\lim_{i\to\infty} h_i = 0$, $\sum_{i=1}^{\infty} h_i = \infty$*;*

Then, under (11.14)*, the sequence* $\{\boldsymbol{\theta}_i\}_{i\in\mathbb{Z}_{>0}}$ *converges to the set of KKT points of* (11.1) *in* $\boldsymbol{\theta}$ *almost surely.*

Proof. Our proof proceeds by verifying that the hypotheses required by [233, Theorem 2.3.1] hold and then invoking this result. First, note that $\{\boldsymbol{\theta}_i\}_{i\in\mathbb{Z}_{>0}}$ is bounded with probability one. Indeed, since $V_{q+1}(\boldsymbol{\theta}_0) \leq 0$ by 1, it follows from 3 and Theorem 11.4.4(iv) that $V_{q+1}(\boldsymbol{\theta}_i) \leq 0$ for all $i \in \mathbb{Z}_{>0}$. This guarantees that $\|\boldsymbol{\theta}_i\| \leq \sqrt{C}$ for all $i \in \mathbb{Z}_{>0}$. Second, $\mathcal{R}_{\alpha,\beta}$ is continuous on θ. Indeed, $\mathcal{R}_{\alpha,\beta}$ is locally Lipschitz on $\mathcal{C}$ by Lemma 11.2.2 and, since for all $\boldsymbol{\theta} \in \Theta \backslash \mathcal{C}$, Slater's condition holds for (11.3) and CRC holds for (11.3) at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$, cf. 2, a similar argument to the one in the proof of Lemma 11.2.2 guarantees that $\mathcal{R}_{\alpha,\beta}$ is locally Lipschitz on $\Theta \backslash \mathcal{C}$. Third, the set of KKT points of (11.1) in Θ is globally asymptotically stable in Θ by

an argument analogous to that of Proposition 11.2.52. Furthermore, we write the dynamics as

$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i + h_i \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i) + h_i(\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) - \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i)).$$

Note that the noise sequence $\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) - \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}_i)$ is asymptotically vanishing with probability one, cf. 4 and the stepsize sequence satisfies $\lim_{i\to\infty} h_i = 0$, $\sum_{i=1}^{\infty} h_i = \infty$, cf. 5. Finally, taking the sequence $\{\xi_n\}$ in the notation of [233, Theorem 2.3.1] equal to zero, we conclude that the sequence $\{\theta_i\}_{i\in\mathbb{Z}_{>0}}$ converges to the set of KKT points in Θ almost surely. □

Remark 11.4.8. (Assumptions in Theorem 11.4.7): Requirement 1 on the initial policy estimate and 2 on constraint qualification conditions are reasonable, given our discussion above. The feasibility requirement in 3 follows in the setting considered in Remark 11.4.5. Regarding requirement 4, we note that, by the same argument as in Lemma 11.2.2, the function $\hat{\xi} : \mathbb{R}^{d(2\tilde{q}+1)+1} \to \mathbb{R}^d$ defined as

$$\begin{aligned} \hat{\xi}(\{A_j\}_{j=1}^{\tilde{q}}, \{B_j\}_{j=0}^{\tilde{q}}, C) = \arg\min_{\xi\in\mathbb{R}^d} \|\xi + B_0\|^2 \\ \text{s.t. } A_j + B_j^\top \xi + \frac{C}{2}\|\xi\|^2 \leq 0,\ j \in [\tilde{q}], \end{aligned} \tag{11.27}$$

is locally Lipschitz. This means that small perturbations in $\{\nabla V_j\}_{j=1}^{\tilde{q}}$ and $\{V_j\}_{j=1}^{\tilde{q}}$ (like the ones obtained from using estimates of such quantities) result in small perturbations in $\mathcal{R}_{\alpha,\beta}$. In particular, this implies that, for $\bar{\epsilon} > 0$, there exists $\bar{\delta}$ such that, if $\left\|\widehat{\nabla V_j}(\theta) - \nabla V_j(\theta)\right\| < \bar{\delta}$ for all $j \in [q] \cup \{0\}$ and $\left\|\hat{V}_j(\theta) - V_j(\theta)\right\| < \bar{\delta}$ for all $j \in [q]$, then $\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\theta) - \mathcal{R}_{\alpha,\beta}(\theta)\right\| < \bar{\epsilon}$. Since the estimates of the value functions and their gradients become arbitrarily close to their true values if a sufficiently large number of episodes is used (cf. Propositions 11.4.1 and 11.4.2), this means that the condition $\lim_{i\to\infty} \left\|\mathcal{R}_{\alpha,\beta}(\theta_i) - \hat{\mathcal{R}}_{\alpha,\beta}(\theta_i)\right\| = 0$ is satisfied if the number of episodes used to create the estimates of the value functions and their gradients increases as the number of iterations increases. Finally, an example of a stepsize sequence verifying 5 is $h_i = \frac{1}{i}$. •

The following result complements the almost sure convergence established in Theorem 11.4.7 by providing a bound on the number of iterations required to

converge to a neighborhood of a KKT point. This finite iteration convergence result is based on ideas from [235, Theorem 4.3].

Theorem 11.4.9. (Finite iteration convergence): *Suppose that Assumptions 10, 11, 13, 14, 15 hold, that* (11.13) *is feasible at every* $\{\theta_i\}_{i\in\mathbb{Z}_{>0}}$*, and let* $h_i = \frac{1}{\alpha\sqrt{i}}$*. Assume* $\{\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\}_{i\in\mathbb{Z}_{>0}}$ *is uniformly bounded by* $\hat{\ell} > 0$*. Define*

$$\mathrm{It}_\epsilon = \min\{i \in \mathbb{Z}_{>0} : \inf_{0\le j\le i} \mathbb{E}\Big[\big\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_j)\big\|^2 \Big] \le \epsilon\}.$$

Further suppose there exists $\bar{\sigma} > 0$ *with* $\mathrm{Var}(\widehat{\nabla V_j}(\boldsymbol{\theta}_i)^{(l)}) \le \bar{\sigma}$ *for all* $i \in [\mathrm{It}_\epsilon]$*,* $j \in \{0\} \cup [q]$*, and* $l \in [d]$*. If* $\epsilon - \hat{\ell}\bar{\sigma}(q+1) > 0$*, then there exists* $\kappa > 0$ *such that*

$$\mathrm{It}_\epsilon \le \Big(\frac{\kappa}{\epsilon - \hat{\ell}\bar{\sigma}(q+1)}\Big)^2.$$

Proof. Using (11.24), we deduce

$$\begin{aligned} V_j(\boldsymbol{\theta}_{i+1}) \le V_j(\boldsymbol{\theta}_i) + (\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}))^\intercal(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \\ \widehat{\nabla V_j}(\boldsymbol{\theta})^\intercal(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \frac{L_j\hat{\ell}^2 h_i^2}{2}, \end{aligned} \tag{11.28}$$

for all $j \in \{0\} \cup [q]$. Define $J_+^i = \{j \in [q] : \widehat{V}_j(\boldsymbol{\theta}_i) \ge 0\}$. For $\epsilon_* > 0$, let

$$V_{\epsilon_*}^i = \widehat{V}_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*}\sum_{j\in J_+^i} \widehat{V}_j(\boldsymbol{\theta}_i).$$

Equivalently,

$$\begin{aligned} V_{\epsilon_*}^{i+1} \le \widehat{V}_0(\boldsymbol{\theta}_{i+1}) - V_0(\boldsymbol{\theta}_{i+1}) + \frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}} \big(\widehat{V}_j(\boldsymbol{\theta}_{i+1}) - V_j(\boldsymbol{\theta}_{i+1})\big) \\ + V_0(\boldsymbol{\theta}_{i+1}) + \frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}} V_j(\boldsymbol{\theta}_{i+1}) \end{aligned}$$

Using (11.28), we have

$$
\begin{aligned}
V_{\epsilon_*}^{i+1} \leq\ & \widehat{V}_0(\boldsymbol{\theta}_{i+1}) - V_0(\boldsymbol{\theta}_{i+1}) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \left(\widehat{V}_j(\boldsymbol{\theta}_{i+1}) - V_j(\boldsymbol{\theta}_{i+1}) \right) \\
& + V_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} V_j(\boldsymbol{\theta}_i) \\
& + (\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i))^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} (\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i))^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \widehat{\nabla V_0}(\boldsymbol{\theta}_i)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \widehat{\nabla V_j}(\boldsymbol{\theta}_i)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \left(\frac{L_0}{2} + \frac{\sum_{j=1}^q L_j}{2\epsilon_*} \right) \hat{\ell} h_i^2. \qquad (11.29)
\end{aligned}
$$

Equivalently,

$$
\begin{aligned}
V_{\epsilon_*}^{i+1} \leq\ & \widehat{V}_0(\boldsymbol{\theta}_{i+1}) - V_0(\boldsymbol{\theta}_{i+1}) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \left(\widehat{V}_j(\boldsymbol{\theta}_{i+1}) - V_j(\boldsymbol{\theta}_{i+1}) \right) \\
& + V_0(\boldsymbol{\theta}_i) - \widehat{V}_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} (V_j(\boldsymbol{\theta}_i) - \widehat{V}_j(\boldsymbol{\theta}_i)) \\
& + \widehat{V}_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1} \cap J_+^i} \widehat{V}_j(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1} \setminus J_+^i} \widehat{V}_j(\boldsymbol{\theta}_i) \\
& + (\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i))^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} (\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i))^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \\
& \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} (\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i))^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \widehat{\nabla V_0}(\boldsymbol{\theta}_i)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \widehat{\nabla V_j}(\boldsymbol{\theta}_i)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\
& + \left(\frac{L_0}{2} + \frac{\sum_{j=1}^q L_j}{2\epsilon_*} \right) \hat{\ell} h_i^2. \qquad (11.30)
\end{aligned}
$$

Using an argument analogous to the one in the proof of Proposition 11.2.51 to obtain equation (11.7), but now with the estimates and the definition (11.13) of

the approximated RSGF, one can derive, for all $i \in \mathbb{Z}_{>0}$,

$$\begin{aligned}\widehat{\nabla V}_0(\boldsymbol{\theta}_i)^\top \hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) &= -\Big(1 + \frac{\beta(\boldsymbol{\theta}_i)}{2} \sum_{j=1}^{q} \hat{u}_i(\boldsymbol{\theta}_i)\Big) \left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2 \\ &+ \sum_{j=1}^{q} \alpha \hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i) \leq -\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2 + \sum_{j=1}^{q} \alpha \hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i), \end{aligned} \tag{11.31}$$

where $\hat{u}_j(\boldsymbol{\theta})$ denotes the Lagrange multiplier associated to constraint j in (11.13). Furthermore, from the constraints in (11.13),

$$\widehat{\nabla V}_j(\boldsymbol{\theta}_i)^\top \hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i) \leq -\alpha \widehat{V}_j(\boldsymbol{\theta}_i), \tag{11.32}$$

for all $j \in [q]$. Substituting (11.31) and (11.32) into (11.30), we get

$$\begin{aligned} V_{\epsilon_*}^{i+1} \leq\ & \widehat{V}_0(\theta_{i+1}) - V_0(\boldsymbol{\theta}_{i+1}) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \left(\widehat{V}_j(\theta_{i+1}) - V_j(\boldsymbol{\theta}_{i+1})\right) \\ &+ V_0(\boldsymbol{\theta}_i) - \widehat{V}_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \left(V_j(\boldsymbol{\theta}_i) - \widehat{V}_j(\boldsymbol{\theta}_i)\right) \\ &+ \widehat{V}_0(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1} \cap J_+^i} \widehat{V}_j(\boldsymbol{\theta}_i) + \frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1} \setminus J_+^i} \widehat{V}_j(\boldsymbol{\theta}_i) \\ &+ \left(\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i)\right)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\ &\frac{1}{\epsilon_*} \sum_{j \in J_+^{i+1}} \left(\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i)\right)^\top (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i) \\ &- h_i \left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2 + \sum_{j=1}^{q} \alpha h_i \hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i) \\ &- \sum_{j \in J_+^{i+1}} \alpha h_i \widehat{V}_j(\boldsymbol{\theta}_i) + \left(\frac{L_0}{2} + \frac{\sum_{j=1}^{q} L_j}{2\epsilon_*}\right) \hat{\ell} h_i^2. \end{aligned} \tag{11.33}$$

Now, since the iterates $\{\boldsymbol{\theta}_i\}_{i \in \mathbb{Z}_{>0}}$ remain bounded in θ, by an argument analogous to that of [98, Lemma D.1], there exists $B_L > 0$ such that $\hat{u}_j(\boldsymbol{\theta}_i) \leq B_L$ for all $j \in [q]$ and $i \in \mathbb{Z}_{>0}$. Take $\epsilon_* < \frac{1}{B_L}$. Since $\widehat{V}_j(\boldsymbol{\theta}_i) \leq 0$ for $j \notin J_+^i$, $\sum_{j=1}^{q} \alpha h_i \hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i) \leq$

$\sum_{j\in J_+^i}\widehat{V}_j(\boldsymbol{\theta}_i)$ and it follows that

$$\sum_{j=1}^{q}\alpha h_i\hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i)-\sum_{j\in J_+^{i+1}}\frac{\alpha h_i}{\epsilon_*}\widehat{V}_j(\boldsymbol{\theta}_i)\leq$$
$$\sum_{j\in J_+^{i}}\alpha h_i\hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i)-\sum_{j\in J_+^{i+1}}\frac{\alpha h_i}{\epsilon_*}\widehat{V}_j(\boldsymbol{\theta}_i)\leq$$
$$\sum_{j\in J_+^{i}\setminus J_+^{i+1}}\alpha h_i\hat{u}_j(\boldsymbol{\theta}_i)\widehat{V}_j(\boldsymbol{\theta}_i)-\sum_{j\in J_+^{i+1}\setminus J_+^{i}}\frac{\alpha h_i}{\epsilon_*}\widehat{V}_j(\boldsymbol{\theta}_i)\leq$$
$$\sum_{j\in J_+^{i}\setminus J_+^{i+1}}\frac{\alpha h_i}{\epsilon_*}\widehat{V}_j(\boldsymbol{\theta}_i)-\sum_{j\in J_+^{i+1}\setminus J_+^{i}}\frac{\alpha h_i}{\epsilon_*}\widehat{V}_j(\boldsymbol{\theta}_i). \tag{11.34}$$

