Stabilization with Guaranteed Safety of Nonlinear Systems

Romdlony, Muhammad Zakiyullah

Stabilization with Guaranteed Safety of Nonlinear Systems

Muhammad Zakiyullah Romdlony

university of groningen

The research described in this dissertation has been carried out at the Engineering and Technology Institute (ENTEG), Faculty of Science and Engineering, University of Groningen, The Netherlands.

disc

This dissertation has been completed in partial fulfillment of the requirements of the Dutch Institute of Systems and Control (DISC) for graduate study.

Printed by Ipskamp Drukkers
Enschede, The Netherlands

ISBN (book): 978-94-034-0417-2
ISBN (e-book): 978-94-034-0418-9

university of groningen

Stabilization with Guaranteed Safety of Nonlinear Systems

PhD thesis

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus Prof. E. Sterken
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

Friday 16 February 2018 at 14.30 hours

by

Muhammad Zakiyullah Romdlony

born on Friday 30 May 1986
in Tasikmalaya, Indonesia

Supervisors
Prof. B. Jayawardhana
Prof. J.M.A. Scherpen

Assessment committee
Prof. A. van der Schaft
Prof. R. Wisniewski
Prof. L. Xie

To the almighty God

Acknowledgments

Alhamdulillah. All praise is for Allah, with his mercy I can complete my PhD journey.

The completion of my PhD is not possible without help and support of many colleagues.

First of all, I would like to thank my mentor, my supervisor, and my first promotor Prof. dr. Bayu Jayawardhana for his patience in guiding me during my four years PhD period. The fruitful discussions with him have triggered my curiosity to conduct the research professionally. I also appreciate him for accompanying me to the USA for the IFAC conference and for supporting me to attend other conferences, workshops and courses. It really improved my knowledge and let me build my research network around the world.

Secondly, I would like to thank my second promotor, Prof. dr. ir Jacquelien M.A. Scherpen for her academic guidance, advises, and comments.

Thridly, I want to thank my roommates, Bao, Jesus, and Nelson for the academic and non-academic discussion. I also point out my gratitude to Rully, Desti, Frederika, and all members of DTPA and SMS.

Fourthly, I want to thank muslim communities in Groningen, e.g. deGromiest, PPIG, Selwerd mosque, Eyup mosque, and all muslim communities around the Netherlands. I also really enjoyed the opportunity to spread the beauty of the Quran to Indonesian communities in many cities, IMEA Enschede, KEMUNI Nijmegen, SGB Utrecht, Pengajian Wageningen, KALAMI Ridderkerk and others. I also enjoyed deGromiest's *tadarus, halaqoh Al Quran* and deGromiest's trip to Turkey for learning the history of Islam.

Fifthly, I want to thank my table tennis coaches in GSTTV Idefix, Koos Kuiper and Thomas Groenevelt who improved my table tennis skills significantly such that I won the Proclamation cup held by Indonesian embassy in The Hague in 2015, and became three times runner-up of Groenscup in 2013, 2014, and 2016. I will fulfill your last command to keep playing table tennis in Indonesia.

The last is for my family. I would like to thank my parents for supporting

me. I also thank my wife Sella for supporting me during my PhD period and for accompanying me travel to many countries. I enjoyed our Ramadan 2015 in Morocco. For my son Faqih Brilly: ”You should be better than me!”.

Contents

Chapter 1

Introduction

Chapter 1
Introduction

With recent surge of research interests in cyber-physical systems and in networked control systems, safety verification and safety control have become an integral part of the control design. Moreover, since cyber-physical systems connect control and computation with physical systems, the control systems must also guarantee systems' safety in both cyber and physical domains. For safety-critical systems, such as autonomous vehicles, chemical plants, manufacturing and robotic systems, where both human operator and the process itself might be at risk whenever certain unsafe states are reached, there are extra high-level performance specifications that should be addressed, i.e. stabilization requirements while guaranteeing safety specifications. Thus it is imperative to avoid unsafe states while controlling them. Consequently the design of feedback stabilizing controller must comply with state constraints, avoid unsafe states and adhere to input constraints. In this thesis, we will focus mainly on this safety aspect in the design of control systems.

Let us exemplify the safety control problem by considering a simple illustrating example as shown in Figure 1.1 where it depicts state space of a second order system containing unsafe state domain (as shown in red). In this example, the plant system is simply given by two integrators and the goal of control systems is to avoid the unsafe state (at all cost) while steering the whole state to the origin. In Figure 1.1, we see the trajectories of the closed-loop system (with our controller which will be discussed in Chapter 3) from four different initial conditions. All trajectories are able to avoid the unsafe state and converge to the origin as desired.

When the trajectories do not enter the unsafe state, we call it safe control systems or control systems with guaranteed safety. Throughout this thesis, we will often refer to the latter notion.

The notion of guaranteed safety is closely related to the notion of safety verification. Loosely speaking, for nonlinear systems given by $\dot{x} = f(x)$ where $x \in \mathbb{R}^n$ with the set of unsafe state is denoted by $\mathcal{D} \subset \mathbb{R}^n$ and the set of initial condition $\mathcal{X}_0 \subset \mathbb{R}^n$, the safety verification problem asks for a formal analysis that shows none of the trajectories starting from $\mathcal{X}_0$ enters $\mathcal{D}$ at any positive time. One of such methods is given by barrier certificate as proposed in [44].

The first obvious approach is to compute the reachable sets by propagating initial conditions $x(0) \in \mathcal{X}_0$ forward in time. However, that solution is expensive and

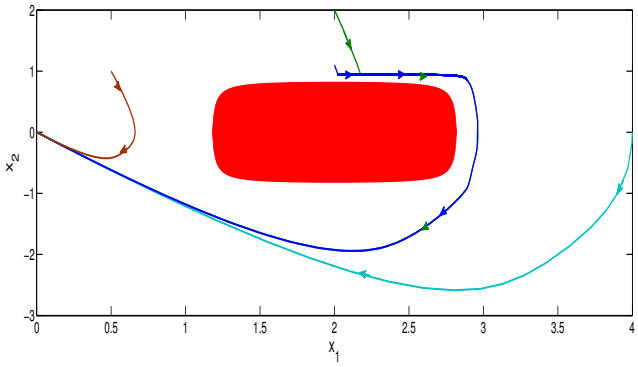

Figure 1.1: *A simulation result of a second-order system whose main goal is to avoid unsafe state while at the same time to converge to the origin The unsafe state is depicted in red area and the trajectories start from four different initial conditions.*

computationally exhaustive. It is often not possible to obtain the exact reachable sets and leads to the approximate solution.

The second approach involves the use of a function so called *barrier certificate* as proposed in [44]. The existence of that function implies the safety of the systems. This method is analogous to the Lyapunov method which can be used to analyze state trajectories behavior without the need to specifically calculate those trajectories.

The work presented throughout this thesis is based on the second approach, i.e. using both barrier certificate and Lyapunov function to analyze and synthesize safe and stable trajectories, respectively. In particular, we will discuss various control design strategies that achieve stability and safety property simultaneously. We also discuss how to measure robustness of safety, since that notion is still lacking in the literature. In the following, we will provide literature overview on topics that are related to our various contributions throughout the thesis.

1.1 Safety control systems

The problem of control systems with guaranteed safety can be regarded as control systems with (state) constraints where in this case the set of unsafe state is defined in the constraints.

There are several control design methods proposed in literature that deal with (non-)linear constraints for (non-)linear systems. For example, Model Predictive Control-based approach has been proposed in [11, 34, 36] and the use of reference governor has been proposed in [9, 10, 20]. Both approaches lead to a high-level

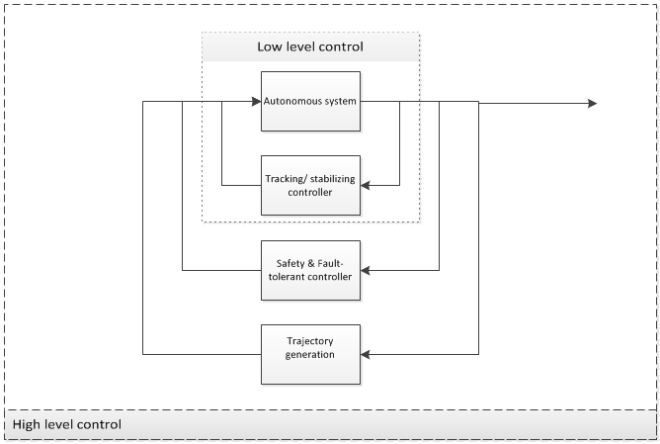

Figure 1.2: *Standard multi-level control configuration*

controller that generates admissible reference signals for the low-level controller, in order to avoid violating the constraints. Another control design approach for dealing with constraint is the invariance control principle proposed in [21, 63].

An implicit assumption in these works is that time-scale separation can be applied to the stabilization (fast-time scale) and to the safety control (slow-time scale), i.e., safety is not considered as a time-critical issue. They fall to the control configuration as depicted in Figure 1.2.

Since we are interested also with time-critical systems, in this thesis we consider a control configuration that put the stabilization and safety control in the same control level, i.e. both should work on the same time scale as shown in Figure 1.3. Based on this configuration, we propose in Chapter 3 a novel control design method of Control Lyapunov-Barrier Function (CLBF) which merges a well-known Control Lyapunov Function (CLF) and recent method of Control Barrier Function (CBF).