Using the fact that $\sum_{j\in J_+^i\setminus J_+^{i+1}}\frac{\widehat{V}_j(\boldsymbol{\theta}_i)}{\epsilon_*}+\sum_{j\in J_+^i\cap J_+^{i+1}}\frac{\widehat{V}_j(\boldsymbol{\theta}_i)}{\epsilon_*}=\sum_{j\in J_+^i}\frac{\widehat{V}_j(\boldsymbol{\theta}_i)}{\epsilon_*}$ along with (11.34) and $\alpha h_i<1$, we get

$$\begin{aligned}V_{\epsilon_*}^{i+1}\leq\widehat{V}_0(\theta_{i+1})-V_0(\theta_{i+1})+\frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}}\left(\widehat{V}_j(\boldsymbol{\theta}_{i+1})-V_j(\boldsymbol{\theta}_{i+1})\right)\\+V_0(\boldsymbol{\theta}_i)-\widehat{V}_0(\boldsymbol{\theta}_i)+\frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}}(V_j(\boldsymbol{\theta}_i)-\widehat{V}_j(\boldsymbol{\theta}_i))\\+\widehat{V}_0(\boldsymbol{\theta}_i)+\frac{1}{\epsilon_*}\sum_{j\in J_+^{i}}\widehat{V}_j(\boldsymbol{\theta}_i)\\+(\nabla V_0(\boldsymbol{\theta}_i)-\widehat{\nabla V_0}(\boldsymbol{\theta}_i))^\top(\boldsymbol{\theta}_{i+1}-\boldsymbol{\theta}_i)+\\\frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}}(\nabla V_j(\boldsymbol{\theta}_i)-\widehat{\nabla V_j}(\boldsymbol{\theta}_i))^\top(\boldsymbol{\theta}_{i+1}-\boldsymbol{\theta}_i)\\-h_i\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2+\left(\frac{L_0}{2}+\frac{\sum_{j=1}^q L_j}{2\epsilon_*}\right)\hat{\ell}h_i^2.\end{aligned}\tag{11.35}$$

Let $\mathcal{F}_i$ be the sigma-algebra generated by the random variables

$$(\{\boldsymbol{\theta}_j\}_{j\in[i]},\mathcal{I}_0,\{\mathcal{J}_j\}_{j\in[i-1]}).$$

Taking expectations on both sides of (11.33) conditioned to $\mathcal{F}_i$, we get

$$\begin{aligned}\mathbb{E}[V_{\epsilon_*}^{i+1}|\mathcal{F}_i]\leq V_{\epsilon_*}^i-h_i\mathbb{E}[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2|\mathcal{F}_i]\\+\mathbb{E}[(\widehat{\nabla V_0}(\boldsymbol{\theta}_i)-\nabla V_0(\boldsymbol{\theta}_i))^\top(\boldsymbol{\theta}_{i+1}-\boldsymbol{\theta}_i)|\mathcal{F}_i]\\+\mathbb{E}[\frac{1}{\epsilon_*}\sum_{j\in J_+^{i+1}}(\widehat{\nabla V_j}(\boldsymbol{\theta}_i)-\nabla V_j(\boldsymbol{\theta}_i))^\top(\boldsymbol{\theta}_{i+1}-\boldsymbol{\theta}_i)|\mathcal{F}_i]\\+\Big(\frac{L_0}{2}+\frac{\sum_{j=1}^q L_j}{2\epsilon_*}\Big)\hat{\ell}h_i^2,\end{aligned}\tag{11.36}$$

where we have used the fact that $V_j(\boldsymbol{\theta}_i) \leq 0$ for $j \notin J_+^i$ and $\alpha h_i < 1$. Let V_* be such that $V_{\epsilon_*}^i \geq V_*$ for all $i \in \mathbb{Z}_{>0}$ (note that such value exists because the value function estimates are uniformly bounded as shown in the proof of Theorem 11.4.4). Define $U_i = V_{\epsilon_*}^i - V_*$ and $L_* = \frac{L_0}{2} + \frac{\sum_{j=1}^q L_j}{2\epsilon_*}$. Summing (11.36) for $i \in [\mathrm{It}_\epsilon]$,

$$\begin{aligned}\sum_{i=1}^{\mathrm{It}_\epsilon} \mathbb{E}\big[\big\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\big\|^2\big] &\leq \sum_{i=1}^{\mathrm{It}_\epsilon} \frac{\mathbb{E}[U_i]}{h_i} - \frac{\mathbb{E}[U_{i+1}]}{h_i} \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} L_* \hat{\ell} h_i + \sum_{i=1}^{\mathrm{It}_\epsilon} \frac{\mathbb{E}[(\theta_{i+1} - \theta_i)^\intercal (\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i))]}{h_i} \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} \sum_{j \in J_+^{i+1}} \frac{\mathbb{E}[(\widehat{\nabla V_j}(\boldsymbol{\theta}_i) - \nabla V_j(\boldsymbol{\theta}_i))^\intercal (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)]}{h_i}.\end{aligned}$$

Equivalently,

$$\begin{aligned}\sum_{i=1}^{\mathrm{It}_\epsilon} \mathbb{E}\big[\big\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\big\|^2\big] &\leq \sum_{i=1}^{\mathrm{It}_\epsilon} \Big(\frac{1}{h_i} - \frac{1}{h_{i-1}}\Big)\mathbb{E}[U_i] + \sum_{i=1}^{\mathrm{It}_\epsilon} L_* \hat{\ell} h_i \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} \frac{\mathbb{E}[(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)^\intercal (\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i))]}{h_i} \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} \sum_{j \in J_+^{i+1}} \frac{\mathbb{E}[(\widehat{\nabla V_j}(\boldsymbol{\theta}_i) - \nabla V_j(\theta_i))^\intercal (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)]}{h_i}. \qquad (11.37)\end{aligned}$$

Since $\{U_i\}_{i \in \mathbb{Z}_{>0}}$ is uniformly upper bounded (cf. Proposition 11.4.1), by letting B_u be such that $|U_i| \leq B_u$ for all $i \in \mathbb{Z}_{>0}$, we have

$$\begin{aligned}&\sum_{i=1}^{\mathrm{It}_\epsilon} \mathbb{E}\big[\big\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\big\|^2\big] \leq \\ &\sum_{i=1}^{\mathrm{It}_\epsilon} \Big(\frac{1}{h_i} - \frac{1}{h_{i-1}}\Big) B_u + \frac{1}{h_{\mathrm{It}_\epsilon}} B_u + \sum_{i=1}^{k} L_* \hat{\ell} h_i \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} \frac{\mathbb{E}[(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)^\intercal (\nabla V_0(\boldsymbol{\theta}_i) - \widehat{\nabla V_0}(\boldsymbol{\theta}_i))]}{h_i} \\ &+ \sum_{i=1}^{\mathrm{It}_\epsilon} \sum_{j \in J_+^{i+1}} \frac{\mathbb{E}[(\widehat{\nabla V_j}(\boldsymbol{\theta}_i) - \nabla V_j(\theta_i))^\intercal (\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)]}{h_i}, \qquad (11.38)\end{aligned}$$

where we have also used that $\frac{1}{h_i} > \frac{1}{h_{i-1}}$ for all $i \in [K_\epsilon]$. By the Cauchy-Schwartz inequality,

$$\begin{aligned}&\mathbb{E}[(\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i)^\intercal (\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i))] \leq \\ &\qquad \sqrt{\mathbb{E}[\|\boldsymbol{\theta}_{i+1} - \boldsymbol{\theta}_i\|^2 \,|\mathcal{F}_i]} \sqrt{\mathbb{E}[\big\|\nabla V_j(\boldsymbol{\theta}_i) - \widehat{\nabla V_j}(\boldsymbol{\theta}_i)\big\|^2]},\end{aligned}$$

for all $j \in \{0\} \cup [q]$. Moreover, since $\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\| \leq \hat{\ell}$ for all $i \in \mathbb{Z}_{>0}$, and since $\max_{i\in[K_\epsilon]} \mathrm{Var}(\widehat{\nabla V_j}(\boldsymbol{\theta}_i)) \leq \bar{\sigma}$ for all $j \in \{0\} \cup [q]$, we have from (11.38) that

$$\frac{1}{\mathrm{It}_\epsilon}\sum_{i=1}^{\mathrm{It}_\epsilon}\mathbb{E}\big[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2\big] \leq \frac{B_u}{\sqrt{\mathrm{It}_\epsilon}h_{\mathrm{It}_\epsilon}} + \frac{\sum_{i=1}^{\mathrm{It}_\epsilon} L_*\hat{\ell}h_i}{\mathrm{It}_\epsilon} + \hat{\ell}\bar{\sigma}(q+1).$$

Using the fact that $\sum_{i=1}^{\mathrm{It}_\epsilon} i^{-a} \leq {\mathrm{It}_\epsilon}^{1-a} - 1$ (cf. [246, page 31]) for any $a \in (0,1)$, we obtain

$$\frac{1}{\mathrm{It}_\epsilon}\sum_{i=1}^{\mathrm{It}_\epsilon}\mathbb{E}\big[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2\big] \leq \frac{B_u\alpha}{\sqrt{\mathrm{It}_\epsilon}} + \frac{L_*\hat{\ell}}{\alpha}\Big(\frac{1}{\sqrt{\mathrm{It}_\epsilon}} - \frac{1}{\mathrm{It}_\epsilon}\Big) + \hat{\ell}\bar{\sigma}(q+1). \tag{11.39}$$

By definition of It_ϵ, $\mathbb{E}\big[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2\big] > \epsilon$, for all $i \in [\mathrm{It}_\epsilon - 1]$, and therefore from (11.39) by taking $\kappa = B_u\alpha + \frac{L_*\hat{\ell}}{\alpha}$,

$$\epsilon \leq \frac{1}{\mathrm{It}_\epsilon - 1}\sum_{i=1}^{\mathrm{It}_\epsilon - 1}\mathbb{E}\big[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_i)\right\|^2\big] \leq \frac{\kappa}{\sqrt{\mathrm{It}_\epsilon - 1}} + \hat{\ell}\bar{\sigma}(q+1),$$

from where the result follows. □

We note the result in Theorem 11.4.9 ensures the existence of $j \in [\mathrm{It}_\epsilon]$ such that $\mathbb{E}[\left\|\hat{\mathcal{R}}_{\alpha,\beta}(\boldsymbol{\theta}_j)\right\|^2] \leq \epsilon$, but does not imply that the convergence in expectation of the norm of $\hat{\mathcal{R}}_{\alpha,\beta}$ is monotonically decreasing. This is akin to the convergence results obtained for policy gradient methods (cf. [235, Theorem 4.3]). We also point out that the iteration number It_ϵ in Theorem 11.4.9 is defined in terms of $\hat{\mathcal{R}}_{\alpha,\beta}$, instead of $\mathcal{R}_{\alpha,\beta}$. As justified in Remark 11.4.8, by using a sufficiently large number of episodes when estimating the value functions and their gradients, $\hat{\mathcal{R}}_{\alpha,\beta}$ and $\mathcal{R}_{\alpha,\beta}$ can be made arbitrarily close at any point with high probability. This means that if the estimates of all policies obtained for $i \in [\mathrm{It}_\epsilon]$ are computed with a sufficiently large number of episodes, Theorem 11.4.9 provides a bound for the number of iterations needed to reach a KKT point with high probability.

Remark 11.4.10. (Assumptions in Theorem 11.4.9): The argument in the proof of Theorem 11.4.9 is valid for any sequence $h_i = \frac{i^{-a}}{\alpha}$ for $a \in (0,1)$, but by following an argument similar to that of [235, Theorem 4.3], the optimal rate is $a = 1/2$, which is the one adopted in the statement. Moreover, Proposition 11.4.2 provides a way to compute the number of episodes necessary to ensure that the condition

$\mathrm{Var}(\widehat{\nabla V_j}(\boldsymbol{\theta}_i)^{(l)}) \leq \bar{\sigma}$ is satisfied for all $j \in \{0\} \cup [q]$, $i \in [\mathrm{It}_\epsilon]$ and $l \in [d]$. Finally, since θ is compact, $\mathcal{R}_{\alpha,\beta}$ is bounded in θ. Hence, $\hat{\ell}$ exists provided that the value function and gradient estimates are taken so that $\left\|\mathcal{R}_{\alpha,\beta} - \hat{\mathcal{R}}_{\alpha,\beta}\right\|$ is bounded. This holds, for example, under the asymptotically vanishing noise assumption discussed in Remark 11.4.8. •

11.5 Simulations

Here we test RSGF-RL in two scenarios: a robot solving a navigation task in a 2D environment and a cart-pole system seeking to keep the pole upright by moving the cart. We compare its performance against other approaches[1] that also solve constrained Markov decision processes: the state-of-the-art constrained policy optimization (CPO) algorithm [248] and on-policy RSGF-RL [3].

Navigation 2D: We tested the algorithm in the Navigation 2D task with single integrator dynamics from our previous work [3]. The state space is given by $s = (x, y) \in \mathbb{R}^2$ representing the position of the agent and the action space is continuous, with $a \in [-5, 5]^2$ representing the velocity in the x and y directions. The goal is to reach a target point $s^* = (8, 8)$ while avoiding obstacles (cf. Figure 11.1).

The reward is set to $R_0(s, a) = -\|s - s^*\|$, and the constraint reward is defined as

$$R_1(s,a) = \begin{cases} \varepsilon(e^{d(s)} - 1), & \text{if } s \in \mathcal{C} \\ 1 - \varepsilon, & \text{otherwise} \end{cases} \tag{11.40}$$

with $\varepsilon = 0.01$ and $d(s)$ being the distance between s and the closest obstacle border. We use the same policy as in [3]. Figure 11.2 shows the performance and safety metrics of the RSGF-RL algorithm, comparing different training strategies: Constrained policy optimization (CPO) [248], on-policy RSGF-RL [3] and RSGF-RL using both on-policy and off-policy data. The training details and hyperparameters are summarized in Table 11.1. To make a fair comparison, all algorithms collected

[1]The interested reader can find in [3] a comparative analysis of on-policy RSGF-RL with primal-dual approaches [89, 90].

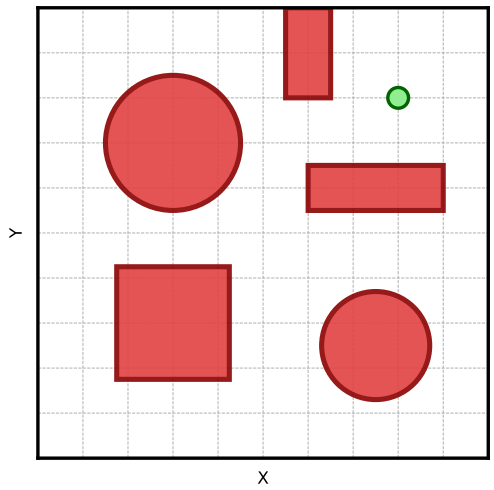


Figure 11.1: Navigation 2D environement. The green circle represents the target point, and obstacles are depicted in red.

the same amount of episodes per iteration ($N_i = 100$) and performed the same number of iterations ($k = 1500$). For the RSGF-RL algorithm, we used $|\mathcal{J}_i| = 2N_i = 200$ containing the $\bar{N}_i = 100$ episodes collected with the current policy (π_{θ_i}), and the $\tilde{N}_i = 100$ episodes from the previous iteration. In addition, to mitigate numerical errors during the training process we clip the values of the importance sampling weights between 0.8 and 1.2. Figure 11.2 shows the performance and safety metrics ($V_0(\theta)$ and $V_1(\theta)$, respectively) for the different training strategies. We can see that all our approaches outperform CPO, while remaining safe during the whole training procedure. Interestingly, the RSGF-RL algorithm without clipping the importance sampling weights performs similarly to the on-policy RSGF-RL algorithm, while the RSGF-RL with clipping significantly outperforms both approaches. This suggests that the off-policy data can improve the training process but introduces a high variance on the estimators that needs to be compensated by clipping or other variance reduction techniques.

Inverted Pendulum: We also evaluated RSGF-RL on the Gymnasium *Inverted Pendulum-v4* environment, where the objective is to learn a policy that keeps the pole upright by applying forces to the cart. The state is $s = (x, \theta, \dot{x}, \dot{\theta}) \in \mathbb{R}^4$, where x is the cart position, θ is the pole angle (relative to vertical), $\dot{x}$ is

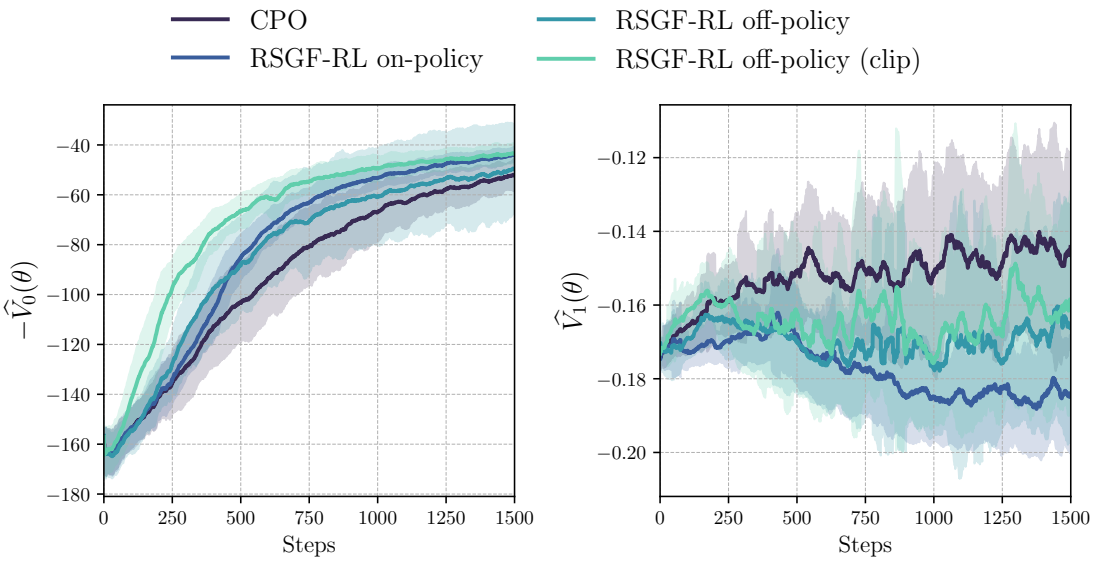


Figure 11.2: Comparison between different RSGF-RL training strategies in the Navigation 2D environment. Left plot shows the average $V(\theta)$ as a performance metric, while the right plot shows the average $V_1(\boldsymbol{\theta})$ as a safety metric.

the cart velocity, and $\dot{\theta}$ is the pole angular velocity. The action space is continuous, with $a \in [-3, 3]$ representing the force applied to the cart. The reward is $R_0(s, a) = 1$, encouraging the pole to remain upright as long as possible. The safe set is defined as $\mathcal{C} = \{s = [x, \theta, \dot{x}, \dot{\theta}] \in \mathbb{R}^4 : x < 0.5\}$, restricting the cart's position (Figure 11.3).

The constraint reward is defined as in (11.40), with $\varepsilon = 0.1$ and $d(s) = [1, 0, 0, 0]^\intercal s - 0.5$. We use a time horizon $T = 200$ and discount factor $\gamma = 0.995$. The policy is parameterized as in [3], using radial basis functions (RBFs) with centers uniformly distributed over $[-3, 3] \times [-\pi/4, \pi/4] \times [-1, 1] \times [-1.5, 1.5] \subset \mathcal{S}$, with ten divisions per dimension, resulting in 10^4 parameters. In this environment due to the high variance of the rewards, we selected the stepsize $h_i = \min\{0.1 \times 10^{-3}, 0.02/\|\hat{\mathcal{R}}_{\alpha,\beta}(\theta_i)\|\}$ such that the update norm is never higher than 0.02. Thirty episodes were run at each iteration ($N_i = 30$). In this case, instead of using the trajectories collected with prior policies we updated the policy twice using two minibaches of $|\mathcal{J}_i| = N_i/2$ episodes (steps 5-7 were run twice in algorithm 3). Figure 11.4 shows the performance and safety metrics ($V_0(\boldsymbol{\theta})$ and $V_1(\boldsymbol{\theta})$, respectively) for the different training algorithms. The training details and hyperparameters are summarized

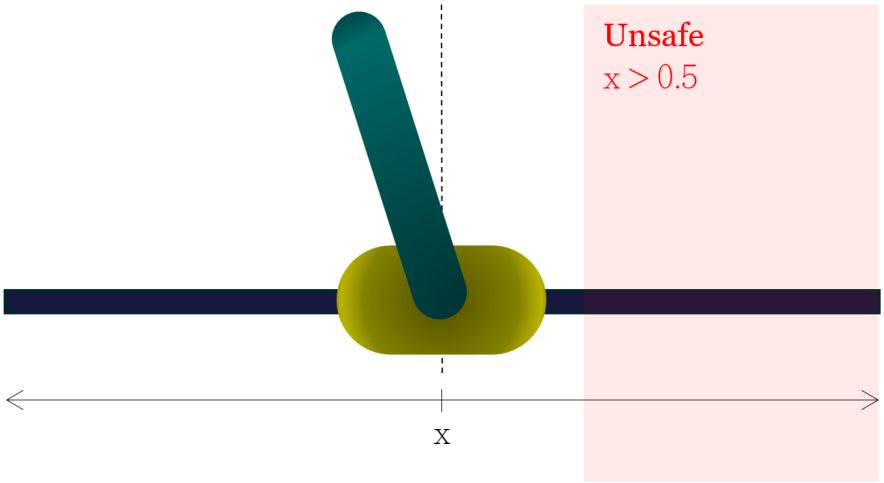


Figure 11.3: Inverted Pendulum environment. The red area represents the unsafe region, i.e., $x > 0.5$. The goal is to keep the pole upright while ensuring the cart remains within this safe region.

in table 11.2. In this environment all our approaches outperformed CPO even the on-policy algorithm RSGF-RL. However similarly to the navigation environment, the RSGF-RL algorithm when clippling the importance sampling weights is able to significatly outperform the other approaches. All approaches are able to maintain the safety constraint below 0.

11.6 Appendix

11.6.1 Lipschitz constants

Lemma 11.6.1. (Lipschitzness of gradient of value functions): *Suppose that Assumptions 14 and 15 hold. Let* $j \in [q] \cup \{0\}$. *Then,* ∇V_j *is Lipschitz with constant*

$$B_j L\Big(\frac{1-\gamma^T}{1-\gamma}\Big)^2 + 2B_j\tilde{B}^2\gamma\frac{1-(T+1)\gamma^T+T\gamma^{T+1}}{(1-\gamma)^2} + B_q\tilde{B}^2\Big(\frac{1-\gamma^T}{1-\gamma}\Big)^2.$$

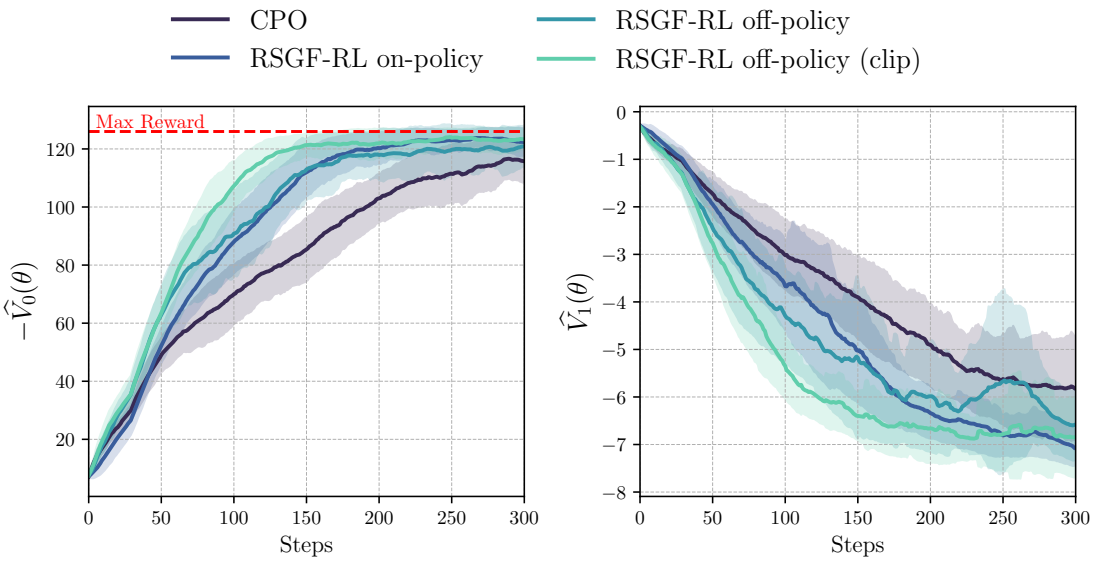


Figure 11.4: Performance comparison of anytime safe algorithms on the Inverted Pendulum environment. The left plot reports the average $V_0(\theta)$ (performance), and the right plot shows the average $V_1(\theta)$ (safety constraint). RSGF-RL (with and without clipping) is compared to CPO [2] and RSGF-RL [3].The shaded area represents the standard deviation over 5 seeds.

Proof. By the Policy Gradient Theorem [241, Section 13.2], for any $\boldsymbol{\theta} \in \mathbb{R}^d$,

$$\nabla V_j(\boldsymbol{\theta}) = \sum_{t=0}^{T}\sum_{\tau=0}^{T} \int_{\mathcal{I}} \gamma^{t+\tau} R_j(s_{t+\tau}, a_{t+\tau}, s_{t+\tau+1}) \nabla \chi_{a_t, s_t} p_{\boldsymbol{\theta}} d\sigma,$$

where $\mathcal{I} = \mathcal{S}^{T+1} \times \mathcal{A}^{T+1}$, $d\sigma = ds_0 ds_1 \cdots ds_T da_0 da_1 \cdots da_T$, and

$$p_{\boldsymbol{\theta}} = \left(\prod_{k=0}^{t+\tau} P(s_{k+1}, s_k, a_k) \right) \left(\prod_{k=0}^{t+\tau} \pi_{\boldsymbol{\theta}}(a_k | s_k) \right) \eta(s_0).$$

Now, by following the same steps as in the proof of [235, Lemma 3.2], it follows that

$$\begin{aligned} \|\nabla V_j(\boldsymbol{\theta}_1) - \nabla V_j(\boldsymbol{\theta}_2)\| \leq & \sum_{t=0}^{T}\sum_{\tau=0}^{T} \gamma^{t+\tau} B_j L \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\| + \\ & \sum_{t=0}^{T}\sum_{\tau=0}^{T} \gamma^{t+\tau} B_j \tilde{B}^2 (t+\tau+1) \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\| \end{aligned}$$

Now, by using the formulas

$$\sum_{t=0}^{T} \gamma^t = \frac{1-\gamma^T}{1-\gamma}, \quad \sum_{t=0}^{T} t\gamma^t = \gamma \frac{1-(T+1)\gamma^T + T\gamma^{T+1}}{(1-\gamma)^2},$$

we get

$$\begin{aligned}\|\nabla V_j(\boldsymbol{\theta}_1) - \nabla V_j(\boldsymbol{\theta}_2)\| \leq B_j L \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\| \Big(\frac{1-\gamma^T}{1-\gamma}\Big)^2 \\ + 2B_j \tilde{B}^2 \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\| \gamma \frac{1-(T+1)\gamma^T + T\gamma^{T+1}}{(1-\gamma)^2} \\ + B_j \tilde{B}^2 \|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\| \Big(\frac{1-\gamma^T}{1-\gamma}\Big)^2,\end{aligned}$$

from where the result follows. □

11.7 Slater's Condition

The following result provides a sufficient condition under which Slater's condition holds for (11.3) for each $\theta \in \mathbb{R}^d \backslash \mathcal{C}$.