For the past few years, a number of control design methods has been proposed in literature on the design of feedback controller that can guarantee both the safety and stability, simultaneously. To name a few, we refer interested readers to [1], [64], [52] and [53]. In [1] and [64], the authors proposed an optimization problem, in the form of a quadratic programming, where both control Lyapunov and control Barrier inequalities are formulated in the constraints. The proposed method generalizes the well-known pointwise min-norm control method for designing a control law using Control Lyapunov Functions via an optimization problem [48]. It has been successfully implemented in the cruise control of autonomous vehicle as reported in [35]. Another direct approach is pursued by us in [49, 53] and presented in Chapter 3 of this thesis which is based on the direct merging of Control

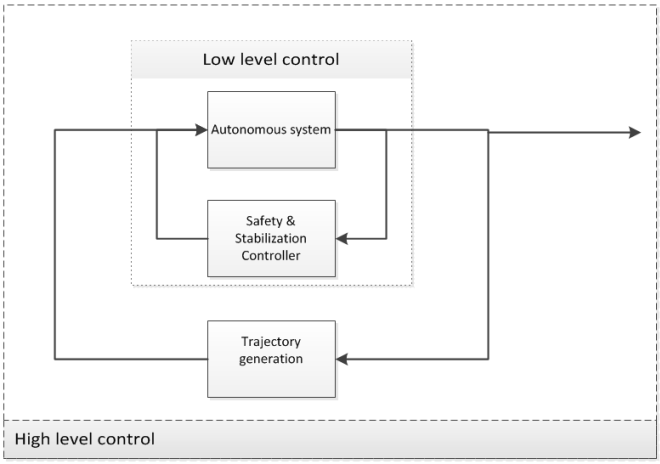

Figure 1.3: *Proposed control configuration for time-critical systems where the safety and stabilizing controllers are active on the same time-scale.*

Lyapunov Function and Control Barrier Function. The merging process results in a Control Lyapunov-Barrier Function which can be used to stabilize the system with guaranteed safety by using Sontag's universal control law.

1.2 Input-to-state safety notion

Despite the appealing idea in the aforementioned works for guaranteeing stability and safety, it remains unclear on how to analyze the robustness of the closed-loop system in the presence of external (disturbance) input signals.

When we deal with stability analysis of a control system, there are many robustness concepts that can be used to quantify the robustness of control system. For instance, robust control theory with H_∞ and L_2-stability notions [24, 55] has become seminal in 90s. It becomes one of the cornerstones in modern control theory. In early 2000, the notions of input-to-state stability (ISS) and integral input-to-state stability (iISS) [56] have played an important role in the robustness analysis of nonlinear control systems and the interconnection of such systems. However, the robustness analysis with an emphasis on safety aspect is still lacking in literature.

In this thesis, we discuss robustness analysis tools for safety certification of safety-critical cyber-physical systems. In particular, in Chapter 4 we introduce a notion of input-to-state safety (ISSf) that captures the dynamical effect of external disturbance/input signals to the safety of the systems. The notion can be used to describe the robustness of a number of safety control designs which have recently

been proposed in literature. To name a few, we refer to our approach based on Control Lyapunov-Barrier Function in [52, 53] and to the min-norm control approach using quadratic programming as in [1, 35, 64].

1.3 Energy-based control systems with guaranteed safety

In recent years, energy-based control design methods have become appealing in the stabilization of nonlinear systems due to its affinity with the physical quantity of energy and power exchanges between different physical systems. For instance if we deal with complex systems which consist of several domains such as electrical, mechanical, thermal, elctromagnetic, etc, we can unify these different physical model of systems in several energy-based framework, e.g., Euler Lagrange [38] and port-Hamiltonian [18] structure. The method for controlling the electromechanical system such as robotics and AC machinery via Passivity-Based Control (PBC) has been addressed in [38]. There have been several energy-based control methods proposed in the literature. To name a few, [8, 13, 14, 19, 28, 39, 40, 41, 42].

In particular, the port-Hamiltonian framework has been popular in the last decade, thanks to its clear physical interpretations. Interconnection between two or more port-Hamiltonian (which is passive) is realized through ports, and the resulting systems is port-Hamiltonian (and passive) [18, 55]. This property is useful, especially in PBC to address the complex systems.

In order to regulate the behavior of the systems, one can assign the desired port-Hamiltonian structure, by designing the desired interconnection and damping matrices, and its Hamiltonian function. This method is termed Interconnection and Damping Assignment Passivity-Based Control (IDA-PBC) [12, 41, 42]. The recent development of IDA-PBC approach has been addressed in [8]. In this paper, the notion of simultaneous IDA-PBC was introduced. The splitting of design process (energy shaping and damping injection) was omitted, i.e., the desired interconnection and damping matrices were designed simultaneously.

Inspired by the aforementioned passivity-based control methods, we investigate also in this thesis the extension of IDA-PBC design approach to the problem of stabilization with guaranteed safety.

In Chapter 5, we study the control design with guaranteed safety via IDA-PBC approach. We show that the standard IDA-PBC method can be extended to the safety control problems. We also show how to achieve global stabilization with guaranteed safety using hybrid control technique.

1.4 Contributions

The contributions of this thesis are three fold. Our first main contribution is on the control design of safety control systems by combining the standard control Lyapunov function (CLF) approach with the control barrier function (CBF) method. Our second contribution is on the robustness analysis of safety control systems where we introduce the notion of input-to-state safety. Our third contribution is on the passivity-based control design method that incorporates guarantee on the safety.

In our first contribution, as presented in Chapter 3, we study the problem of stabilization with guaranteed safety where two control problems, namely, stabilization and safety control, are combined. We introduce such problem in Section 3.2. In this chapter, we are looking for ways to combine the well-known CLF-based control design with the recently introduced CBF-based control design. Both use the universal control law as proposed by Sontag. The CLF-based method is popular due to its simplicity and generality. In a similar manner, the CBF-based method aims to emulate the simplicity of the CLF approach for guaranteeing the safety of closed-loop systems. The commonality between these two approaches implies that they can be combined directly. However, as discussed in Chapter 3, the convex combination of the two functions may have an undesired effect of shifting the equilibrium point. In Section 3.3, we present our proposed control design method which is based on a linear combination of CLF and compactly supported CBFs. This solution preserves the simplicity of the original solution and in particular, we can still apply the same universal control law to the combined control Lyapunov-Barrier function. In Section 3.4, we extend this result to the case when the domain of the unsafe state comprises of a finite number of compact sets. We implement our proposed methods to two examples in Section 3.5. The first one is related to the control of a nonlinear mechanical system with guaranteed safety and the second one is related to control of a mobile robot with guaranteed safety.

In our second contribution, as presented in Chapter 4, we study the robustness analysis corresponding to the safety control system as discussed in the preceding chapter, i.e., Chapter 3. This is highly relevant in practice where there are external disturbances that can jeopardize our safety control systems. Firstly, in Section 4.2, we provide a review on the barrier certificate that has been widely used to provide certification of safety for autonomous systems. Then in Section 4.3, we propose our robustness notion of input-to-state safety (ISSf) where we modify the well-known input-to-state safety inequality into the one that is suitable for safety control systems. Based on this new notion, we provide sufficient conditions using an ISSf Lyapunov-barrier function satisfying some conditions that are similar to the popular ISS Lyapunov function. In Sections 4.4 and 4.5, we study the particular case of exponential rate ISSf inequality that is pertinent for linear systems, as well

as, nonlinear systems admitting quadratic Lyapunov-barrier functions.

In our final contribution, as written in Chapter 5, we investigate the safety control problem from the perspective of the passivity-based control approach. In this case, we generalize the standard Interconnection and Damping Assignment Passivity-Based Control (IDA PBC) method to the stabilization with guaranteed safety case. In particular, in Section 5.3, we present our extension of IDA PBC to our safety control problem. The resulting conditions resemble those of the original IDA PBC with the exception that the resulting passivity-based Lyapunov function may contain many minima which are not present / assumed in the standard IDA PBC. This gives rise to multiple equilibria and although the safety aspect can always be guaranteed with such method, the stabilization to the desired position may not be global. In order to circumvent this, we introduce a hybrid control solution with a minimum of two states automata. The first automaton is responsible for guaranteeing safety using the IDA PBC while the second automaton is used to steer all trajectories from the neighborhood of undesired equilibria to the desired one.

1.5 Publications

Several peer-reviewed journal and conference papers contributing to this thesis are as follows.

Journal papers

- ”Stabilization with guaranteed safety using Control Lyapunov-Barrier Function”, Automatica, Volume 66, Pages 39-47. (Chapter 3 of this thesis)
- ”Robustness Analysis of Systems’ Safety through a New Notion of Input-to-State Safety”, *ArXiv: 1702.01794*. (Chapter 4 of this thesis)
- ”Passivity-Based Control with Guaranteed Safety”, *Submitted*. (Chapter 5 of this thesis)

Conference papers

- ”Uniting control Lyapunov and control barrier functions”, 53rd IEEE Conference on Decision and Control, December 15-17, 2014, Los Angeles, CA, USA. (Chapter 3 of this thesis)
- ”Passivity-based control with guaranteed safety via interconnection and damping assignment” , 5th IFAC Conference on Analysis and Design of Hybrid Systems, October 14-16, 2015, Atlanta, GA, USA. (Chapter 5 of this thesis)
- ”On the new notion of Input-to-State Safety”, 55th IEEE Conference on Decision and Control, December 12-14, 2016, Las Vegas, NV, USA. (Chapter 4 of this thesis)

- ”On the sufficient conditions for input-to-state safety”, 13th IEEE International Conference on Control and Automation, July 3-6, 2017 Ohrid, Macedonia. (Chapter 4 of this thesis)

Some materials on this thesis have been also partially presented at (local) scientific meetings as follows.

Conference abstracts

- ”On the Construction of Control Lyapunov-Barrier Function”, 34th Benelux Meeting on Systems and Control, March 24-26, 2015, Lommel, Belgium.
- ”Stabilization with guaranteed safety via IDA-PBC” 35th Benelux Meeting on Systems and Control, March 22-24, 2016, Soesterberg, The Netherlands.

Poster

- ”Stabilization with Guaranteed Safety Using CLBF”, ENTEG PhD Meeting, October 8, 2016, Groningen, The Netherlands.

1.6 Thesis Outline

This thesis is organized as follows. Chapter 2 starts with preliminaries that provide necessary theoretical backgrounds for the subsequent chapters. It includes preliminaries on stabilization via CLBF, robustness analysis of systems' stability, and IDA-PBC.

Chapter 3 discusses the concept of stabilization with guaranteed safety for affine nonlinear systems. Chapter 4 discusses a new notion of input-to-state safety to quantify the robustness of the systems' safety in the presence of disturbance signals. Chapter 5 discusses IDA-PBC design method with guaranteed safety that is applied to port-Hamiltonian systems. The conclusions and future works are given in Chapter 6.