Lemma 11.7.1. (Slater's condition): *Let $\delta : \mathbb{R}^d \to \mathbb{R}_+$ be a continuous function, and suppose that for each $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$, there exists $\xi \in \mathbb{R}^d$ that satisfies $\alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \xi < -\delta(\boldsymbol{\theta})$. Consider $\xi^* : \mathbb{R}^d \to \mathbb{R}^d$ defined as*

$$\begin{aligned}\xi^*(\boldsymbol{\theta}) = \arg\min_{\xi \in \mathbb{R}^d} \|\xi\|^2 \\ s.t.\ \alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \xi \leq 0,\ j \in [q].\end{aligned} \tag{11.41}$$

Select a differentiable function β such that

$$\frac{\beta(\boldsymbol{\theta})}{2} \left\|\xi^*(\{V_j(\boldsymbol{\theta}), \nabla V_j(\boldsymbol{\theta})\}_{j=1}^q)\right\| < \delta(\boldsymbol{\theta}).$$

Then, Slater's condition holds for (11.3) *for every $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$.*

Proof. Note that since (11.41) satisfies Slater's condition for all $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$, ξ^* is continuous at every $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$ [173, Theorem 5.3]. Therefore, a differentiable β as required in the statement exists. Now, it follows that $\xi^*(\{V_j(\boldsymbol{\theta}), \nabla V_j(\boldsymbol{\theta})\}_{j=1}^q)$ is strictly feasible for (11.3) for each $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$, from where the result follows. □

In particular, if δ is uniformly lower bounded by a positive constant and ξ^* is uniformly upper bounded, there exists a constant β function that makes Slater's condition hold for $\boldsymbol{\theta} \in \mathbb{R}^d \backslash \mathcal{C}$. We also note that the feasibility of the linear inequalities $\alpha V_j(\boldsymbol{\theta}) + \nabla V_j(\boldsymbol{\theta})^\top \xi < -\delta(\boldsymbol{\theta})$ can be verified using Farkas' Lemma [203,

Theorem 22.1]. Therefore, one can verify the feasibility of such linear inequalities and select an appropriate β to satisfy Slater's condition in $\mathbb{R}^d \backslash \mathcal{C}$.

The following result provides a condition under which the CRC holds for (11.3).

Lemma 11.7.2. (Constant rank condition): *Let $\tilde{q} = 1$, $\theta \in \mathcal{C}$ and suppose that* (11.2) *satisfies MFCQ. Then,* (11.3) *satisfies CRC at $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$.*

Proof. If the single constraint of (11.3) is not active, then CRC trivially holds. Suppose that it is active. The gradient with respect to ξ of the single constraint of (11.3) evaluated at $\xi = \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})$ is $g_{\boldsymbol{\theta}} = \nabla V_1(\boldsymbol{\theta}) + \beta(\boldsymbol{\theta})\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta})$. Note that if $g_{\boldsymbol{\theta}} \neq \mathbf{0}_d$, then there exists a neighborhood $\mathcal{N}$ of $(\boldsymbol{\theta}, \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}))$ such that if $(\bar{\boldsymbol{\theta}}, \bar{\xi}) \in \mathcal{N}$, then $\nabla V_1(\bar{\boldsymbol{\theta}}) + \beta(\bar{\boldsymbol{\theta}})\bar{\xi}$ has the same rank as $g_{\boldsymbol{\theta}}$. Alternatively, if $g_{\boldsymbol{\theta}} = 0$, then $0 = \alpha V_1(\boldsymbol{\theta}) + \nabla V_1(\boldsymbol{\theta})^\top \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) + \frac{\beta(\boldsymbol{\theta})}{2} \left\| \mathcal{R}\alpha, \beta(\boldsymbol{\theta}) \right\|^2 == \alpha V_1(\boldsymbol{\theta}) - \frac{\beta(\boldsymbol{\theta})}{2} \left\| \mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) \right\|^2$. This implies that $V_1(\boldsymbol{\theta}) = 0$ and $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) = \mathbf{0}_d$. Since MFCQ holds for (11.2) and $V_1(\boldsymbol{\theta}) = 0$, then $\nabla V_1(\boldsymbol{\theta}) \neq \mathbf{0}_d$ necessarily. However, since $\mathcal{R}_{\alpha,\beta}(\boldsymbol{\theta}) = \mathbf{0}_d$ this contradicts the fact that $g_{\boldsymbol{\theta}} = \mathbf{0}_d$. □

Next we state a few inequalities from probability theory that are useful throughout this paper.

Lemma 11.7.3. (Popoviciu's inequality [242, Corollary 1]): *Let X be a real-valued random variable. Suppose that there exist $m, M \in \mathbb{R}$ such that $m \leq X \leq M$ almost surely. Then, $Var(X) \leq \frac{(M-m)^2}{4}$.*

Lemma 11.7.4. (Hoeffding's inequality [243]): *Let $X_1, \cdots, X_n$ be independent random variables. Suppose that there exist $a_i, b_i \in \mathbb{R}$ for $i \in [n]$ such that $a_i \leq X_i \leq b_i$ almost surely. Let $S_n = X_1 + \cdots + X_n$. Then, for any $\epsilon > 0$,*

$$\mathbb{P}(|S_n - \mathbb{E}[S_n]| \geq \epsilon) \leq 2 \exp\Big(- \frac{2\epsilon^2}{\sum_{i=1}^n (b_i - a_i)^2} \Big).$$

Lemma 11.7.5. (Fréchet's Inequality [244]): *Let $\{A_i\}_{i=1}^n$ be $n \in \mathbb{Z}_{>0}$ events. Then,*

$$\mathbb{P}\Big(\bigcap_{i=1}^n A_i \Big) \geq \max\Big\{ 0, \sum_{i=1}^n \mathbb{P}(A_i) - (n-1) \Big\}.$$

11.7.1 Simulation's hyperparameters

Table 11.1: Hyperparameters the Navigation 2D environment

Parameter	**Value**
Environment	
Time horizon (T)	50
Discount factor (γ)	0.98
Reward (R_0)	$-\|\|s - s^*\|\|$
Constraint reward (R_1)	Eq. (11.40)
ε	0.01
Policy	
Type	Gaussian RBFs
Centers	$[0, 10]^2$
Number of centers	400
Policy variance σ	0.5
General	
Number of iterations (k)	1500
N_i	100
V_0 baseline ($b_0(s)$)	0
V_1 baseline ($b_1(s)$)	0
On-policy RSGF-RL	
Step size (h)	0.1
α	9
RSGF-RL	
Step size (h)	0.1
$\|\mathcal{J}_i\|$	200
updates per iteration (m)	1
α	9
β	1
CPO	
δ	0.1

Table 11.2: Hyperparameters the Inverted Pendulum environment

Parameter	**Value**
Environment	
Time horizon (T)	200
Discount factor (γ)	0.995
Reward (R_0)	1
Constraint reward (R_1)	Eq. (11.40)
Safety threshold	$x > 0.5$
ε	0.1
Policy	
Type	Gaussian RBFs
Centers	$[0, 10]^2$
Number of centers	1000
Policy variance σ	0.2
General	
Number of iterations (k)	300
N_i	30
V_0 baseline ($b_0(s)$)	neural network
V_1 baseline ($b_1(s)$)	neural network
On-policy RSGF-RL	
Step size (h)	10^-3
α	0.1
RSGF-RL	
Step size (h)	$\min\{10^{-3}, 0.02/\|\hat{\mathcal{R}}_{\alpha,\beta}\|\}$
$\|\mathcal{J}_i\|$	15
updates per iteration (m)	2
α	0.1
β	1
CPO	
δ	4×10^{-4}

Chapter 12

Conclusions

In this dissertation we have advanced the understanding of the design of autonomous systems in safety-critical scenarios through the use of CBFs.

12.1 Summary

12.1.1 Part I: Control Design with Safety and Stability Guarantees

In the first part of the dissertation we have considered the problem of designing controllers that achieve safe stabilization of known control affine systems.

In Chapter 3 we have designed an optimization with penalty-based controller that has one of the objectives as a hard constraint and the other as a soft constraint. The controller depends on a penalty parameter that can be tuned to enhance the soft objective at the cost of reduced optimality, while guaranteeing the satisfaction of the hard constraint. An advantage of the proposed design is that the controller is automatically Lipschitz and has a closed-form expression. Next we show that the controller can introduce undesired equilibrium points different from the origin. By choosing the penalty parameter appropriately, and under some technical conditions, these undesired equilibria can be eliminated. Finally, our third contribution shows that the proposed controller can be tuned to provide an inner approximation of the region of attraction of the origin for the closed-loop system. As a conse-

quence of this analysis, we have provided conditions under which all of the safe set belongs to the region of attraction of the origin for the closed-loop system.

In Chapter 4 we have turned our attention to studying the dynamical properties of CBF-based safety filters, paying special attention to the emergence of undesired behaviors. We have characterized the undesired equilibria that emerge in closed-loop systems and show that finding them is equivalent to solving an algebraic equation. We have studied the structure of the set of undesired equilibria and show that, in general, it can be a continuum but provide conditions under which the equilibria are isolated points. We have also shown that, in general, the trajectories of the closed-loop system can be unbounded and identify conditions under which the trajectories of the closed-loop system remain bounded. In the case of planar systems, we have provided conditions under which the closed-loop system does not contain any limit cycles and characterize the number of undesired equilibria and their stability properties. We have shown that in some cases, asymptotically stable undesired equilibria exist for any choice of stabilizing nominal controller. Finally, for the special case where the unsafe set is an ellipse, we have provided analytical expressions for the undesired equilibria and their stability properties. Our contributions highlight the intrincate relationship between the system dynamics, the geometry of the safe set, and the existence of undesired equilibria and their stability properties. They have also served as a cautionary note to practitioners, for whom we provide a variety of methods to tune (when possible) their controllers to avoid this plethora of undesirable behaviors.

In Chapter 5, we have introduced a variety of converse results regarding the existence of CBFs for the study of safety and safe stabilization of control systems. Speficially, we have provided an example that shows that for unbounded safe sets, there might be candidate CBFs (i.e., functions whose zero superlevel set is the safe set) which are not CBFs, and candidate CBFs which are. This is in contrast to the case of bounded safe sets, where all candidate CBFs are CBFs. Given a safe set, we have provided a set of general conditions on the dynamics and the safe set under which a CBF is guaranteed to exist. These conditions include safe sets for which there exists a safe controller such that trajectories of the closed-loop system

do not get arbitrarily close to the boundary of the safe set, or polynomial systems with polynomial safe set and safe feedback. We have also defined an extended notion of CBF, termed *extended control barrier function* (eCBF), which relies on a generalization of the notion of extended class $\mathcal{K}_\infty$ function and show that they are always guaranteed to exist for any given dynamics and safe set. Drawing on existing results in the literature, we provide a result that shows that if the unsafe set has a bounded connected component, there does not exist a CLBF or a strictly compatible CLF-CBF pair, and if the safe set is unbounded, there does not exist a CLBF. However, for a compact safe set, we show that if there exists a controller satisfying the CBF condition strictly and another controller that is stabilizing, the safe set admits a CLBF and a strictly compatible CLF-CBF pair. We have also shown that if the origin is safely stabilizing, under the same conditions that we can guarantee the existence of a CBF, we can also guarantee the existence of a compatible CLF-CBF pair.

In Chapter 6 we have provided an integrative presentation of insights and results about the regularity properties of optimization-based controllers, and their implication in different properties of interest of control systems.

Under appropriate constraint qualifications and conditions on the data that defines the optimization problem, we have shown that optimization-based controllers are locally Lipschitz, continuously differentiable, and even analytic. We have also characterized the properties enjoyed by parametric optimizers arising from optimization problems defined by second-order continuously differentiable objective function and constraints, strictly (or strongly) convex objective function, and feasible set with nonempty interior (the same properties as in Robinson's counterexample). We have shown that, even though such parametric optimizers might not be locally Lipschitz, they enjoy other important regularity properties, like point-Lipschitz continuity. Even if the optimization-based controller is discontinuous, under appropriate conditions on the optimization problem data, we have shown that it is measurable and locally bounded.

The results presented in this chapter show that the regularity properties of optimization-based controllers are determined by the smoothness/convexity and

constraint qualification properties of the optimization problems defining them. This opens the door to the possibility of designing optimization problems with the appropriate conditions and constraint qualification properties in order to endow the associated optimization-based controller with certain desired regularity properties.

12.1.2 Part II: Motion Planning using Safe and Stable Controllers

In the second part of the dissertation we have leveraged the safe and stable controllers studied in the first part to achieve safe navigation in robotic systems.

In Chapter 7 we have designed a distributed controller for safe navigation of multi-agent robotic systems. We have proposed a synthesis framework which leverages CBFs to formulate obstacle avoidance and inter-agent collision avoidance constraints as affine inequalities in the control input. These constraints are included in a state-dependent network optimization problem that finds the control inputs allowing the agents to reach different waypoints of interest while maintaining a given formation and satisfying the safety constraints.

Motivated by this problem, we have developed a distributed algorithm for anytime constrained optimization. We have shown that the separable structure permits the intoduction of auxiliary variables to reformulate the original problem into one with local constraints while still preserving the same solution set. However, this reformulation still does not allow to fully decouple the optimization problem into one per agent because the auxiliary variables require coordination. In order to sort this hurdle, our technical approach constructs a dynamical system by combining the use of projected saddle-point dynamics, which are distributed but not anytime, and the safe gradient flow, which is anytime but not distributed. First, we have established the well-posedness of the proposed dynamical system. Second, we have shown that it is distributed, exhibits the anytime property and is scalable.

We have leveraged such algorithm for distributed anytime constrained optimization to propose a controller design that is distributed, safe, and asymptotically converges to the solution of the state-dependent network optimization problem. We also implement the proposed controller in a variety of different environments,

robots and formations, both in simulation and in real hardware.

In Chapter 8 we consider the problem of designing motion planning algorithms that generate collision-free paths from an initial to a final destination for systems with control-affine dynamics. To ensure that the sequence of waypoints generated by the sampling-based algorithm can be tracked by a controller while ensuring safety and stability, we have leveraged the theory of CBFs and CLFs. First, we have introduced a result of independent interest which shows that the problem of verifying whether a CLF and a CBF are compatible in a set of interest can be solved by solving an optimization problem. Although in general such optimization problem is non-convex, we show that for linear systems and CBFs of polytopic or ellipsoidal obstacles, it reduces to a quadratically constrained quadratic program (QCQP), and for CBFs of circular obstacles it can be solved in closed form. Next, we have leveraged the results on compatibility checking of a CLF-CBF pair to develop Compatible CLF-CBF-RRT (or `C-CLF-CBF-RRT` for short), a sampling-based motion planning algorithm that is a variant of RRT. We show that, by construction, `C-CLF-CBF-RRT` generates collision-free paths that can be executed with a CLF-CBF-based controller, and formally establish it is probabilistically complete. We have illustrated our results in simulation and hardware experiments for differential drive robots and compare them with the literature, showing that `C-CLF-CBF-RRT` can generate safe and stable paths with a better average execution time.

12.1.3 Part III: Learning in Safety-Critical Systems under Uncertainty

In the third part of the dissertation we have studied the use of learning-based techniques to ensure safety, stability, and optimality in systems with uncertainty.

In Chapter 9 we have studied the problem of safe stabilization of control-affine systems under uncertainty. We consider two scenarios for the estimates of the dynamics and safe set: either worst-case error bounds or probabilistic descriptions in the form of Gaussian Processes (GPs) are available. In both cases, the problem of designing a safe stabilizing controller can be reduced to satisfying two SOCCs

at every point in the safe set. We have given conditions for the feasibility of each pair of SOCCs. The first result is a sufficient condition that requires a bound on the norm of a safe and stabilizing controller and quantifies what model errors are tolerable while still being able to find a controller that guarantees safe stabilization. Our second result is a sufficient condition that does not require knowledge of such bound and consists of finding a root of a scalar nonlinear equation. We have also established different regularity properties for controllers satisfying a set of SOCCs. First we show that if each pair of SOCCs is feasible, then there exists a smooth safe stabilizing controller. Second, we show that the minimum-norm controller satisfying each pair of SOCCs is point-Lipschitz. Third, we provide a universal formula for satisfying a single SOCC and hence achieving either safety or stability.

In Chapter 10 we have also studied the problem of safe stabilization of control-affine systems under uncertainty. However, in this case we assume that the distribution of the uncertainty is unknown and formulate the control design problem through a second-order cone program using distributionally robust versions of the CLF and CBF constraints constructed on the basis of uncertainty samples. We have derived a necessary condition and two sufficient conditions for the feasibility of the optimization problem. We have characterized the computational complexity of these conditions and show that, for a large number of samples, it is significantly smaller than solving the SOCP directly, which makes them useful to efficiently check whether the problem is feasible without having to solve it. Our first sufficient condition is dependent on the quality of the uncertainty samples but is limited to a single control objective. Our second sufficient condition is only dependent on the number of samples but can be used for any number of constraints. We have also shown that the solution of this distributionally robust optimization problem is point-Lipschitz, and hence continuous, which means that solutions of the closed loop system are guaranteed to exist and the controller obtained from it can be implemented without inducing chattering.

In Chapter 11 we have considered the problem of designing an algorithm that finds the optimal policy of a constrained RL problem and is anytime (i.e., it satisfies the constraints of the problem at every iteration). To achieve this goal, first

we have introduced the Robust Safe Gradient Flow (RSGF), a continuous-time algorithm for constrained optimization that is a variation of the recently introduced Safe Gradient Flow. We have established a set of assumptions under which the RSGF is locally and globally Lipschitz, it is anytime, and converges to the set of KKT points of the original constrained optimization problem. Second, we have defined estimates for the value functions defining the constrained RL problem as well as their gradients. These estimates are off-policy, in the sense that the estimates of any given policy can be constructed using trajectories generated by other policies. We have establish different statistical properties of these estimates such as their mean, a bound on their variance, and the probability that the difference between the estimates and their true values is within a tolerance. Next, we have introduced Reinforcement Learning-based Robust Safe Gradient Flow (RL-RSGF), an off-policy algorithm that is based on a discretization of RSGF and utilizes the introduced estimates of the value function and their estimates. We have shown that for any prescribed confidence, if the estimates are generated with a sufficiently large number of episodes (which we quantify), RL-RSGF updates safe policies to safe policies. We also show that the iterates of RL-RSGF asymptotically converge to a KKT point with probability one, and characterize its rate of convergence. Finally, we have illustrated the performance of RL-SGF in different simulation examples.

12.2 Outlook

Our ultimate goal is to develop an integrative theory for designing autonomous systems with rigorous safety guarantees. This is challenging due to the multi-objective and modular nature of modern autonomous systems, as well as the need to incorporate learning-based components into the system to handle uncertainty, and the requirement that the decision-making process is made in real time and computationally efficiently. In this thesis we have shown that CBFs are a flexible tool that can be used to address some of these challenges. As shown in the first part of this dissertation we have shown that CBFs can be used to design safe and sta-

ble controllers. One of the main limitations of CBF-based controllers is that they are usually implemented *myopically* (i.e., without any future prediction), which can significantly degrade their performance, particularly in cases where a topological obstruction is present. In these cases, hierarchical solutions such as the one developed in the second part of this dissertation hold promise. Additionally, this hierarchical approach is particularly appealing in applications with modular stacks, such as autonomous driving, where the different modules need to be combined so that the overall system has a desired performance. As shown in the third part of this dissertation, another attractive feature of CBFs is their ability to provide robustness guarantees under various types of uncertainty models.

It should be pointed out that some of the features of CBFs discussed in this dissertation (such as integration with stability, robustness or distributed implementation) are not unique to CBFs, and can also be achieved with other control-theoretic techniques such as Model Predictive Control or Artificial Potential Fields.

Additionally, we should also note that one limitation of the work presented in this dissertation is that it generally assumes the availability of a CBF or a known control invariant set *a priori*. Although it has not been the focus of this dissertation, there has been a lot of work on obtaining CBFs or control invariant sets, including HJ reachability techniques [14], sum-of-squares [209], or neural methods [249].

Finally, we would also like to stress the power of using *CBFs for optimization*, as previously introduced in [98] and Chapter 11. This new use of CBFs opens a new realm of possibilities for their use in any constrained optimization problem.

12.3 Future Work

The contributions of this dissertation set the stage for exploring many research venues, some of which we detail next.

(1) **Dynamical properties of CBF-based controllers:** Although [5] has outlined some of the limitations of CBF-based safety filters, it has also illustrated that for some systems of interest, they induce the best possible

behavior given the topological obstructions of the problem of safe stabilization. A full characterization of which systems and safe sets have such best possible dynamical behavior is lacking in the state of the art, and constitutes an important open problem in the field of safe and stable control.

(2) **Optimality guarantees in CBF-based control:** Despite the simplicity in the implementation of CBF-based controllers, one of their main drawbacks is the fact that they are *myopic* and only *pointwise optimal*. This means that CBF-based controllers are in general not optimal over a long time horizon. Although predictive versions of the standard CBF theory have been recently considered [250, 26], as well as its inverse optimality [251], a theory for optimal CBF-based control is still lacking, and remains an important area of future research. A promising line of future research to address this issue revolves around the use of high-level planners along with CBF-based controllers, in a fashion similar to Chapter 8, where the high-level planner needs to be designed to ensure some notion of optimality for the low-level controller.

(3) **Theory of optimization-based controllers in closed-loop**: As discussed in Chapter 6, CBF-based controllers are only a special class of *optimization-based controllers*, i.e., controllers that are computed at every state as the solution of an optimization problem. Since exact online solutions to such problems can be difficult to obtain, specially if the optimization problem is non-convex and high-dimensional, one must resort to inexact solutions or approximations computed offline. An important area of future research is the development of a theory that can guarantee *safety*, *stability*, and *good performance* for such *inexact* optimization-based controllers.

(4) **Hierarchical motion planning and control:** The algorithm presented in [11] is only one possible instantiation of a hierarchical controller for motion planning combining a low-level controller with a high-level motion planner. Future work will explore the extension of the results to other sampling-based algorithms (e.g., RRT*, bidirectional RRT), construct asymptotically opti-

mal versions of `C-CLF-CBR-RRT` using model predictive control, and integrate available computational tools to find CLFs and verify the compatibility of CLF-CBF pairs into these algorithms. We also plan to extend this class of algorithms to systems that do not admit CLFs, such as driftless systems with less control inputs than states, which are common in robotics.

(5) **Control-theoretic methods for (safe) reinforcement learning:** The algorithm presented in Chapter 11 showcases the potential of using control-theoretic methods in reinforcement learning (recall that CBFs are the foundation of the safe gradient flow [98] and the RSGF, upon which RL-RSGF is built). In the future, we plan to explore other ways to synergize control-theoretic tools and RL algorithms. For example, an important observation is that the algorithm developed in Chapter 11 presupposes that safety constraints are given as the expected value of cumulative returns. In practice, the safety constraints that we are interested in robotics applications take a different form. One example is a type of constraint where we want to ensure that the probability of staying in a given safe set of interest over a finite time horizon is greater than a prescribed tolerance. Developing RL algorithms suited for this type of constraints is part of our future work. Furthermore, we also plan to incorporate such Safe RL algorithms into a hierarchical framework that combines low-level safe controllers, as well as mid-level motion planners.

Bibliography

[1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2017.

[2] J. Achiam, D. Held, A. Tamar, and P. Abbeel, "Constrained policy optimization," in *Proceedings of the 34th International Conference on Machine Learning*, vol. 70, Sydney, Australia, 2017, pp. 22–31.

[3] P. Mestres, A. Marzabal, and J. Cortés, "Anytime safe reinforcement learning," in *Learning for Dynamics and Control Conference*, ser. Proceedings of Machine Learning Research, 2025, to appear.

[4] P. Mestres and J. Cortés, "Optimization-based safe stabilizing feedback with guaranteed region of attraction," *IEEE Control Systems Letters*, vol. 7, pp. 367–372, 2023.

[5] P. Mestres, Y. Chen, E. Dall'Anese, and J. Cortés, "Control barrier function-based safety filters: characterization of undesired equilibria, unbounded trajectories, and limit cycles," *Journal of Nonlinear Science*, 2025, submitted.

[6] Y. Chen, P. Mestres, E. Dall'Anese, and J. Cortés, "Characterization of the dynamical properties of safety filters for linear planar systems," in *IEEE Conf. on Decision and Control*, Milan, Italy, 2024, pp. 2397–2402.

[7] P. Mestres and J. Cortés, "Converse theorems for certificates of safety and stability," *IEEE Transactions on Automatic Control*, 2024, submitted. Available at https://arxiv.org/abs/2406.14823.

[8] P. Mestres, A. Allibhoy, and J. Cortés, "Regularity properties of optimization-based controllers," *European Journal of Control*, vol. 81, p. 101098, 2025.

[9] P. Mestres, C. Nieto-Granda, and J. Cortés, "Distributed safe navigation of multi-agent systems using control barrier function-based controllers," *IEEE Robotics and Automation Letters*, vol. 9, no. 7, pp. 6760–6767, 2024.

[10] P. Mestres and J. Cortés, "Distributed and anytime algorithm for network optimization problems with separable structure," in *IEEE Conf. on Decision and Control*, Singapore, 2023, pp. 5457–5462.

[11] P. Mestres, C. Nieto-Granda, and J. Cortés, "Safe and dynamically-feasible motion planning using control lyapunov and barrier functions," *IEEE Transactions on Robotics*, 2024, submitted.

[12] P. Mestres and J. Cortés, "Feasibility and regularity analysis of safe stabilizing controllers under uncertainty," *Automatica*, vol. 167, p. 111800, 2024.

[13] P. Mestres, K. Long, N. Atanasov, and J. Cortés, "Feasibility analysis and regularity characterization of distributionally robust safe stabilizing controllers," *IEEE Control Systems Letters*, vol. 8, pp. 91–96, 2024.

[14] H. Jacobi Reachability: A Brief Overview and Recent Advances, "S. bansal and m. chen and s. herbert and c. j. tomlin," in *IEEE Conf. on Decision and Control*, Melbourne, Australia, Dec. 2017, pp. 2242–2253.

[15] M. Chen, S. L. Herbert, M. Vashishtha, S. Bansal, and C. J. Tomlin, "Decomposition of reachable sets and tubes for a class of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 11, pp. 3675–3688, 2018.

[16] J. Darbon and S. Osher, "Algorithms for overcoming the curse of dimensionality for certain Hamilton-Jacobi equations arising in control theory and elsewhere," *Research in the Mathematical Sciences*, vol. 3, no. 1, p. 19, 2016.

[17] D. E. Koditschek, "Exact robot navigation by means of potential functions: some topological considerations," in *IEEE Int. Conf. on Robotics and Automation*, Raleigh, NC, USA, 1987, pp. 1–6.

[18] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," *International Journal of Robotics Research*, vol. 5, no. 1, pp. 90–98, 1986.

[19] J. B. Rawlings, D. Q. Mayne, and M. M. Diehl, *Model Predictive Control: Theory, Computation, and Design.* Nob Hill Publishing, 2017.

[20] P. A. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, California Institute of Technology, 2000.

[21] R. T. A. Majumdar, A. A. Ahmadi, "Control design along trajectories with sums of squares programming," in *IEEE Int. Conf. on Robotics and Automation*, Karlsruhe, Germany, 2013, pp. 4054–4061.

[22] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proceedings Volumes*, vol. 40, no. 12, pp. 462–467, 2007.

[23] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: theory and applications," in *European Control Conference*, Naples, Italy, 2019, pp. 3420–3431.

[24] S. Tonkens and S. Herbert, "Refining control barrier functions through Hamilton-Jacobi reachability," in *IEEE/RSJ Int. Conf. on Intelligent Robots & Systems*, 2022, pp. 13 355–13 362.

[25] J. Zeng, B. Zhang, and K. Sreenath, "Safety-Critical Model Predictive Control with Discrete-Time Control Barrier Function," in *2021 American Control Conference*, New Orleans, USA, May 2021, pp. 3882–3889.

[26] J. Breeden and D. Panagou, "Predictive control barrier functions for online safety critical control," in *IEEE Conf. on Decision and Control*, Cancun, Mexico, Dec. 2022, pp. 924–931.

[27] E. D. Sontag, *Mathematical Control Theory: Deterministic Finite Dimensional Systems*, 2nd ed., ser. TAM. Springer, 1998, vol. 6.

[28] M. Z. Romdlony and B. Jayawardhana, "Stabilization with guaranteed safety using control Lyapunov-barrier function," *Automatica*, vol. 66, pp. 39–47, 2016.

[29] E. D. Sontag, "A universal construction of Artstein's theorem on nonlinear stabilization," *Systems & Control Letters*, vol. 13, no. 2, pp. 117–123, 1989.

[30] P. Braun and C. M. Kellett, "On (the existence of) control Lyapunov barrier functions," Newcastle, Australia, 2017, available at https://epub.uni-bayreuth.de/id/eprint/3522/1/CLBFs_submission_pbraun.pdf.

[31] P. Ong and J. Cortés, "Universal formula for smooth safe stabilization," in *IEEE Conf. on Decision and Control*, Nice, France, Dec. 2019, pp. 2373–2378.

[32] B. J. Morris, M. J. Powell, and A. D. Ames, "Continuity and smoothness properties of nonlinear optimization-based feedback controllers," in *IEEE Conf. on Decision and Control*, Osaka, Japan, Dec 2015, pp. 151–158.

[33] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, vol. 96, pp. 359–367, 2018.