Chapter 2

Preliminaries

Chapter 2
Preliminaries

In this chapter we will review relevant existing results on stabilization and safety control of (non-) linear systems, interconnection and damping assignment passivity-based control (IDA-PBC), and input-to-state stability (ISS) which will be elemental throughout the rest of the thesis. We will summarize some standard results on stabilization of non-linear systems based on the use of Control Lyapunov Function in Section 2.1. The results in this section will be useful to our contribution in Chapter 3 where we introduce Control Lyapunov-Barrier Function for achieving simultaneous stabilization and safety control of nonlinear systems. In Section 2.2, we will review well-known results on IDA-PBC control design method. The results in this section will be recalled in Chapter 5 where we present our IDA-PBC with guaranteed safety. In Section 2.3 and 2.4, we present preliminaries on safety verification and safety analysis which are based on the use of barrier certificate. The preliminaries in these two sections are relevant for all subsequent chapters. Finally, in Section 2.5, we review a robustness analysis tool for nonlinear systems which is based on the concept of input-to-state stability (ISS). It will be used later in Chapter 4 when we discuss our new notion of input-to-state safety.

2.1 Stabilization of (non-)linear systems

2.1.1 Stabilization problem

Consider a nonlinear affine system in the form of

$$\dot{x} = f(x) + g(x)u, \qquad x(0) = x_0, \tag{2.1}$$

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^p$ denote the state and the control input of the system, respectively. We assume also that the functions $f(x)$ and $g(x)$ are smooth, $f(0) = 0$, and $g(x) \in \mathbb{R}^{n\times p}$ is full rank [1] for all x. As usual, we define $L_fV(x)$ and $L_gV(x)$ by $L_fV(x) := \frac{\partial V(x)}{\partial x} f(x)$ and $L_gV(x) := \frac{\partial V(x)}{\partial x} g(x)$. A function $V : \mathbb{R}^n \to \mathbb{R}$ is called *proper* if the set $\{x|V(x) \leqslant c\}$ is compact for all constant $c \in \mathbb{R}$, or equivalently, V is

[1] Here, the rank of matrix function $g(x)$ is defined as the number of linearly independent rows/columns in $g(x)$.

radially unbounded. The space $\mathcal{C}^1(\mathbb{R}^l, \mathbb{R}^p)$ consists of all continuously differentiable functions $F : \mathbb{R}^l \to \mathbb{R}^p$.

Stabilization control problem: Given the system (2.1) with a given set of initial conditions $\mathcal{X}_0$, design a feedback law $u = \alpha(x)$ such that the closed loop system is asymptotically stable, i.e. $\lim_{t\to\infty} \|x(t)\| = 0$. Moreover, when $\mathcal{X}_0 = \mathbb{R}^n$ we call it the *global stabilization problem*.

In nonlinear control theory, there have been several existing approaches for designing (globally) asymptotically stabilizing feedback such as backstepping, forwarding, feedback linearization, passivation, and others. In the following, we adopt a stabilizer design procedure of Control Lyapunov Function (CLF) using universal control formula proposed in [58]

2.1.2 Stabilization via CLF

In the following, let us recall some basic results related to Control Lyapunov Functions and its universal control laws (see also [58]).

A proper, positive-definite function $V \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}_+)$ that satisfies

$$L_f V(x) < 0 \qquad \forall x \in \{z \in \mathbb{R}^n \backslash \{0\} \mid L_g V(z) = 0\} \tag{2.2}$$

is called a *Control Lyapunov Function* (CLF).

Given a CLF $V \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}_+)$, the system (2.1) has the *Small Control Property* (SCP) with respect to V if for every $\varepsilon > 0$ there exists a $\delta > 0$ such that for every $x \in \mathbb{B}_\delta$

$$\exists u \in \mathbb{R}^p \qquad \text{such that} \qquad \|u\| < \varepsilon \quad \text{and} \qquad L_f V(x) + L_g V(x) u < 0.$$

We define a function $k : \mathbb{R} \times \mathbb{R} \times \mathbb{R}^p \to \mathbb{R}^p$ by

$$k(\gamma, a, b) = \begin{cases} -\frac{a + \sqrt{a^{2+\gamma\|b\|^4}}}{b^T b} b & \text{if} \quad b \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{2.3}$$

Using the notions of CLF and small-control property, Sontag in [58] has proposed a universal control law as summarized in the following theorem.

Theorem 2.1. *Assume that the nonlinear system* (2.1) *has a CLF* $V \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}_+)$ *and satisfies the small-control property w.r.t.* V. *Then the feedback law*

$$u = k(\gamma, L_f V(x), (L_g V(x))^T) \qquad \gamma > 0, \tag{2.4}$$

is continuous at the origin and ensures that the closed-loop system is globally-asymptotically stable.

2.2 Stabilization via IDA-PBC

Consider a non-linear affine system described by

$$\dot{x} = f(x) + g(x)u \tag{2.5a}$$
$$y = h(x) \tag{2.5b}$$

where $x(t) \in \mathbb{R}^n$ denotes the state vector, $u(t), y(t) \in \mathbb{R}^m$ denote the control input and the output of the system, respectively. The functions $f(x)$, $g(x)$ and $h(x)$ are $\mathcal{C}^1$, and $g(x)$ and its left annihilator $g^{\perp}(x) \in \mathbb{R}^{(n-m)\times n}$ are full rank for all $x \in \mathbb{R}^n$. For $a \in \mathbb{R}^n$, we define $\mathbb{B}_\epsilon(a) := \{x \in \mathbb{R}^n | \|x - a\| < \epsilon\}$.

Let us now recall the results on the Interconnection and Damping Assignment-Passivity based control (IDA-PBC) design method as discussed in [41].

The IDA-PBC method aims at stabilizing the system (2.5) at a desired equilibrium x^* by designing a feedback law $u = \beta(x)$ that transforms (2.5) into a port-Hamiltonian structure which has a desirable damping component ensuring the asymptotic stability of x^* (which is the minimum of the desired energy function). More precisely, it is stated in the following theorem.

Theorem 2.2. *Suppose that we can design an energy function $H_d : \mathbb{R}^n \to \mathbb{R}$ and interconnection and damping matrices $J_d, R_d : \mathbb{R}^n \to \mathbb{R}^{n\times n}$ such that*

$$g^{\perp}(x)f(x) = g(x)^{\perp}(J_d(x) - R_d(x))\nabla H_d \tag{2.6a}$$
$$\nabla^2 H_d(x^*) > 0 \tag{2.6b}$$
$$J_d(x) = -J_d^{\top}(x) \tag{2.6c}$$
$$R_d(x) = R_d^{\top}(x) > 0 \tag{2.6d}$$

where $x^* = \arg\min H_d(x)$ is the desired equilibrium. Then, the stabilizing feedback law $u = \beta(x)$ via IDA-PBC is given by

$$\beta(x) = (g^{\top}(x)g(x))^{-1}g^{\top}(x)((J_d(x) - R_d(x))\nabla H_d(x) - f(x)). \tag{2.7}$$

Using this control law, the closed-loop system can be represented as a port-Hamiltonian system in the form of

$$\dot{x} = (J_d(x) - R_d(x))\,\nabla H_d(x) \tag{2.8}$$

where x^* is (locally) stable equilibrium point. Furthermore, x^* is asymptotically stable if it is an isolated minimum, and is globally stable if H_d is proper and x^* is the largest invariant set of (2.8) *in $\{x \in \mathbb{R}^n | -\nabla^{\top} H_d(x)R_d(x)\nabla H_d(x) = 0\}$.*

We define $\mathcal{E} := \{x \mid \nabla H_d(x) = 0\}$ as a set of equilibria which contains also the desired equilibrium point x^*. As will be shown later, our construction of H_d using IDA-PBC for solving the stabilization with guaranteed safety problem (which will

be defined shortly) may result in $\mathcal{E}$ that is not a singleton. Thus, the sole use of IDA-PBC may only stabilize x^* locally although the closed-loop system is globally safe. In Chapter 5, we show how to modify the IDA-PBC approach for solving the global stabilization case. In this regard, we denote $\mathcal{E}_u := \mathcal{E} \backslash x^*$ as the set of undesired equilibria.

A straightforward generalization of IDA-PBC has recently been proposed in [8] where, instead of restricting the closed-loop system to a particular structure with the interconnection and damping matrices $J_d(x)$ and $R_d(x)$, we can lump both matrices into a single matrix $F_d(x)$ which satisfies

$$F_d(x) + F_d^\top(x) \leqslant 0. \tag{2.9}$$

The new partial differential equation (PDE) that has to be solved is

$$g^\perp(x) f(x) = g^\perp(x) F_d(x) \nabla H_d(x) \tag{2.10}$$

and its corresponding control input is given by

$$u = \beta(x) = \big(g^\top(x) g(x)\big)^{-1} g^\top(x) \big(F_d(x) \nabla H_d(x) - f(x)\big) \tag{2.11}$$

In this case, the resulting port-Hamiltonian closed-loop system is given by

$$\dot{x} = F_d(x) \nabla H_d(x) \tag{2.12}$$

and this control design is often referred to as the Simultaneous IDA-PBC approach.

2.3 Safety analysis

Let us recall few main results in literature on safety analysis. Let $\mathcal{X}_0 \subset \mathbb{R}^n$ be the set of initial conditions and let an open and bounded set $\mathcal{D} \subset \mathbb{R}^n$ be the set of unsafe states, where we assume that $\mathcal{D} \cap \mathcal{X}_0 = \varnothing$. For a given set $\mathcal{D} \subset \mathbb{R}^n$, we denote the boundary of $\mathcal{D}$ by $\partial\mathcal{D}$ and the closure of $\mathcal{D}$ by $\overline{\mathcal{D}}$.

In order to verify the safety of system (2.1) with respect to a given unsafe set $\mathcal{D}$, a Lyapunov-like function which is called barrier certificate has been introduced in [44] where the safety of the system can be verified through the satisfaction of a Lyapunov-like inequality without having to explicitly evaluate all possible systems' trajectories. The barrier certificate theorem is summarized as follows.

Theorem 2.3. *Consider the (autonomous) system* (2.1) *with* $u = 0$*, i.e.,* $\dot{x} = f(x)$ *where* $x(t) \in \mathcal{X} \subset \mathbb{R}^n$*, with a given unsafe set* $\mathcal{D} \subset \mathcal{X}$ *and set of initial conditions*

$\mathcal{X}_0 \subset \mathcal{X}$. Assume that there exists a barrier certificate $B : \mathcal{X} \to \mathbb{R}$ satisfying

$$B(\xi) > 0 \quad \forall \xi \in \mathcal{D} \tag{2.13}$$

$$B(\xi) < 0 \quad \forall \xi \in \mathcal{X}_0 \tag{2.14}$$

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leqslant 0 \quad \forall \xi \in \mathcal{X} \quad \textit{such that} \quad B(\xi) = 0. \tag{2.15}$$

Then the system is safe.