[34] M. F. Reis, A. P. Aguilar, and P. Tabuada, "Control barrier function-based quadratic programs introduce undesirable asymptotically stable equilibria," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 731–736, 2021.

[35] X. Tan and D. V. Dimarogonas, "On the undesired equilibria induced by control barrier function based quadratic programs," *arXiv preprint arXiv:2104.14895*, 2021.

[36] L. Wang, A. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Transactions on Robotics*, vol. 33, no. 3, pp. 661–674, 2017.

[37] W. S. Cortez and D. V. Dimarogonas, "On compatibility and region of attraction for safe, stabilizing control laws," *IEEE Transactions on Automatic Control*, vol. 67, no. 9, pp. 7706–7712, 2022.

[38] F. Castañeda, J. J. Choi, B. Zhang, C. J. Tomlin, and K. Sreenath, "Pointwise feasibility of Gaussian process-based safety-critical control under model uncertainty," in *IEEE Conf. on Decision and Control*, Austin, Texas, USA, 2021, pp. 6762–6769.

[39] ——, "Gaussian process-based min-norm stabilizing controller for control-affine systems with uncertain input effects and dynamics," in *American Control Conference*, New Orleans, LA, 2021, pp. 3683–3690.

[40] M. Li and Z. Sun, "Safe stabilization with model uncertainties: A universal formula with gaussian process learning," *arXiv preprint arXiv:2312.02892*, 2023.

[41] K. Long, V. Dhiman, M. Leok, J. Cortés, and N. Atanasov, "Safe control synthesis with uncertain dynamics and constraints," *IEEE Robotics and Automation Letters*, vol. 7, no. 3, pp. 7295–7302, 2022.

[42] K. Long, C. Qian, J. Cortés, and N. Atanasov, "Learning barrier functions with memory for robust safe navigation," *IEEE Robotics and Automation Letters*, vol. 6, no. 3, pp. 4931–4938, 2021.

[43] K. Long, Y. Yi, J. Cortés, and N. Atanasov, "Safe and stable control synthesis for uncertain system models via distributionally robust optimization," in *American Control Conference*, San Diego, California, Jun. 2023, pp. 4651–4658.

[44] V. Dhiman, M. J. Khojasteh, M. Franceschetti, and N. Atanasov, "Control barriers in Bayesian learning of system dynamics," *IEEE Transactions on Automatic Control*, vol. 68, no. 1, pp. 214–229, 2023.

[45] F. Castañeda, J. J. Choi, W. Jung, B. Zhang, C. J. Tomlin, and K. Sreenath, "Probabilistic safe online learning with control barrier functions," *https://arxiv.org/pdf/2208.10733.pdf*, 2022.

[46] U. Borrmann, L. Wang, A. D. Ames, and M. Egerstedt, "Control barrier certificates for safe swarm behavior," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 68–73, 2015.

[47] X. Tan and D. V. Dimarogonas, "Distributed implementation of control barrier functions for multi-agent systems," *IEEE Control Systems Letters*, vol. 6, pp. 1879–1884, 2022.

[48] V. N. Fernandez-Ayala, X. Tan, and D. V. Dimarogonas, "Distributed barrier function-enabled human-in-the-loop control for multi-robot systems," in *IEEE Int. Conf. on Robotics and Automation*, London, UK, 2023, pp. 7706–7712.

[49] X. Tan, C. Liu, K. H. Johansson, and D. V. Dimarogonas, "A continuous-time violation-free multi-agent optimization algorithm and its applications to safe distributed control," *arXiv preprint arXiv:2404.07571*, 2024.

[50] C. Liu, X. Tan, X. Wu, D. V. Dimarogonas, and K. H. Johansson, "Achieving violation-free distributed optimization under coupling constraints," *arXiv preprint arXiv:2404.07609*, 2024.

[51] N. de Carli, P. Salaris, and P. R. Giordano, "Distributed control barrier functions for global connectivity maintenance," in *IEEE Int. Conf. on Robotics and Automation*, Yokohama, Japan, 2024.

[52] M. Diehl, H. G. Bock, H. Diegam, and P. B. Wieber, *Fast Motions in Biomechanics and Robotics*. New York: Springer, 2006.

[53] F. Augugliaro, A. P. Schoellig, and R. D'Andrea, "Generation of collision-free trajectories for a quadrocopter fleet: A sequential convex programming approach," in *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems*, Algarve, Portugal, 2012, pp. 1917–1922.

[54] X. Zhang, A. Liniger, and F. Borrelli, "Optimization-Based Collision Avoidance," *IEEE Transactions on Control Systems Technology*, vol. 29, no. 3, pp. 972–983, 2021.

[55] J. Tordesillas and J. P. How, "MADER: Trajectory planner in multiagent and dynamic environments," *IEEE Transactions on Robotics*, vol. 38, no. 1, pp. 463–476, 2021.

[56] ——, "PANTHER: Perception-aware trajectory planner in dynamic environments," *IEEE Access*, vol. 10, pp. 22 662–22 677, 2022.

[57] W. Ding, W. Gao, K. Wang, and S. Shen, "An efficient B-spline-based kinodynamic replanning framework for quadrotors," *IEEE Transactions on Robotics*, vol. 35, no. 6, pp. 1287–1306, 2019.

[58] C. Richter, A. Bry, and N. Roy, *Polynomial Trajectory Planning for Aggressive Quadrotor Flight in Dense Environments*. New York: Springer, 2016.

[59] N. Csomay-Shanklin, W. D. Compton, and A. D. Ames, "Dynamically feasible path planning in cluttered environments via reachable bezier polytopes," *arXiv preprint arXiv:2411.13507*, 2023.

[60] T. Marcucci, M. Petersen, D. V. Wrangel, and R. Tedrake, "Motion planning around obstacles with convex optimization," *Science Robotics*, vol. 8, no. 84, p. eadf7843, 2023.

[61] T. Marcucci, J. Umemberger, P. Parrillo, and R. Tedrake, "Shortest Paths in Graphs of Convex Sets," *SIAM Journal on Optimization*, vol. 34, no. 1, pp. 507–532, 2024.

[62] L. E. Kavraki, P. Švestka, J. C. Latombe, and M. H. Overmars, "Probabilistic roadmaps for path planning in high-dimensional space," *IEEE Transactions on Robotics and Automation*, vol. 12, no. 4, pp. 566–580, 1996.

[63] S. M. LaValle, "Rapidly-exploring random trees : a new tool for path planning," *The Annual Research Report*, 1998.

[64] J. Kuffner and S. LaValle, "RRT-connect: an efficient approach to single-query path planning," in *IEEE Int. Conf. on Robotics and Automation*, San Francisco, USA, 2000, pp. 995–1001.

[65] S. Karaman and E. Frazzoli, "Sampling-based algorithms for optimal motion planning," *International Journal of Robotics Research*, vol. 30, no. 7, pp. 846–894, 2011.

[66] S. M. LaValle, *Planning Algorithms*. Cambridge University Press, 2006, available at `http://planning.cs.uiuc.edu`.

[67] D. J. Webb and J. van den Berg, "Kinodynamic RRT*: Asymptotically optimal motion planning for robots with linear dynamics," in *IEEE Int. Conf. on Robotics and Automation*, Karlsruhe, Germany, 2013, pp. 5054–5061.

[68] L. Yi, Z. Littlefield, and K. E. Bekris, "Asymptotically optimal sampling-based kinodynamic planning," *International Journal of Robotics Research*, vol. 35, no. 5, pp. 528–564, 2016.

[69] E. Glassman and R. Tedrake, "A quadratic regulator-based heuristic for rapidly exploring state space," in *IEEE Int. Conf. on Robotics and Automation*, Anchorage, USA, 2010, pp. 5021–5028.

[70] A. Perez, R. Platt, G. Konidaris, L. Kaelbling, and T. Lozano-Perez, "Optimal sampling-based motion planning with automatically derived extension heuristics," in *IEEE Int. Conf. on Robotics and Automation*, St. Paul, USA, 2012, pp. 2537–2542.

[71] A. J. LaValle, B. Sakcak, and S. M. LaValle, "Bang-bang boosting of RRTs," in *IEEE/RSJ Int. Conf. on Intelligent Robots & Systems*, Detroit, USA, 2023, pp. 2869–2876.

[72] L. Palmieri and K. O. Arras, "Distance metric learning for RRT-based motion planning with constant-time inference," in *IEEE Int. Conf. on Robotics and Automation*, Seattle, USA, 2015, pp. 637–643.

[73] Y. Li and K. E. Bekris, "Learning approximate cost-to-go metrics to improve sampling-based motion planning," in *IEEE Int. Conf. on Robotics and Automation*, Shanghai, China, 2011, pp. 4196–4201.

[74] W. J. Wolfslag, M. Bharatheesha, T. M. Moerland, and M. Wisse, "RRT-CoLearn: Towards kinodynamic planning without numerical trajectory optimization," *IEEE Robotics and Automation Letters*, vol. 3, no. 3, pp. 1655–1662, 2018.

[75] H. L. Chiang, J. Hsu, M. Fiser, L. Rapia, and A. Faust, "RL-RRT: kinodynamic motion planning via learning reachability estimators from RL policies," *IEEE Robotics and Automation Letters*, vol. 4, no. 4, pp. 4298–4305, 2019.

[76] R. Tedrake, I. R. Manchester, M. Tobenkin, and J. W. Roberts, "LQR-trees: Feedback Motion Planning via Sums-of-Squares Verification," *The International Journal of Robotics Research*, vol. 29, no. 8, pp. 1038–1052, 2010.

[77] A. Ahmad, C. Belta, and R. Tron, "Adaptive sampling-based motion planning with control barrier functions," in *IEEE Conf. on Decision and Control*, Cancun, Mexico, Dec. 2022, pp. 4513–4518.

[78] K. Majd, S. Yaghoubi, T. Yamaguchi, B. Hoxha, D. Prokhorov, and G. Fainekos, "Safe navigation in human occupied environments using sampling and control barrier functions," in *IEEE/RSJ Int. Conf. on Intelligent Robots & Systems*, Prague, Czech Republic, 2021, pp. 5794–5800.

[79] G. Yan, B. Vang, Z. Serlin, C. Belta, and R. Tron, "Sampling-based motion planning using control barrier functions," in *International Conference on Automation, Control and Robots*, Prague, Czech Republic, 2019, pp. 22–29.

[80] A. Manjunath and Q. Nguyen, "Safe and Robust Motion Planning for Dynamic Robotics via Control Barrier Functions," in *IEEE Conf. on Decision and Control*, Austin, USA, 2021, pp. 2122–2128.

[81] G. Yang, M. Cai, A. Ahmad, A. Prorok, R. Tron, and C. Belta, "LQR-CBF-RRT*: Safe and Optimal Motion Planning," *arXiv preprint arXiv:2304.00790*, 2023.

[82] L. Brunkel, M. Greeff, A. W. Hall, Z. Yuan, S. Zhou, J. Panerati, and A. P. Schoellig, "Safe learning in robotics: from learning-based control to safe reinforcement learning," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 5, pp. 411–444, 2022.

[83] Y. Liu, H. Avishai, and X. Liu, "Policy learning with constraints in model-free reinforcement learning: a survey," in *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence*, Montreal, Canada, 2021, pp. 4508–4515.

[84] J. Garcia and F. Fernandez, "A comprehensive survey on safe reinforcement learning," *Journal of Machine Learning Research*, vol. 16, pp. 1437–1480, 2015.

[85] S. Gu, L. Yang, Y. Du, G. Chen, F. Walter, J. Wang, and A. Knoll, "A review of safe reinforcement learning: methods, theory and applications," *arXiv preprint arXiv:1809.01674v2*, 2022.

[86] E. Altman, *Constrained Markov Decision Processes*. CRC Press, 1999, vol. 7.

[87] Y. Chow, M. Ghavamzadeh, L. Janson, and M. Pavone, "Risk-constrained reinforcement learning with percentile risk criteria," *The Journal of Machine Learning Research*, vol. 18, no. 1, pp. 6070–6120, 2017.

[88] S. Paternain, L. Chamon, M. Calvo-Fullana, and A. Ribeiro, "Constrained Reinforcement Learning Has Zero Duality Gap," in *Proceedings of the 32nd Conference in Neural Information Processing Systems*, vol. 32, Vancouver, Canada, 2019, pp. 7555–7565.

[89] S. Paternain, M. Calvo-Fullana, L. F. O. Chamon, and A. Ribeiro, "Safe Policies for Reinforcement Learning via Primal-Dual Methods," *IEEE Transactions on Automatic Control*, vol. 68, no. 3, pp. 1321–1336, 2023.

[90] D. Ding, K. Zhang, T. Basar, and M. Jovanovic, "Natural Policy Gradient Primal-Dual Method for Constrained Markov Decision Processes," in *Proceedings of the 33rd Conference on Neural Information Processing Systems*, vol. 33, Online Conference, 2020, pp. 8378–8390.

[91] D. Ding, X. Wei, Z. Yang, Z. Wang, and M. Jovanovic, "Provably efficient safe exploration via primal-dual policy optimization," in *Proceedings of the 24th International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, vol. 130, Online Conference, 2021, pp. 3304–3312.

[92] S. Zeng, T. T. Doan, and J. Romberg, "Finite-time complexity of online primal-dual natural actor-critic algorithm for constrained Markov decision processes," in *IEEE Conf. on Decision and Control*, Cancun, Mexico, 2022, pp. 4028–4033.

[93] Q. Bai, A. S. Bedi, M. Agarwal, A. Koppel, and V. Aggarwal, "Achieving zero constraint violation for constrained reinforcement learning via primal-dual approach," in *Proceedings of the 36th AAAI Conference on Artificial Intelligence*, Vancouver, Canada, 2022, pp. 3682–3689.

[94] Q. Bai, A. S. Bedi, and V. Aggarwal, "Achieving zero constraint violation for constrained reinforcement learning via conservative natural policy gradient primal-dual algorithm," in *Proceedings of the 37th AAAI Conference on Artificial Intelligence*, Washington D. C., USA, 2023, pp. 6737–6744.

[95] Y. Liu, J. Ding, and X. Liu, "IPO: Interior-Point Policy Optimization under Constraints," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, New York, USA, 2020, pp. 4940–4947.

[96] Y. Chow, O. Nachum, E. Duenez-Guzman, and M. Ghavamzadeh, "A Lyapunov-based Approach to Safe Reinforcement Learning," in *Proceedings of the 31st Conference on Neural Information Processing Systems*, Montreal, Canada, 2018, pp. 8103–8112.

[97] W. Suttle, V. K. Sharma, K. C. Kosaraju, S. Seetharaman, J. Liu, V. Gupta, and B. M. Sadler, "Sampling-based safe reinforcement learning for nonlinear dynamical systems," in *Proceedings of the 27th International Conference on Artificial Intelligence and Statistics*, vol. 238, Valencia, Spain, 2024, pp. 4420–4428.

[98] A. Allibhoy and J. Cortés, "Control barrier function-based design of gradient flows for constrained nonlinear programming," *IEEE Transactions on Automatic Control*, vol. 69, no. 6, pp. 3499–3514, 2024.

[99] G. Still, "Lectures On Parametric Optimization: An Introduction," *Preprint, Optimization Online*, 2018.

[100] R. T. Rockafellar and R. J. B. Wets, *Variational Analysis*, ser. Comprehensive Studies in Mathematics. New York: Springer, 1998, vol. 317.

[101] L. Perko, *Differential Equations and Dynamical Systems*, 3rd ed., ser. Texts in Applied Mathematics. New York: Springer, 2000, vol. 7.

[102] R. A. Freeman and P. V. Kototovic, *Robust Nonlinear Control Design: State-space and Lyapunov Techniques*. Cambridge, MA, USA: Birkhauser Boston Inc., 1996.

[103] M. Alyaseen, N. Atanasov, and J. Cortés, "Continuity and boundedness of minimum-norm CBF-safe controllers," *IEEE Transactions on Automatic Control*, vol. 70, no. 6, 2025, to appear.

[104] R. Konda, A. D. Ames, and S. Coogan, "Characterizing safety: minimal control barrier functions from scalar comparison systems," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 523–528, 2021.

[105] E. D. Sontag and H. J. Sussmann, "Remarks on continuous feedback control," in *IEEE Conf. on Decision and Control*, New Orleans, LA, USA, 1995, pp. 2799–2805.

[106] P. Glotfelter, J. Cortés, and M. Egerstedt, "Nonsmooth approach to controller synthesis for Boolean specifications," *IEEE Transactions on Automatic Control*, vol. 66, no. 11, pp. 5160–5174, 2021.

[107] A. Cherukuri and J. Cortés, "Distributed algorithms for convex network optimization under non-sparse equality constraints," in *Allerton Conf. on Communications, Control and Computing*, Monticello, IL, Sep. 2016, pp. 452–459.

[108] M. Kleinbort, K. Solovey, Z. Littlefield, K. Bekris, and D. Halperin, "Probabilistic completeness of RRT for geometric and kinodynamic planning with forward propagation," *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. i–vii, 2019.

[109] A. Nemirovski and A. Shapiro, "Convex approximations of chance constrained programs," *SIAM Journal on Optimization*, vol. 17, no. 4, pp. 969–996, 2006.

[110] P. M. Esfahani and D. Kuhn, "Data-driven distributionally robust optimization using the Wasserstein metric: performance guarantees and tractable reformulations," *Mathematical Programming*, vol. 171, no. 1-2, pp. 115–166, 2018.

[111] W. S. Cortez and D. V. Dimarogonas, "On compatibility and region of attraction for safe, stabilizing control laws," *arXiv preprint arXiv:2008.12179*, 2021.

[112] D. G. Luenberger, *Linear and Nonlinear Programming*, 2nd ed. Addison-Wesley, 1984.

[113] ——, *Optimization by Vector Space Methods*. Wiley, 1969.

[114] X. Xu, "Constrained control of input-output linearizable systems using control sharing barrier functions," *Automatica*, vol. 87, pp. 195–201, 2018.

[115] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York, USA: Cambridge University Press, 2012.

[116] F. W. Wilson, "The structure of the level surfaces of a Lyapunov function," *Journal of Differential Equations*, vol. 3, no. 323-329, 1967.

[117] P. Braun and C. M. Kellett, "Comment on "Stabilization with guaranteed safety using control Lyapunov–barrier function"," *Automatica*, vol. 122, p. 109225, 2020.

[118] X. Tan and D. V. Dimarogonas, "On the undesired equilibria induced by control barrier function based quadratic programs," *Automatica*, vol. 159, p. 111359, 2024.

[119] Y. Yi, S. Koga, B. Gavrea, and N. Atanasov, "Control synthesis for stability and safety by differential complementarity problem," *IEEE Control Systems Letters*, vol. 7, pp. 895–900, 2023.

[120] Y. Chen, P. Mestres, J. Cortés, and E. Dall'Anese, "Equilibria and their stability do not depend on the control barrier function in safe optimization-based control," *Automatica*, 2024, submitted. https://arxiv.org/abs/2409.06808.

[121] H. Khalil, *Nonlinear Systems, 3rd ed.* Englewood Cliffs, NJ: Prentice Hall, 2002.

[122] J. D. Meiss, *Differential Dynamical Systems*. SIAM, 2007.

[123] P. Hartman, *Ordinary Differential Equations*, 2nd ed. SIAM, 2002, no. 38.

[124] S. P. Bhat and D. S. Bernstein, "Nontangency-based Lyapunov tests for convergence and stability in systems having a continuum of equilibria," *SIAM Journal on Control and Optimization*, vol. 42, no. 5, pp. 1745–1775, 2003.

[125] A. Hurwitz, "Ueber die bedingungen, unter welchen eine gleichung nur wurzeln mit negativen reellen theilen besitzt," *Mathematische Annalen*, vol. 46, no. 1, pp. 273–284, 1895.

[126] M. Nagumo, "Über die Lage der Integralkurven gewöhnlicher Differentialgleichungen," *Proceedings of the Physico-Mathematical Society of Japan*, vol. 24, pp. 551–559, 1942.

[127] B. Lin, W. Yao, and M. Cao, "On Wilson's theorem about domains of attraction and tubular neigborhoods," *Systems & Control Letters*, vol. 167, p. 105322, 2022.

[128] M. Maghenem and R. G. Sanfelice, "On the converse safety problem for differential inclusions: Solutions, regularity, and time-varying barrier functions," *IEEE Transactions on Automatic Control*, vol. 68, no. 1, pp. 172–187, 2023.

[129] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, "Robust control barrier-value functions for safety-critical control," in *IEEE Conf. on Decision and Control*, Austin, TX, USA, 2021, pp. 6814–6821.

[130] W. Rudin, *Real and Complex Analysis*, 3rd ed. McGraw-Hill, 1987.

[131] Y. Lin, E. D. Sontag, and Y. Wang, "A smooth converse Lyapunov theorem for robust stability," *SIAM Journal on Control and Optimization*, vol. 34, no. 1, pp. 124–160, 1996.

[132] S. Hsu, X. Xu, and A. D. Ames, "Control barrier function based quadratic programs with applications to bipedal robot walking," in *American Control Conference*, Chicago, USA, July 2015.

[133] M. Maghenem and M. Ghanbarpour, "A converse robust-safety theorem for differential inclusions," *arXiv preprint arXiv:2208.11364*, 2022.

[134] Y. Meng, Y. Li, M. Fitzsimmons, and J. Liu, "Smooth converse Lyapunov-barrier theorems for asymptotic stability with safety constraints and reach-avoid-stay specifications," *Automatica*, vol. 144, p. 110478, 2022.

[135] J. M. Lee, "Smooth manifolds," in *Introduction to Smooth Manifolds*. Springer, 2013, pp. 1–31.

[136] C. E. Garcia, D. M. Prett, and M. Morari, "Model predictive control: Theory and practice–A survey," *Automatica*, vol. 25, no. 3, pp. 335–348, 1989.

[137] M. Colombino, E. Dall'Anese, and A. Bernstein, "Online optimization as a feedback controller: Stability and tracking," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 422–432, 2020.

[138] A. Hauswirth, S. Bolognani, G. Hug, and F. Dörfler, "Optimization algorithms as robust feedback controllers," *arXiv preprint arXiv:2103.11329*, 2021.

[139] A. V. Fiacco and G. P. McCormick, *Nonlinear Programming: Sequential Unconstrained Minimization Techniques*, ser. Classics in Applied Mathematics. Philadelphia, PA: SIAM, 1990, vol. 4.

[140] J. F. Bonnans and A. Shapiro, "Optimization problems with perturbations: a guided tour," *SIAM Review*, vol. 40, no. 2, pp. 228–264, 1998.

[141] P. Seiler, M. Jankovic, and E. Hellstrom, "Control barrier functions with unmodeled input dynamics using integral quadratic constraints," *IEEE Control Systems Letters*, vol. 6, pp. 1664–1669, 2021.

[142] A. J. Taylor, V. D. Dorobantu, S. Dean, B. Recht, Y. Yue, and A. D. Ames, "Towards robust data driven control synthesis for nonlinear systems with actuation uncertainty," in *IEEE Conf. on Decision and Control*, Austin, Texas, USA, 2021, pp. 6469–6476.

[143] G. Teschl, *Ordinary Differential Equations and Dynamical Systems*, ser. Graduate Studies in Mathematics. Providence, RI: American Mathematical Society, 2012, vol. 140.

[144] A. Davydov and F. Bullo, "Exponential stability of parametric optimization-based controllers via Lur'e contractivity," *arXiv preprint arXiv:2403.08159*, 2024.

[145] E. Dall'Anese and A. Simonetto, "Optimal power flow pursuit," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 942–952, 2016.

[146] L. S. P. Lawrence, J. W. Simpson-Porco, and E. Mallada, "Linear-convex optimal steady-state control," *IEEE Transactions on Automatic Control*, vol. 66, no. 11, pp. 5377–5384, 2021.

[147] S. H. Low, F. Paganini, and J. C. Doyle, "Internet congestion control," *IEEE Control Systems*, vol. 22, no. 1, pp. 28–43, 2002.

[148] G. Bianchin, J. Cortés, J. I. Poveda, and E. Dall'Anese, "Time-varying optimization of LTI systems via projected primal-dual gradient flows," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 1, pp. 474–486, 2022.

[149] K. Arrow, L. Hurwitz, and H. Uzawa, *Studies in Linear and Non-Linear Programming*. Stanford, CA: Stanford University Press, 1958.

[150] R. W. Brockett, "Dynamical systems that sort lists, diagonalize matrices, and solve linear programming problems," *Linear Algebra and Its Applications*, vol. 146, pp. 79–91, 1991.

[151] U. Helmke and J. B. Moore, *Optimization and Dynamical Systems*. Springer, 1994.

[152] A. Nagurney and D. Zhang, *Projected Dynamical Systems and Variational Inequalities with Applications*, ser. International Series in Operations Research and Management Science. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1996, vol. 2.

[153] A. Nagurney, "Network economics," in *Handbook of Computational Econometrics*, D. A. Belsley and E. J. Kontoghiorghes, Eds. New York: Wiley, 2009, pp. 429–486.

[154] D. K. Molzahn, F. Dörfler, H. Sandberg, S. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.

[155] A. Hauswirth, F. Dorfler, and A. Teel, "Anti-windup approximations of oblique projected dynamics for feedback-based optimization," *arXiv preprint arXiv:2003.00478*, 2020.

[156] A. Nagurney and D. Zhang, "Projected dynamical systems in the formulation, stability analysis and computation of fixed demand traffic network equilibria," *Transportation Science*, vol. 31, no. 2, pp. 101–195, 1997.

[157] A. Hauswirth, S. Bolognani, and F. Dörfler, "Projected dynamical systems on irregular, non-Euclidean domains for nonlinear optimization," *SIAM Journal on Control and Optimization*, vol. 59, no. 1, pp. 635–668, 2021.

[158] W. P. M. H. Heemels, M. K. Camlibel, and M. F. Heertjes, "Oblique projected dynamical systems and incremental stability under state constraints," *IEEE Control Systems Letters*, vol. 4, no. 4, pp. 1060–1065, 2020.

[159] A. Allibhoy and J. Cortés, "Anytime solvers for variational inequalities: the (recursive) safe monotone flows," *Automatica*, 2025, to appear. https://arxiv.org/abs/2311.09527.

[160] G. Delimpaltadakis, J. Cortés, and W. P. M. H. Heemels, "Continuous approximations of projected dynamical systems via control barrier functions," *IEEE Transactions on Automatic Control*, vol. 70, no. 1, pp. 681–688, 2025.

[161] J. Cortés, "Discontinuous dynamical systems – a tutorial on solutions, nonsmooth analysis, and stability," *IEEE Control Systems*, vol. 28, no. 3, pp. 36–73, 2008.

[162] F. Blancini and S. Miani, *Set-theoretic Methods in Control*. Boston, MA: Birkhäuser, 2008.

[163] P. O. M. Scokaert, J. B. Rawlings, and E. S. Meadows, "Discrete-time stability with perturbations: application to model predictive control," *Automatica*, vol. 33, pp. 463–470, 1997.

[164] A. Isaly, M. Ghanbarpour, R. G. Sanfelice, and W. E. Dixon, "On the feasibility and continuity of feedback controllers defined by multiple control barrier functions for constrained differential inclusions," in *American Control Conference*, Atlanta, Georgia, 2022, pp. 5160–5165.

[165] S. M. Robinson, "Generalized equations and their solutions, part II: Applications to nonlinear programming," in *Optimality and Stability in Mathematical Programming*, ser. Mathematical Programming Studies, M. Guignard, Ed. New York: Springer, 1982, vol. 19, pp. 200–221.

[166] M. Alyaseen, N. Atanasov, and J. Cortés, "Safety-critical control of discontinuous systems with nonsmooth safe sets," *Automatica*, 2024, submitted.

[167] E. D. Sontag, "Smooth stabilization implies coprime factorization," *IEEE Transactions on Automatic Control*, vol. 34, no. 4, pp. 435–443, 1989.

[168] M. Cohen, P. Ong, G. Bahati, and A. D. Ames, "Characterizing smooth safety filters via the implicit function theorem," *IEEE Control Systems Letters*, vol. 7, pp. 3890–3895, 2023.

[169] M. Li, Z. Sun, and S. Weiland, "Unifying controller design for stabilizing nonlinear systems with norm-bounded control inputs," *arXiv preprint arXiv:2403.03030*, 2024.

[170] A. V. Fiacco, "Sensitivity analysis for nonlinear programming using penalty methods," *Mathematical Programming*, vol. 10, no. 1, pp. 287–311, 1976.

[171] S. M. Robinson, "Strongly regular generalized equations," *Mathematics of Operations Research*, vol. 5, no. 1, pp. 43–62, 1980.