The proof of this theorem is based on the fact that the evolution of B starting from a non-positive value (c.f. (2.14)) will never cross the zero level set due to (2.15), i.e., the state trajectory will always be safe according to (2.13).

Following safety definition in [53], the (autonomous) system (2.1) with $u = 0$ is called *safe* if for all $x_0 \in \mathcal{X}_0$ and for all $t \in \overline{\mathbb{R}}_+$, $x(t) \notin \overline{\mathcal{D}}$. Additionally, (2.1) with $u = 0$ is called (asymptotically) stable with guaranteed safety if it is both (asymptotically) stable and safe.

2.4 Incorporation of safety in control

In order to incorporate the safety aspect into the control design, we modify the safety definition as used in [61] as follows.

Definition 1 (Safety)**.** *Given an autonomous system*

$$\dot{x} = f(x), \qquad x(0) = x_0 \in \mathcal{X}_0, \tag{2.16}$$

where $x(t) \in \mathbb{R}^n$, the system is called safe *if for all $x_0 \in \mathcal{X}_0$ and for all $t \in \overline{\mathbb{R}}_+$, $x(t) \notin \overline{\mathcal{D}}$.*

In the definition of safety as in [61], the safety of any trajectory $x(t)$ is only evaluated in a finite-time interval $[0, T]$ where $T > 0$. If this condition holds for arbitrary $T > 0$, it does not immediately imply that the state trajectory $x(t)$ will not converge to $\partial\mathcal{D}$ as $t \to \infty$. Therefore we add the asymptotic behavior condition to the definition of safety above for excluding such case.

Using this safety definition, the control problem that is considered in [61] is given as follows (see also *Problem 5* in [61]).

Safety control problem: Given the system (2.1) with a given initial condition $\mathcal{X}_0$ and a given set of unsafe states $\mathcal{D} \subset \mathbb{R}^n$, design a feedback law $u = \alpha(x)$ s.t. the closed loop system $\dot{x} = f(x) + g(x)\alpha(x)$, $x(0) = x_0 \in \mathcal{X}_0$ is safe.

In order to solve the above problem and motivated by universal control law based on CLF, Wieland and Allgöwer have recently proposed the concept of Control

Barrier Function in [61]. Let us recall the basic definition of a Control Barrier Function as in [61].

Given a set of unsafe states $\mathcal{D} \subset \mathbb{R}^n$, the function $B \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ satisfying

$$B(x) > 0 \qquad \forall x \in \mathcal{D} \tag{2.17a}$$
$$L_f B(x) \leqslant 0 \qquad \forall x \in \{z \in \mathbb{R}^n \setminus \mathcal{D} | L_g B(z) = 0\} \tag{2.17b}$$
$$\mathcal{U} := \{x \in \mathbb{R}^n | \ B(x) \leqslant 0\} \neq \varnothing \tag{2.17c}$$

is called a *Control Barrier Function* (CBF).

In the following theorem, we present the safety control design method which generalizes the result in [61].

Theorem 2.4. *Assume that the nonlinear system* (2.1) *has a CBF* $B \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ *with a given set of unsafe states* $\mathcal{D} \subset \mathbb{R}^n$*, then the feedback law*

$$u = k(\gamma, L_f B(x), (L_g B(x))^T) \qquad \gamma > 0, \tag{2.18}$$

solves the safety control problem, i.e. the closed-loop system is safe with admissible initial condition $\mathcal{X}_0 = \mathcal{U}$ *with* $\mathcal{U}$ *be as in* (2.17c)*.*
Additionally if

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing \tag{2.19}$$

holds then the closed-loop system is globally safe with $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$*.*

In comparison to Theorem 7 in [61], in Theorem 2.4 we allow the possibility of having an initial state x_0 such that $B(x_0) > 0$ with $x_0 \notin \mathcal{D}$; in particular, in [61] it is assumed that $\mathcal{X}_0 \subset \mathcal{U}$. For completeness, we provide the proof to Theorem 2.4 below.

Proof : The proof of the first claim follows the same line as in the proof of Theorem 7 in [61]. Note that the closed-loop system is given by

$$\dot{x} = f(x) + g(x)k(\gamma, L_f B(x), (L_g B(x))^T) =: F_B(x) \tag{2.20}$$

and it follows from (2.17a)-(2.17c) that the time-derivative of B along the solution of (2.20) satisfies

$$\frac{\partial B(x)}{\partial x} F_B(x) \leqslant 0 \qquad \forall x \in \mathbb{R}^n \setminus \mathcal{D}, \tag{2.21}$$

which implies that B is non-increasing along the trajectory x satisfying (2.20).

For proving the first claim, we consider the case $\mathcal{X}_0 = \mathcal{U}$ such that $B(x(0)) \leqslant 0$ for all $x(0) \in \mathcal{X}_0$. By using (2.21), we also have that B satisfies

$$B(x(t)) - B(x(0)) \leqslant 0 \qquad \forall t \in \mathbb{R}_+. \tag{2.22}$$

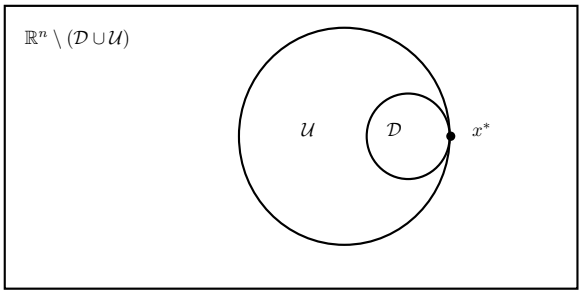

Figure 2.1: *A counter example where we have* $B(x) = 0$ *for all* $x \in \partial\mathcal{D} \nRightarrow (2.19)$.

Therefore $x(t) \in \mathcal{U}$ for all $t \in \mathbb{R}_+$. This proves the first claim since $\mathcal{D} \cap \mathcal{U} = \varnothing$.

We will now prove the second claim where $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$. When $x(0) \in \mathcal{U}$, it has been shown before that $x(t) \in \mathcal{U}$ for all $t \in \mathbb{R}_+$. It remains now to show that for all $x(0) \in \mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$, we have $x(t) \notin \mathcal{D}$ for all $t \in \mathbb{R}_+$. In this case, we note that $B(x(0)) \geqslant 0$ and, as before, B is non-increasing along the trajectory of x for all t.

Since the set $\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})}$ does not intersect with the set $\overline{\mathcal{D}}$, it implies that the trajectory $x(t)$ which starts in $\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$ will not enter $\mathcal{D}$ before it reaches first the boundary of $\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$ (modulo the infinity), in which case, $B(x) = 0$. Once the trajectory $x(t)$ is on the boundary of $\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$, the inequality (2.22) implies that $x(t)$ will remain in $\mathcal{U}$ thereafter. □

Remark 2.5. If (2.17a) and (2.17c) hold, then the condition (2.19) implies that $B(x) = 0$ for all $x \in \partial\mathcal{D}$. Indeed, this can be shown by contradiction. Suppose that there exists $x^* \in \partial\mathcal{D}$ such that $B(x^*) \neq 0$ and (2.19) holds. It follows from (2.17a) that $B(x^*) > 0$. Hence $x^* \in (\mathbb{R}^n \setminus \mathcal{D}) \cap (\mathbb{R}^n \setminus \mathcal{U}) = \mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U}) \subset \overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})}$. Since x^* is also in $\overline{\mathcal{D}}$, we have a contradiction.

However the converse is not true. Figure 2.1 shows graphical illustration of a counter-example to this claim (i.e., $B(x) = 0$ for all $x \in \partial\mathcal{D} \nRightarrow (2.19)$). In this counter-example, the sets $\overline{\mathcal{D}}$ and $\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})}$ intersect at a single point x^*, which implies that (2.19) does not hold but we have $B(x^*) = 0$ according to (2.17c). One such numerical example of B is given by

$$B(x) = \begin{cases} \text{dist}(x, \partial\mathcal{D}) & \forall x \in \mathcal{D} \\ -\text{dist}(x, \partial\mathcal{D} \cup \partial\mathcal{U}) & \forall x \in \mathcal{U} \\ \text{dist}(x, \partial\mathcal{U}) & \forall x \in \mathbb{R}^2 \setminus \{\mathcal{D} \cup \mathcal{U}\}, \end{cases}$$

where $\mathcal{D} := \mathbb{B}_1\left(\left[\begin{smallmatrix}3\\0\end{smallmatrix}\right]\right)$, $\mathcal{U} := \overline{\mathbb{B}}_4 \setminus \mathbb{B}_1\left(\left[\begin{smallmatrix}3\\0\end{smallmatrix}\right]\right)$ and dist denotes the usual set distance. In this numerical example, $\partial\mathcal{D}$ and $\partial\mathcal{U}$ intersect only at $\left[\begin{smallmatrix}4\\0\end{smallmatrix}\right]$.

2.4.1 Handling state and output constraint

Unsafe state or constraint can usually emerge in state or output due to physical limitation of the systems, for example, saturation or due to performance specification. There are several existing approaches for handling constraints in state and in output. One of them is based on barrier Lyapunov method as proposed in [60]. Let us recall the result.

Lemma 2.6. *For any $a, b \in \mathbb{R}_+$, let $\mathcal{X}_c := \{x_c \in \mathbb{R} : -a < x_c < b\}$ and $\mathcal{X} := \mathbb{R}^l \times \mathcal{X}_c \subset \mathbb{R}^{l+1}$. Consider a nonlinear system*

$$\dot{x} = f(x), \quad x := [x_c, x_f]^T \in \mathcal{X}, \quad f : \mathbb{R}_+ \times \mathcal{X} \to \mathbb{R}^{l+1} \tag{2.23}$$

where x_c is constrained state, x_f is free state. Suppose that there exist a barrier function $B : \mathcal{X}_c \to \mathbb{R}_+$ and a Lyapunov function $V : \mathbb{R}^l \to \mathbb{R}_+$ such that

$$B(x_c) \to \infty, \quad x_c \to -a \quad \textit{or} \quad x_c \to b \tag{2.24}$$

$$\alpha(\|x_f\|) \leqslant V(x_f) \leqslant \beta(\|x_f\|) \tag{2.25}$$

where $\alpha, \beta \in \mathcal{K}_\infty$. Let $W(x) := B(x_c) + V(x_f)$, and $x_c(0) \in (-a, b)$. If

$$\dot{W} = L_f W \leqslant 0 \tag{2.26}$$

then $x_c(t) \in (-a, b), \quad \forall t$.

Remark 2.7. The above lemma involves barrier function B and standard Lyapunov function V. In this approach, there is separation of the state space $x \in \mathcal{X}$ between constrained state x_c and free state x_f. Barrier function B is designed to prevent the state x_c from violating the constraints, (i.e. crossing the limits $-a$ and b) by pushing the value of B to be infinity or unbounded as x_c approach the boundary of x_c. This will restrict the applicability of the approach.

In our approach which will be discussed later in Chapter 3 we do not impose unbounded condition on the boundary of unsafe state domain, and we also consider more general problem where the constraint or unsafe state can be any open and bounded set in state domain (in contrast to this lemma that consider saturation-like constraint only).

2.5 Stability robustness analysis via ISS

Consider again affine non-linear system described by

$$\dot{x} = f(x) + g(x)u, \qquad x(0) = x_0, \tag{2.27}$$

where $x(t) \in \mathbb{R}^n$ denotes a state vector, $u(t) \in \mathcal{U} \subseteq \mathbb{R}^m$ denotes an (external) input or disturbance to the system. The functions $f(x)$ and $g(x)$ are $\mathcal{C}^1$ where the space $\mathcal{C}^1(\mathbb{R}^l, \mathbb{R}^m)$ consists of all continuously differentiable functions $F : \mathbb{R}^l \to \mathbb{R}^m$. Without loss of generality and for simplicity of presentation, we will assume throughout that the solution to (2.27) is complete (i.e., it exists for all $t \geqslant 0$) for any bounded signal u. This assumption holds when the system has the input-to-state stability (ISS) property which we will recall shortly.

For a given signal $x : \mathbb{R}_+ \to \mathbb{R}^n$, its L^p norm is given by $\|x\|_{L^p} := (\int_0^\infty \|x(t)\|^p dt)^{1/p}$ for $p = [1, \infty)$ and its L^∞ norm is defined by $\|x\|_{L^\infty} := (\text{ess}) \sup_t(\|x(t)\|)$. For a given bounded set $\mathcal{M} \subset \mathcal{X} \subset \mathbb{R}^n$, we define the distance of a point $\xi \in \mathbb{R}^n$ with respect to $\mathcal{M}$ by $|\xi|_{\mathcal{M}} := \min_{a \in \mathcal{M}} \|\xi - a\|$ where $\|\cdot\|$ is a metric norm. We define an open ball centered at a point $a \in \mathbb{R}^n$ with radius $r > 0$ by $\mathbb{B}_r(a) := \{\xi \in \mathbb{R}^n | \|\xi - a\| < r\}$ and its closure is denoted by $\overline{\mathbb{B}}_r(a)$.

We define the class of continuous strictly increasing functions $\alpha : \mathbb{R}_+ \to \mathbb{R}_+$ by $\mathcal{P}$ and denote by $\mathcal{K}$ all functions $\alpha \in \mathcal{P}$ which satisfy $\alpha(0) = 0$. Moreover, $\mathcal{K}_\infty$ denotes all functions $\alpha \in \mathcal{K}$ which satisfy $\alpha(r) \to \infty$ as $r \to \infty$. By $\mathcal{KL}$ we denote all functions $\beta : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $\beta(\cdot, t) \in \mathcal{K}$ for a fixed $t \geqslant 0$ and $\beta(s, \cdot)$ is decreasing and converging to zero for a fixed $s \geqslant 0$. Correspondingly, we also denote by $\mathcal{KK}$ all functions $\mu : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $f(0, 0) = 0$ and $f(s, t)$ is srictly increasing in both arguments.

Analyzing the robustness of systems stability in the presence of an (external) input signal can be done using the input-to-state stability (ISS) framework [57, 58]. Let us briefly recall the ISS concept from [57].

The system (2.27) is called *input-to-state stable* if there exist a $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}$ such that for any $u \in L^\infty$ and $x_0 \in \mathcal{X}_0$, the following inequality holds for all t:

$$\|x(t)\| \leqslant \beta(\|x_0\|, t) + \gamma(\|u\|_{L^\infty([0,t))}). \tag{2.28}$$

In this notion, the functions β and γ in (2.28) describe the decaying effect from a non-zero initial condition x_0 and the influence of a bounded input signal u to the state trajectory x, respectively. The Lyapunov characterization of ISS systems is provided in the following well-known theorem from [57, 58].

Theorem 2.8. *The system* (2.27) *is ISS if and only if there exists a smooth* $V : \mathbb{R}^n \to \mathbb{R}_+$*, functions* $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{K}_\infty$ *and a function* $\gamma \in \mathcal{K}$ *such that*

$$\alpha_1(\|\xi\|) \leqslant V(\xi) \leqslant \alpha_2(\|\xi\|) \tag{2.29}$$

and

$$\frac{\partial V(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -\alpha_3(\|\xi\|) + \gamma(\|v\|) \tag{2.30}$$

hold for all $\xi \in \mathbb{R}^n$ *and for all* $v \in \mathbb{R}^m$.

The notion of ISS and its Lyapunov characterization as above have been seminal in the study of nonlinear systems robustness with respect to the uncertainties in the initial conditions and to the external disturbance signals. For instance, a well-known nonlinear small-gain theorem in [29] is based on the use of β and γ. The study of convergence input convergence state property as in [25] is based on the use of ISS Lyapunov function. However, as mentioned in the Introduction, existing results on robustness have focused on the systems' stability and there is not many attention on the robustness analysis on systems' safety.

Chapter 3

Stabilization with guaranteed safety via CLBF

Chapter 3

Stabilization with guaranteed safety via CLBF

In this chapter, we investigate the case where safety control is time-critical and propose a nonlinear control design that can simultaneously stabilize the closed-loop systems and guarantee the safety of the systems.

Firstly, we discuss the problem of stabilization with guaranteed safety and the concept of Control Lyapunov-Barrier function in Section 3.2. Subsequently we propose control design methods that merge a CBF and a CLF in Section 3.3. We discuss the extension of the proposed method to the multiple CBFs case in Section 3.4. Finally, in Section 3.5, we also provide numerical simulations where in one example we present the design of a stabilizer with guaranteed safety for a nonlinear system and in the other one, we present an example of merging multiple CBFs with a single CLF for the navigation of mobile robots. The results presented in this chapter are based on our published works in [49] and [53].

3.1 Introduction

One of the modern control design tools for the stabilization of affine nonlinear systems is the so-called Control Lyapunov Function (CLF) method. Artstein in [5] has given necessary and sufficient conditions for the existence of such CLF, which has been used to design a universal control law for affine nonlinear systems in [58]. Recently, various Lyapunov-based control designs have been proposed using the same principle as CLF, such as, Passivity Based Control [38, 42], backstepping [31], stabilization via forwarding [45], and contraction-based method [3].

Since CLFs can be designed to meet specific performance criteria, such as, optimality, transient behaviour or robustness properties, the question on how to combine several CLFs for mixed performance objectives has been addressed, to name a few, in [2, 6, 15, 22, 46, 47]. With the exception of combining/merging/uniting CLF approach proposed in [15] that results in a non-smooth CLF, the synthesis of the combined (or merged) CLF is generally achieved by a convex combination of two CLFs where the weights can be state-dependent.

Akin to the CLF method, Wieland and Allgöwer in [61] have proposed the construction of Control Barrier Functions (CBF), where the Lyapunov function is

interchanged with the Barrier certificate studied in [43, 44]. Using a CBF as in [61], one can design a universal feedback law for steering the states from the set of initial conditions to the set of terminal conditions, without visiting the set of unsafe states.

In order to combine the stabilization property of CLF with the safety aspect from the CBF, we study in this chapter a simple control design procedure where we merge a CLF with a CBF. Some previous relevant works, where a barrier function is incorporated explicitly in the CLF control design method, have been proposed in [37] and [60]. In these papers, a stabilization control problem with state saturation is considered which is solved by incorporating explicitly a "barrier function" in the design of a CLF. The resulting CLF has a strong property of being unbounded on the boundary of the state's domain. While in this chapter, we consider a more general problem where the unsafe set can be any form of open and bounded set in the domain of the state. It is solved by combining a CLF and CBF that results in a Control Lyapunov-Barrier Function (CLBF) control design method which does not impose unboundedness condition on the boundary of the unsafe set. Hence we admit a larger class of functions than the former approaches.

As mentioned earlier, there are various results in literature on combining several CLFs for improving control performances, which include the use of convex combination as pursued in Andrieu and Prieur [2] or Grammatico et al [22]. Based on these works, one can intuitively consider to merge or to unite the CLF and CBF for solving the stabilization with guaranteed safety. However, such an approach may not solve the problem. Note that the important features of the CLF for stabilizing the origin are the (local-) convexity and global minimum at the origin. Hence, the merged CLF (as a result of merging multiple CLFs) has these properties and they are inherited from the original CLFs. On the other hand, the important characteristic of the CBF is that it is (locally-)concave with the level-set of zero belongs to the safe domain. Moreover, CBF may not have a global minimum at all. As a result, CBF and CLF cannot be merged using the same principle of merging multiple CLFs. It may shift the desired equilibrium point (away from the origin) and the merged CLF-CBF may not be proper (i.e., the level-set may not be compact). A recent paper on the uniting of CLF and CBF has also appeared in [1] that uses a quadratic programming approach to combine the Lyapunov inequality and Barrier certificate inequality.

Another related control problem in the literature is the obstacle avoidance control problem [16], where the systems are described by a single integrator and the proposed control law is based on a gradient of a particular potential function. Similar works in the context of avoidance control problem for multi-agent systems are [17, 59]. One important characteristic of the potential function in such method is that it grows unbounded as it reaches the boundary of the obstacle (or the set of unsafe state), akin to the works in [37] and [60] which is generally complicated and difficult to construct.