[172] J. Liu, "Sensitivity analysis in nonlinear programs and variational inequalities via continuous selections," *SIAM Journal on Control and Optimization*, vol. 33, no. 4, pp. 1040–1060, 1995.

[173] A. V. Fiacco and J. Kyparisis, "Sensitivity analysis in nonlinear programming under second order assumptions," *Systems and Optimization*, vol. 66, pp. 74–97, 1985.

[174] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming*. Philadelphia: SIAM, 1994.

[175] B. Stellato, G. Banjac, P. Goulart, A. Bemporad, and S. Boyd, "OSQP: an operator splitting solver for quadratic programs," *Mathematical Programming Computation*, vol. 12, pp. 637–672, 2020.

[176] A. L. Dontchev and R. T. Rockafellar, *Implicit Functions and Solution Mappings: A View from Variational Analysis; 2nd ed.* New York, NY: Springer, 2014.

[177] M. S. Berger, *Nonlinearity and Functional Analysis: Lectures on Nonlinear Problems in Mathematical Analysis.* Elsevier, 1977.

[178] N. Andréasson, A. Evgrafov, and M. Patriksson, *An Introduction to Continuous Optimization: Foundations and Fundamental Algorithms.* Courier Dover Publications, 2020.

[179] N. D. Yen, "Hölder continuity of solutions to a parametric variational inequality," *Applied Mathematics and Optimization*, vol. 31, pp. 245–255, 1995.

[180] D. Kinderlehrer and G. Stampacchia, *An Introduction to Variational Inequalities and Their Applications*, ser. Classics in Applied Mathematics. Philadelphia, PA: SIAM, 1980, vol. 31.

[181] T. Rockafellar, "Lipschitzian properties of multifunctions," *Nonlinear Analysis, Theory, Methods and Applications*, vol. 9, no. 8, pp. 867–885, 1985.

[182] D. Ralph and S. Dempe, "Directional derivatives of the solution of a parametric nonlinear program," *Mathematical Programming*, vol. 70, no. 1, pp. 159–172, 1995.

[183] C. D. Aliprantis and K. C. Border, *Infinite Dimensional Analysis: A Hitchhiker's Guide*, ser. Studies in Economic Theory. New York: Springer, 1999.

[184] W. B. Carver, "Systems of linear inequalities," *Annals of Mathematics*, vol. 23, no. 3, pp. 212–220, 1922.

[185] E. A. Coddington and N. Levinson, *Theory of Ordinary Differential Equations.* New York: McGraw-Hill, 1955.

[186] R. P. Agarwal and V. Lakshmikantham, *Uniqueness and Nonuniqueness Criteria for Ordinary Differential Equations*, ser. Series in Real Analysis. Singapore: World Scientific Publishing, 1993, vol. 6.

[187] A. F. Filippov, *Differential Equations with Discontinuous Righthand Sides*, ser. Mathematics and Its Applications. Kluwer Academic Publishers, 1988, vol. 18.

[188] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[189] M. Maghenem and R. G. Sanfelice, "Sufficient conditions for forward invariance and contractivity in hybrid inclusions using barrier functions," *Automatica*, vol. 124, p. 109328, 2021.

[190] P. Glotfelter, I. Buckley, and M. Egerstedt, "Hybrid nonsmooth barrier functions with applications to provably safe and composable collision avoidance for robotic systems," *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. 1303–1310, 2019.

[191] M. Aicardi, G. Casalino, A. Bicchi, and A. Balestrino, "Closed Loop Steering of Unicycle-like Vehicles via Lyapunov Techniques," *IEEE Robotics and Automation Magazine*, vol. 2, no. 1, pp. 27–35, 1995.

[192] F. P. Kelly, A. K. Maulloo, and D. K. H. Tan, "Rate control in communication networks: Shadow prices, proportional fairness and stability," *Journal of the Operational Research Society*, vol. 49, no. 3, pp. 237–252, 1998.

[193] A. Cherukuri and J. Cortés, "Distributed generator coordination for initialization and anytime optimization in economic dispatch," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, pp. 226–237, 2015.

[194] T. Erseghe, "Distributed optimal power flow using ADMM," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2370–2380, 2014.

[195] L. Xiao and S. Boyd, "Optimal scaling of a gradient method for distributed resource allocation," *Journal of Optimization Theory & Applications*, vol. 129, no. 3, pp. 469–488, 2006.

[196] A. Nedic, A. Ozdaglar, and P. A. Parrilo, "Constrained consensus and optimization in multi-agent networks," *IEEE Transactions on Automatic Control*, vol. 55, no. 4, pp. 922–938, 2010.

[197] A. Cherukuri, E. Mallada, S. H. Low, and J. Cortés, "The role of convexity in saddle-point dynamics: Lyapunov function and robustness," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2449–2464, 2018.

[198] H. Brezis, "On a characterization of flow-invariant sets," *Communications on Pure and Applied Mathematics*, vol. 23, pp. 261–263, 1970.

[199] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Prentice Hall, 2002.

[200] F. Watbled, "On singular perturbations for differential inclusions on the infinite interval," *Journal of Mathematical Analysis and Applications*, vol. 310, no. 2, pp. 362–378, 2005.

[201] X. X. Tan and D. Dimarogonas, "Compatibility checking of multiple control barrier functions for input constrained systems," in *IEEE Conf. on Decision and Control*, Cancún, Mexico, 2022, pp. 939–944.

[202] M. S. Andersen, J. Dahl, and L. Vandenberghe, "CVXOPT: A python package for convex optimization, version 1.1.6." *Available at cvxopt.org, 2013*, 2013.

[203] R. T. Rockafellar, *Convex Analysis*. Princeton University Press, 1970.

[204] H. Tuy, *Nonconvex Quadratic Programming*. New York: Springer, 1998.

[205] J. Park and S. Boyd, "General heuristics for nonconvex quadratically constrained quadratic programming," *arXiv preprint arXiv:1703.07870v2*, 2017.

[206] W. Xiao and C. Belta, "Control barrier functions for systems with high relative degree," in *IEEE Conf. on Decision and Control*, Nice, France, Dec. 2019, pp. 474–479.

[207] G. Yang, C. Belta, and R. Tron, "Self-triggered control for safety critical systems using control barrier functions," in *American Control Conference*, Philadelphia, USA, Jul. 2019, pp. 4454–4459.

[208] W. Tan, "Nonlinear control analysis and synthesis using sum-of-squares programming," Ph.D. dissertation, University of California, Berkeley, 2006.

[209] H. Dai, C. Jian, H. Zhang, and A. Clark, "Verification and Synthesis of Compatible Control Lyapunov and Control Barrier Functions," in *IEEE Conf. on Decision and Control*, Milan, Italy, 2024, pp. 8178–8185.

[210] C. Dawson, Z. Qin, S. Gao, and C. Fan, "Safe nonlinear control using robust neural Lyapunov-barrier functions," in *Conference on Robot Learning*, London, UK, 2021.

[211] Y.-C. Chang, N. Roohi, and S. Gao, "Neural Lyapunov control," in *Conference on Neural Information Processing Systems*, vol. 32, Vancouver, Canada, Dec. 2019, pp. 3240–3249.

[212] H.Ravanbakhsh and S. Sankaranarayanan, "Learning control Lyapunov functions from counterexamples and demonstrations," *Autonomous Robots*, vol. 43, pp. 275–307, 2019.

[213] R. D. Yates and D. J. Goodman, *Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers*. John Wiley and Sons, 2004.

[214] M. Fliess, J. Lévine, P. Martin, and P. Rouchon, "On differentially flat nonlinear system," in *IFAC Symposium on Nonlinear Control Systems*, Bourdeaux, France, 1992, pp. 408–412.

[215] D. Mellinger and V. Kumar, "Minimum snap trajectory generation and control for quadrotors," in *IEEE Int. Conf. on Robotics and Automation*, Shanghai, China, 2011, pp. 2520–2525.

[216] L. E. Beaver and A. A. Malikopoulos, "Optimal control of differentially flat systems is surprisingly easy," *Automatica*, vol. 159, p. 111404, 2024.

[217] J. Lévine, "On the equivalence between differential flatness and dynamic feedback linearizability," *IFAC Proceedings Volumes*, vol. 40, no. 20, pp. 338–343, 2007.

[218] P. Virtanen, R. Gommers, T. E. Oliphant *et al.*, "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python," *Nature Methods*, vol. 17, pp. 261–272, 2020.

[219] K. Garg, E. Arabi, and D. Panagou, "Fixed-time control under spatiotemporal and input constraints: A quadratic programming based approach," *Automatica*, vol. 141, p. 110314, 2022.

[220] A. A. Ahmadi and A. Majumdar, "Some applications of polynomial optimization in operations research and real-time decision making," *Optimization Letters*, vol. 10, no. 4, p. 709–729, 2016.

[221] A. J. Taylor, V. D. Dorobantu, H. M. Le, Y. Yue, and A. D. Ames, "Episodic learning with control Lyapunov functions for uncertain robotic systems," in *IEEE/RSJ Int. Conf. on Intelligent Robots & Systems*, Macau, 2019, pp. 6878–6884.

[222] K. Long, Y. Yi, J. Cortés, and N. Atanasov, "Distributionally robust Lyapunov function search under uncertainty," in *Learning for Dynamics and Control Conference*, ser. Proceedings of Machine Learning Research, N. Matni, M. Morari, and G. J. Pappas, Eds. PMLR, 2023, vol. 211, pp. 864–877.

[223] N. Srinivas, A. Krause, S. M. Kakade, and M. Seeger, "Gaussian process optimization in the bandit setting: no regret and experimental design," *arXiv preprint arXiv:0912.3995*, 2010.

[224] P. S. Wang, "The undecidability of the existence of zeros of real elementary functions," *Journal of the ACM*, vol. 21, no. 4, pp. 586–589, 1974.

[225] M. Spivak, *Calculus on Manifolds*. Addison-Wesley Publishing Company, 1995.

[226] A. Domahidi, E. Chu, and S. Boyd, "Ecos: An SOCP Solver for Embedded Systems," *European Control Conference*, pp. 3071–3076, 2013.

[227] P. Ong, "Uniting and balancing control objectives: safety, stability, smoothness and resource conservation," Ph.D. dissertation, University of California, San Diego, 2022, electronically available at http://terrano.ucsd.edu/jorge/group/data/PhDThesis-PioOng-21.pdf.

[228] F. Alizadeh and D. Goldfarb, "Second-order cone programming," *Mathematical Programming*, vol. 95, no. 1, pp. 3–51, 2003.

[229] M. S. Lobo, L. Vandenberghe, S. Boyd, and H. Levret, "Applications of second-order cone programming," *Linear algebra and its applications*, vol. 284, pp. 193–228, 1997.

[230] A.-L. Cholesky, "Sur la résolution numerique des systèmes d'équations linéaires," *Bulletin de la société des amis de la bibliothèque de l'École polytechnique*, vol. 39, 2005.

[231] J. Cortés and M. Egerstedt, "Coordinated control of multi-robot systems: A survey," *SICE Journal of Control, Measurement, and System Integration*, vol. 10, no. 6, pp. 495–503, 2017.

[232] S. Diamond and S. Boyd, "CVXPY: A python-embedded modeling language for convex optimization," *Journal of Machine Learning Research*, vol. 17, no. 83, pp. 1–5, 2016.

[233] H. J. Kushner and D. S. Clark, *Stochastic approximation methods for constrained and unconstrained systems*. New York: Springer, 1978.

[234] V. S. Borkar, *Stochastic Approximation A Dynamical Systems Viewpoint*. New Delhi, India: Hindustan Book Agency, 2008.

[235] K. Zhang, A. Koppel, H. Zhu, and T.Başar, "Global convergence of policy gradient methods to (almost) locally optimal policies," *SIAM Journal on Control and Optimization*, vol. 58, no. 6, pp. 3586–3612, 2020.

[236] G. Di Pillo and L. Grippo, "Exact penalty functions in constrained optimization," *SIAM Journal on Control and Optimization*, vol. 27, no. 6, pp. 1333–1360, 1989.

[237] A. Auslender, R. Shefi, and M. Teboulle, "A moving balls approximation method for a class of smooth constrained minimization problems," *SIAM Journal on Optimization*, vol. 20, no. 6, pp. 3232–3259, 2010.

[238] T. Xu, Z. Yang, Z. Wang, and Y. Liang, "Doubly robust off-policy actor-critic: convergence and optimality," in *The 38th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, vol. 139, Virtual Conference, 2021, pp. 11 581–11 591.

[239] J. Huang and N. Jiang, "On the convergence rate of off-policy policy optimization methods with density-ratio correction," in *The 25th International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, vol. 151, Virtual Conference, 2022, pp. 2658–2705.

[240] Q. Bai, W. U. Mondal, and V. Aggarwal, "Regret analysis of policy gradient algorithm for infinite horizon average reward Markov decision processes," in

Proceedings of the 38th AAAI Conference on Artificial Intelligence, Vancouver, Canada, 2024, pp. 10 980–10 988.

[241] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. MIT Press, 2018.

[242] R. Bhatia and C. Davis, "A better bound on the variance," *The American Mathematical Monthly*, vol. 107, no. 4, pp. 353–357, 2000.

[243] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[244] M. Fréchet, "Généralizations du théorème des probabilités totales," *Fundamenta Mathematicae*, vol. 1, no. 25, pp. 379–387, 1935.

[245] W. Rudin, *Principles of Mathematical Analysis*. McGraw-Hill, 1953.

[246] K. Zhang, A. Koppel, H. Zhu, and T.Başar, "Global convergence of policy gradient methods to (almost) locally optimal policies," *arXiv preprint arXiv:1506.08472*, 2020.

[247] Y. Nesterov, *Lectures on Convex Optimization*, 2nd ed., ser. Springer Optimization and Its Applications. Springer International Publishing, 2018, vol. 137.

[248] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," 2017.

[249] C. Dawson, S. Gao, and C. Fan, "Safe control with learned certificates: A survey of neural Lyapunov, barrier, and contraction methods," *arXiv preprint arXiv:2202.11762*, 2022.

[250] K. P. Wabersich and M. N. Zeilinger, "Predictive control barrier functions: enhanced safety mechanisms for learning-based control," *IEEE Transactions on Automatic Control*, vol. 68, no. 5, pp. 2638–2651, 2023.

[251] M. Krstic, "Inverse optimal safety filters," *IEEE Transactions on Automatic Control*, vol. 69, no. 1, pp. 16–31, 2024.