Recently, we have developed a control design technique that combine our results in this chapter with the idea of the Interconnection-and-Damping Assignment Passivity-Based Control (IDA-PBC) (see, for example, [42]) in [52]. Using existing numerical tools for implementing the classical IDA-PBC, our results in [52] enable further development of numerical tools for implementing our control approach.

3.2 Stabilization with guaranteed safety

Let us now consider the incorporation of the safety aspect in standard stabilization problem as follows.

Stabilization with guaranteed safety control problem: Given the system (2.1) with a given set of initial conditions $\mathcal{X}_0$ and a given set of unsafe states $\mathcal{D}$, design a feedback law $u = \alpha(x)$ s.t. the closed loop system is safe and asymptotically stable, i.e. $\lim_{t\to\infty} \|x(t)\| = 0$. Moreover, when $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$ we call it the *global stabilization with guaranteed safety control problem*.

As briefly discussed in the Introduction, one can intuitively consider to merge or to unite the CLF and CBF by a convex combination a'la Andrieu and Prieur [2] or Grammatico et al [22] for solving the above problem. However, such approach may not immediately guarantee the solvability of the problem. Firstly, the convex combination can lead to the shifting of the global minimum of the combined function which can result in the shifting of the equilibrium point away from the origin. This does not happen in the uniting/merging CLFs since each CLF has minimum at the origin. In the extreme case, when the function of $B(x)$ is not lower-bounded, the combined function may not even admit a global minimum. Secondly, we need a theoretical framework to combine the stability analysis via Lyapunov method and the safety analysis via Barrier Certificate. Motivated by the safety analysis using Barrier Certificate (see, for example [44], [62]), we provide below a proposition on the stability with safety.

Proposition 3.1. *Consider an autonomous system*

$$\dot{x} = f(x), \qquad x(0) = x_0, \tag{3.1}$$

with a set of unsafe state $\mathcal{D}$ which is open. Suppose that there exists a proper and lower-bounded function $W \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ such that

$$W(x) > 0 \qquad \forall x \in \mathcal{D} \tag{3.2a}$$

$$L_f W(x) < 0 \qquad \forall x \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) \tag{3.2b}$$

$$\mathcal{U} := \{x \in \mathbb{R}^n | W(x) \leqslant 0\} \neq \varnothing \tag{3.2c}$$

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing \tag{3.2d}$$

then the origin of (3.1) is asymptotically stable and the system (3.1) is safe with $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$.

Proof : We firstly prove that if $x_0 \in \mathcal{X}_0$, then the state trajectory x never enters $\mathcal{D}$, i.e., for all $t \geqslant 0$, $x(t) \notin \mathcal{D}$.

If $x_0 \in \mathcal{U}$ (i.e. $W(x(0)) \leqslant 0$ by definition) then it follows from (3.2b), that $\dot{W} < 0$ thus $W(x(t)) - W(x(0)) < 0$ for all $t \in R_+$. Hence, it implies that $W(x(t)) < 0$ for all $t \in R_+$. In other words, the set $\mathcal{U}$ is forward invariant and $x(t) \notin \mathcal{D}$ for all $t \in R_+$ by (3.2a). Moreover, by the properness of W, the set $\mathcal{U}$ is compact. Note that by the compactness of $\mathcal{U}$, it holds that $\lim_{t\to\infty} x(t) \notin \mathcal{D}$. Now consider the other case when $x_0 \in \mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$. By using the same argument as in the proof of the second claim of Theorem 2.4, the trajectory x will remain in $\mathcal{U}$ and will never enter $\mathcal{D}$.

We will now prove that if $x_0 \in \mathbb{R}^n \setminus \mathcal{D}$ then $x(t) \to 0$ as $t \to \infty$.

Let $x_0 \in \mathbb{R}^n \setminus \mathcal{D}$ which (according to the previous arguments) implies that the trajectory $x(t) \notin \mathcal{D}$ for all $t \geqslant 0$. Correspondingly, it follows from (3.2b) that

$$\begin{aligned} &\frac{d}{dt}W(x(t)) < 0 \qquad \forall x(t) \notin (\mathcal{D} \cup \{0\}) \\ \Rightarrow\ &W(x(t)) < W(x(0)) < \infty \qquad \forall t \geqslant 0. \end{aligned} \tag{3.3}$$

By the properness of W, the last inequality implies that the trajectory x is bounded, and thus it is pre-compact[1], i.e., the closure of $\{x(t) | t \in [0, \infty)\}$ is compact. This implies that the ω-limit set $\Omega(x_0)$ is non-empty, compact, connected and $\lim_{t\to\infty} d(x(t), \Omega(x_0)) = 0$ where d defines the distance[2].

Additionally, since the function $\mathcal{W} := W \circ x$ is an absolutely continuous function of t and bounded from below, (3.3) implies that $\mathcal{W}(t)$ is monotonically decreasing and it has a limit h as $t \to \infty$. On the other hand, for any point ξ in the ω-limit set $\Omega(x_0)$, there is a sequence (t_n) in $\mathbb{R}_+$ such that $t_n \to \infty$ and $x(t_n) \to \xi$. By the continuity of W, $W(\xi) = \lim_n \mathcal{W}(t_n) = h$. Therefore, in the invariant set $\Omega(x_0)$, W is constant and is given by h. Using (3.2b), and the fact that $\mathcal{D} \not\subset \Omega(x(0))$, we have that W is constant only at $x = 0$ and thus $\Omega(x_0) = \{0\}$. Hence,

$$\lim_{t\to\infty} \|x(t)\| = 0.$$

□

We will make a few remarks on the assumptions in Proposition 3.1. When we restrict the state space to $\mathcal{D} \cup \mathcal{U}$, the conditions in (3.2a)-(3.2c) are reminiscent of

[1]The trajectory x in $\mathcal{X}$ is *pre-compact* if it is bounded for all $t \in [0, \infty)$ and for any sequences (t_n) in $[0, \infty)$, the limit $\lim_{n\to\infty} x(t_n)$ exists and is in $\mathcal{X}$ [32].

[2]For the concept of ω-limit set, we refer interested readers to [23, 24, 32].

the conditions in Barrier Certificate theorem (c.f. [43, Prop. 2.18]).

On the other hand, the properness of W together with (3.2b) resemble the standard Lyapunov stability theorem (albeit, in this proposition, we do not impose positive-definiteness of W). The addition of condition (3.2d) is to ensure that the first entry point to the set of $\mathcal{D} \cup \mathcal{U}$ is the boundary of $\mathcal{D} \cup \mathcal{U}$, and not that of $\mathcal{D}$.

Obviously, one can observe from the condition (3.2b) and (3.2c) that the origin lies inside the set of $\mathcal{U}$. Indeed, we can prove this by contradiction. Suppose that $0 \notin \mathcal{U}$. Let $x_0 \in \mathcal{U}$ which implies that $x(t) \in \mathcal{U}$ for all t (following the same argument as in the proof of Proposition 3.1). By (3.2b), $W(x(t))$ is decreasing and converge to a constant. Similar to the last arguments in the proof of Proposition 3.1), the ω-limit set is a singleton $\{0\}$ which is a contradiction.

Let us now present a control design framework for solving the stabilization with guaranteed safety control problem. For this, we introduce the notion of Control Lyapunov-Barrier Function as follows.

Definition 2 (CLBF)**.** *Given a set of unsafe state $\mathcal{D}$, a proper and lower-bounded function $W \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ satisfying*

$$W(x) > 0 \quad \forall x \in \mathcal{D} \tag{3.4a}$$

$$L_f W(x) < 0 \quad \forall x \in \{z \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) | L_g W(z) = 0\} \tag{3.4b}$$

$$\mathcal{U} := \{x \in \mathbb{R}^n | W(x) \leqslant 0\} \neq \varnothing \tag{3.4c}$$

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing \tag{3.4d}$$

is called a Control Lyapunov-Barrier Function (CLBF).

Using this notion and Proposition 3.1, we can solve the problem in the following theorem.

Theorem 3.2. *Assume that the system* (2.1) *admits a CLBF $W \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ with a given set of unsafe states $\mathcal{D}$ and satisfies the small-control property w.r.t. W, then the feedback law*

$$u = k(\gamma, L_f W(x), (L_g W(x))^T) \qquad \gamma > 0, \tag{3.5}$$

is continuous at the origin and solves the global stabilization with guaranteed safety control problem.

Proof : We prove the theorem by showing that the conditions (3.2a)-(3.2d) in Proposition 3.1 hold for the closed-loop autonomous system

$$\dot{x} = F_W(x)$$

where $F_W(x) := f(x) + g(x)k(\gamma, L_f W(x), (L_g W(x))^T)$.

The conditions (3.2a), (3.2c) and (3.2d) follow trivially from (3.4a), (3.4c) and (3.4d), respectively. Now, for all $x \in \{z \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) \mid L_g W(z) \neq 0\}$, we have that

$$\begin{aligned} L_F W(x) &= L_f W(x) + L_g W(x) k(\gamma, L_f W(x), (L_g W(x))^T) \\ &= -\sqrt{\|L_f W(x)\|^2 + \gamma \|L_g W(x)\|^4} \\ &< 0 \end{aligned}$$

holds. On the other hand, for all $x \in \{z \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) \mid L_g W(z) = 0\}$, the condition (3.4b) implies that

$$L_F W(x) < 0.$$

These two inequalities show that (3.2b) also holds.

The continuity of the feedback law at the origin follows the same proof as in [58]. □

Using the same argument as in the proof of Proposition 3.1, it can be checked that the condition (3.4b) can be weakened by

$$L_f W(x) \leqslant 0 \qquad \forall x \in \mathcal{M},$$

where the CLBF function W is still assumed to be $\mathcal{C}^1$,

$$\mathcal{M} := \{z \in \mathbb{R}^n \setminus \mathcal{D} | L_g W(z) = 0\}$$

and the largest invariant set in $\mathcal{M}$ is $\{0\}$. This condition will be useful later in the simulation result. This is formalized in the following proposition.

Proposition 3.3. *Let $\mathcal{D}$ be a given set of unsafe states. Assume that the system in* (2.1) *has a proper and lower-bounded function $W \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ satisfying*

$$W(x) > 0 \qquad \forall x \in \mathcal{D} \tag{3.6a}$$

$$L_f W(x) \leqslant 0 \ \ \forall x \in \mathcal{M} := \{z \in \mathbb{R}^n \setminus \mathcal{D} \mid L_g W(z) = 0\} \tag{3.6b}$$

$$\mathcal{U} := \{x \in \mathbb{R}^n \mid W(x) \leqslant 0\} \neq \varnothing \tag{3.6c}$$

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing. \tag{3.6d}$$

Assume also that the system is zero-state detectable with respect to $L_g W(x)$, i.e., $L_g W(x(t)) = 0 \ \forall t \geqslant 0 \Rightarrow x(t) \to 0$. Suppose that the system in (2.1) *has the small-control property w.r.t. W. Then the feedback law*

$$u = k\left(\gamma, L_f W(x), (L_g W(x))^T\right) \qquad \gamma > 0, \tag{3.7}$$

is continuous at the origin and solves the global stabilization with guaranteed safety control problem.

Proof : The proof is akin to the proof of Theorem 3.2 and Proposition 3.1. Similar to the proof of Proposition 3.1, if $x_0 \in \mathbb{R}^n \setminus \mathcal{D}$ then the trajectory x will never enter $\mathcal{D}$, i.e., $x(t) \in \mathbb{R}^n \setminus \mathcal{D}$ for all $t \geqslant 0$ and $\mathcal{D} \nsubseteq \Omega(x_0)$.

It remains to show that in the closed-loop system, for every $x_0 \in \mathbb{R}^n \setminus \mathcal{D}$ we have $\Omega(x_0) = \{0\}$. As in the proof of Theorem 3.2, the time-derivative of W satisfies

$$\begin{aligned} L_F W(x) &= -\sqrt{\|L_f W(x)\|^2 + \gamma \|L_g W(x)\|^4} \\ &\leqslant -\sqrt{\gamma}\|L_g W(x)\|^2 \qquad \forall x \in \mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{M}). \end{aligned}$$

On the other hand, for all $x \in \mathcal{M}$, the assumption (3.6b) implies that $L_F W(x) \leqslant 0$. Hence, combining these two inequalities, we have that for all $x(t) \in \mathbb{R}^n \setminus \mathcal{D}$,

$$\dot{W}(x(t)) \leqslant -\sqrt{\gamma}\|L_g W(x(t))\|^2.$$

This inequality implies that W converges to a constant and the trajectory x converges to the largest invariant set $\mathcal{N}$ contained in $\mathcal{M}$, i.e., $\Omega(x_0) \subset \mathcal{N} \subset \mathcal{M}$. By the zero-state detectability assumption with respect to $L_g W$, we have that the largest invariant set $\mathcal{N} = \{0\}$. Hence, $\Omega(x_0) = \mathcal{N} = \{0\}$, i.e., $\lim_{t\to\infty} \|x(t)\| = 0$. □

3.3 Constructive design of a CLBF

Equipped with Theorem 3.2 we can now present results on the construction of CLBF by uniting a CLF and a CBF. This will potentially allow us to separate the control design for achieving the asymptotic stability and safety by designing the CLF and CBF, independently, and then combine them together. In the following proposition, we assume first that B is lower-bounded.

Proposition 3.4. *Suppose that for system* (2.1)*, with a given set of unsafe states $\mathcal{D}$ that is open , there exist a CLF $V \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}_+)$ and a CBF $B \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ which satisfy*

$$c_1\|x\|^2 \leqslant V(x) \leqslant c_2\|x\|^2 \qquad \forall x \in \mathbb{R}^n \qquad c_2 > c_1 > 0, \tag{3.8}$$

and a compact and connected set $\mathcal{X}$ s.t.

$$\mathcal{D} \subset \mathcal{X},\ 0 \notin \mathcal{X} \text{ and } B(x) = -\varepsilon,\ \varepsilon > 0 \qquad \forall x \in \mathbb{R}^n \setminus \mathcal{X}. \tag{3.9}$$

If

$$L_f W(x) < 0 \qquad \forall x \in \{z \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) | L_g W(z) = 0\} \tag{3.10}$$

where

$$W(x) = V(x) + \lambda B(x) + \kappa,$$

with $\lambda > \frac{c_2 c_3 - c_1 c_4}{\varepsilon}$, $\kappa = -c_1 c_4$, $c_3 := \max_{x \in \partial \mathcal{X}} \|x\|^2$, $c_4 := \min_{x \in \partial \mathcal{D}} \|x\|^2$, *then the feedback law* (3.5) *solves the stabilization with guaranteed safety control problem with the set of initial states* $\mathcal{X}_0 = \mathbb{R}^n \backslash \mathcal{D}_{relaxed}$ *where* $\mathcal{D}_{relaxed} := \{x \in \mathcal{X} | W(x) > 0\} \supset \mathcal{D}$. *Moreover if* (2.1) *has the small-control property w.r.t.* V *then it has also the small-control property w.r.t.* W. *In which case, the feedback law* (3.5) *is continuous at the origin.*

Proof : The proof of the proposition will be based on proving that $\mathcal{D} \subset \mathcal{D}_{relaxed}$ and (3.4a)-(3.4d) hold with $\mathcal{D}$ being replaced by $\mathcal{D}_{relaxed}$. Note that (3.4a) holds by the definition of $\mathcal{D}_{relaxed}$. A routine computation shows that for all $x \in \mathcal{D}$,

$$\begin{aligned} W(x) &= V(x) + \lambda B(x) - c_1 c_4 \\ &> c_1 \|x\|^2 - c_1 c_4 \\ &> 0, \end{aligned} \tag{3.11}$$

since $\lambda > 0$, $B(x) > 0$ for all $x \in \mathcal{D}$ and $\|x\|^2 > c_4$ for all $x \in \mathcal{D}$.

Also for all $x \in \partial \mathcal{X}$,

$$\begin{aligned} W(x) &= V(x) + \lambda B(x) - c_1 c_4 \\ &= V(x) - \lambda \varepsilon - c_1 c_4 \\ &\leqslant c_2 \|x\|^2 - \lambda \varepsilon - c_1 c_4 \\ &< c_2 c_3 - (c_2 c_3 - c_1 c_4) - c_1 c_4 = 0, \end{aligned} \tag{3.12}$$

where the strict inequality is due to the hypotheses of $\lambda > \frac{c_2 c_3 - c_1 c_4}{\varepsilon}$. Hence we have that (3.4c) holds. By the continuity of $W(x)$, the inequality (3.11) and (3.12) implies that the open set $\mathcal{D}_{relaxed}$ is the interior of $\mathcal{X}$ and moreover $\mathcal{D} \subset \mathcal{D}_{relaxed}$. Hence $\partial \mathcal{X} \cap \partial \mathcal{D}_{relaxed} = \varnothing$ and we have

$$\mathcal{D} \subset \mathcal{D}_{relaxed} \subset \mathcal{X} \subset \mathcal{D}_{relaxed} \cup \mathcal{U}. \tag{3.13}$$

The last relation is due to the decomposition of $\mathcal{X} = \mathcal{D}_{relaxed} \cup \mathcal{X}_-$ where $\mathcal{X}_- := \{x \in \mathcal{X} | W(x) \leqslant 0\} \subset \mathcal{U}$. Since $\mathcal{D} \subset \mathcal{D}_{relaxed}$, we have that (3.10) $\implies$ (3.4b) (with $\mathcal{D}$ being replaced by $\mathcal{D}_{relaxed}$). Finally, since the boundary of $\mathcal{X}$ does not intersect with the boundary of $\mathcal{D}_{relaxed}$, (3.13) implies that $\overline{\mathbb{R}^n \setminus (\mathcal{D}_{relaxed} \cup \mathcal{U})} \cap \overline{\mathcal{D}_{relaxed}} = \varnothing$, i.e. (3.4d) holds.

The proof on the claim of SCP follows trivially from the hypothesis in (3.9). Indeed, since $0 \notin \mathcal{X}$ and $\mathcal{X}$ being compact, we can define a neighborhood $\mathbb{B}_\delta = \{x | \|x\| < \delta\}$ such that $\mathbb{B}_\delta \cap \mathcal{X} = \varnothing$. In $\mathbb{B}_\delta$ it holds that $L_f W(x) + L_g W(x) = L_f V(x) + L_g V(x)$ since B is constant outside $\mathcal{X}$. Thus if (2.1) has SCP w.r.t V then

it has also SCP w.r.t. W. □

We note that the condition (3.10) implies that the function W has a global minimum in $\mathbb{R}^n \setminus \mathcal{D}$ at 0. This can be shown by contradiction. Suppose that W admits another minimum $x^* \neq 0$ in $\mathbb{R}^n \setminus \mathcal{D}$ such that (3.10) holds. The point x^* being minimum implies that $\frac{\partial W(x^*)}{\partial x} = 0$ so that $L_f W(x^*) = 0$, which contradicts (3.10).

In Proposition 3.4, it is assumed that B is lower-bounded. In general, when the CBF $B(x)$ is not lower-bounded, we can always construct another CBF $\widetilde{B}(x)$ satisfying (3.9) based on $B(x)$ which satisfies (2.17a)-(2.17c). Hence Proposition 3.4 can still be applicable using this new CBF $\widetilde{B}(x)$.

Proposition 3.5. *Suppose that the set of unsafe states $\mathcal{D}$ is bounded and simply-connected. Assume that there exist a CBF $B \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ and $\delta > 0$ such that $\mathcal{J} := \{x | B(x) \geqslant -\delta\}$ is simply-connected, contains $\mathcal{D}$ and B is strictly-concave on $\mathcal{J}$. Let $\rho : \mathbb{R} \to [0, 1]$ be a non-decreasing $\mathcal{C}^1$ function such that $\rho(z) = 0$ for all $z \leqslant -\delta$ and $\rho(z) = 1$ for all $z \geqslant 0$. By using any arbitrary point $\omega \in \partial\mathcal{D}$, define the function $\widetilde{B}(x) \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ by*

$$\widetilde{B}(x) = \begin{cases} B(\omega) + \oint\limits_{\Gamma} \rho(B(\sigma)) \frac{\partial B(\sigma)}{\partial x} d\sigma & \forall x \in \mathcal{J} \\ -\varepsilon & \textit{otherwise}, \end{cases} \tag{3.14}$$

where Γ is any path from ω to $x \in \mathcal{J}$ and the constant ε is defined by $\varepsilon = -\widetilde{B}(\phi)$ where ϕ is any point on $\partial\mathcal{J}$, i.e.

$$\varepsilon = -B(\omega) - \oint\limits_{\Gamma_{\omega \to \phi}} \rho(B(\sigma)) \frac{\partial B(\sigma)}{\partial x} d\sigma,$$

where $\Gamma_{\omega \to \phi}$ is any path from ω to ϕ. Then $\widetilde{B}$ is also a CBF satisfying the conditions (2.17a)-(2.17c) *and also* (3.9) *with $\mathcal{X}$ be given by $\overline{\mathcal{J}}$.*

Proof : We prove the proposition by showing (2.17a)-(2.17c) holds with the same $\mathcal{D}$. Notice that the integration in (3.14) is proper and $\widetilde{B}$ is a potential function. Indeed, it is trivial to check that the Hessian matrix of (3.14) is symmetric and hence, it defines a potential function.

Now, for every $x \in \mathcal{D}$, there exists a path Γ from ω to x since $\mathcal{D}$ is connected and it follows that

$$\widetilde{B}(x) = B(\omega) + \oint\limits_{\Gamma} \frac{\partial B(\sigma)}{\partial x} d\sigma = B(x) > 0$$

where we have used the fact that $\rho(B(\sigma)) = 1$ for all $\sigma \in \Gamma$. Hence (2.17a) holds.

In order to show that (2.17b) holds with the new CBF $\widetilde{B}$, we first note that for all $x \in \mathcal{J}$, we have that $\frac{\partial \widetilde{B}}{\partial x} g(x) = 0 \Leftrightarrow \frac{\partial B}{\partial x} g(x) = 0$. Hence, for all $x \in \{z \in \mathcal{J} \setminus \mathcal{D} | L_g \widetilde{B}(z) = 0\}$ we have

$$\frac{\partial \widetilde{B}}{\partial x} f(x) = \rho(B(x)) \frac{\partial B}{\partial x} f(x) \leqslant 0. \tag{3.15}$$

On the other hand, for all $x \in \mathbb{R}^n \setminus \mathcal{J}$, we have $\frac{\partial \widetilde{B}}{\partial x} = 0$ which implies that $L_f \widetilde{B}(x) = 0, \forall x \in \{z \in \mathbb{R}^n \setminus \mathcal{J} | L_g \widetilde{B}(z) = 0\}$. Together with (3.15), we have that (2.17b) holds.

Equation (2.17c) follows trivially. Now we will prove (3.9), i.e., $\widetilde{B}(x)$ is a negative constant in $\mathbb{R}^n \setminus \mathcal{J}$. By using the concavity of $B(x)$ on $\mathcal{J}$, and since $\mathcal{J} \supset \mathcal{D}$, we have that for any point $\phi \in \partial\mathcal{J}$, $\widetilde{B}(\phi) = -\varepsilon < 0$, i.e., (3.9) holds with $\mathcal{X} = \overline{\mathcal{J}}$. □

One can show easily that the constant ε as calculated in Proposition 3.5 is less than or equal to δ.

As it was shown in the proof of Proposition 3.5, the set $\mathcal{X}$ is closely related to the parameter δ used to define ρ in (3.14). One can immediately check that for every enlargement of $\mathcal{D}$ with a radius of $\mu > 0$, i.e. $\mathcal{D} + \mathbb{B}_\mu$ [3], we can always find $\delta > 0$ such that the resulting $\mathcal{X}$ lies in the interior of $\mathcal{D} + \mathbb{B}_\mu$. This property will be useful later when we want to combine multiple CBFs with a single CLF.

Corollary 3.6. *For every $\mu > 0$ there exists $\delta > 0$ such that $\widetilde{B}(x)$ as constructed in* (3.14) *satisfies* (3.9) *with $\mathcal{X} \subset \mathcal{D} + \mathbb{B}_\mu$.*

Proof : By the continuity of B there exists a neighborhood Ω of $\mathcal{D}$ such that $\Omega \subset \mathcal{D} + \mathbb{B}_\mu$ and $B(\partial\Omega) = -\delta < 0$. The proof of the claim follows the same line as that of Proposition 4. Note that, here $\mathcal{J}$ (as used in the proposition) is given by Ω. □

3.4 Handling multiple sets of unsafe state

In the previous section, we dealt with the problem of combining a CLF with a CBF for designing a CLBF, i.e., it handles only a set of unsafe states $\mathcal{D}$.

For accommodating a general set of unsafe states $\mathcal{D}$, we present in this section a constructive method for combining multiple CBFs and a single CLF. The main assumption in this study is that we can decompose $\mathcal{D}$ into a finite number of disjoint simply-connected sets $\mathcal{D}_1, \mathcal{D}_2 ... \mathcal{D}_N$, each of which admits a CBF. Our main result

[3] Here, we use the Minkowski sum for the set addition.

in Proposition 3.4 cannot directly be used in this case, even if there exists a CBF that covers the multiple sets of unsafe state $\mathcal{D}_1, \mathcal{D}_2 ... \mathcal{D}_N$. Our proposed approach is based on combining the CBFs together to make a CBF which can then be merged with a CLF as before.

Let us assume that the set of unsafe states $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup ... \cup \mathcal{D}_N$ where $\overline{\mathcal{D}_i} \cap \overline{\mathcal{D}_j} = \varnothing$ for all $i \neq j$ and for every i, $\mathcal{D}_i$ is bounded and simply-connected. Suppose that for every i, there exists a CBF B_i for $\mathcal{D}_i$ such that (2.17a)-(2.17c) hold. Using these functions $B_i, i = 1, ...N$, we can construct a family of CBFs B for $\mathcal{D}$ as follows.

By the boundedness of $\mathcal{D}_i$ and since the set $\mathcal{D}_i, i = 1, ..N$ are disjoint, there exist $\mu > 0$ such that the open sets $\mathcal{D}_i + \mathbb{B}_\mu, i = 1, ..N$ are also disjoint. Indeed, by the assumptions, the distance between the sets $\mathcal{D}_i$ and $\mathcal{D}_j$, $i \neq j$, is strictly positive. Hence by choosing $\mu > 0$ such that

$$\mu < \frac{1}{4} \min_{i,j} d(\mathcal{D}_i, \mathcal{D}_j), \tag{3.16}$$

it follows that the sets $\mathcal{D}_i + \mathbb{B}_\mu$ and $\mathcal{D}_j + \mathbb{B}_\mu$, for all $i \neq j$, are disjoint. By Corollary 1, for every i, there exist $\widetilde{B}_i(x)$ and $\delta_i > 0$ (which is constructed using $B_i(x)$ and μ) such that (3.9) holds with $\mathcal{X}_i \subset \mathcal{D}_i + \mathbb{B}_\mu$ and $\varepsilon_i > 0$. Finally, a family of CBFs B for $\mathcal{D}$ is given by

$$B(x) = \sum_i \lambda_i \widetilde{B}_i(x) \tag{3.17}$$

where $\lambda_i \geqslant 0, i = 1, ...N$ are design parameter that can be chosen appropriately when it is merged with a CLF.

In the following proposition, we present a slight modification to Proposition 3.4 where we merge B as in (3.17) with a proper CLF V.

Proposition 3.7. *Assume that for system* (2.1)*, there exists a CLF* $V \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}_+)$ *and CBFs* $\widetilde{B}_i \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ *which satisfy*

$$c_1 \|x\|^2 \leqslant V(x) \leqslant c_2 \|x\|^2 \qquad \forall x \in \mathbb{R}^n, \qquad c_2 > c_1 > 0. \tag{3.18}$$

If

$$L_f W(x) < 0 \qquad \forall x \in \{z \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) | L_g W(z) = 0\} \tag{3.19}$$

where

$$W(x) = V(x) + \sum_i \lambda_i \widetilde{B}_i(x) + \kappa$$

with λ_i *and* κ *be choosen such that*

$$\sum_{j \neq i} \lambda_j \varepsilon_j - c_1 c_{4i} < \kappa < \sum_i \lambda_i \varepsilon_i - c_2 c_{3i} \qquad \forall i, \tag{3.20}$$

$c_{3i} := \max_{x\in\partial\mathcal{X}_i} \|x\|^2, c_{4i} := \min_{x\in\partial\mathcal{D}_i} \|x\|^2$*, then the feedback law* (3.5) *solves the stabilization with guaranteed safety control problem with the set of initial states* $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}_{relaxed}$ *where* $\mathcal{D}_{relaxed} := \{x \in \mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \cup ... \cup \mathcal{X}_N | W(x) > 0\}$.

Proof : The proof follows similar arguments as those in Proposition 3.4. The main differences are in the computation of $W(x) > 0$ for all $x \in \mathcal{D}_i$ and $W(x) < 0$ for all $x \in \partial\mathcal{X}_i$.

For all $x \in \mathcal{D}_i$, it can be checked that

$$\begin{aligned} W(x) &= V(x) + \lambda_i \widetilde{B}_i(x) - \sum_{j\neq i} \lambda_j \varepsilon_j + \kappa \\ &\geqslant c_1 \|x\|^2 - \sum_{j\neq i} \lambda_j \varepsilon_j + \kappa \\ &\geqslant c_1 c_{4i} - \sum_{j\neq i} \lambda_j \varepsilon_j + \kappa > 0, \end{aligned} \tag{3.21}$$

thus (3.4a) holds. Equation (3.4b) holds by the assumption of (3.19). Now it remains to verify (3.4c) and (3.4d).

Note that for all $x \in \partial\mathcal{X}_i$,

$$\begin{aligned} W(x) &\leqslant c_2 \|x\|^2 + \sum_i \lambda_i \widetilde{B}_i(x) + \kappa \\ &= c_2 \|x\|^2 - \sum_i \lambda_i \varepsilon_i + \kappa \\ &\leqslant c_2 c_{3i} - \sum_i \lambda_i \varepsilon_i + \kappa < 0, \end{aligned} \tag{3.22}$$

and hence (3.4c) holds. Similar to Proposition 3.4, (3.21) and (3.22) $\implies$ $\mathcal{D}_{relaxed} \subset \mathcal{X}$ and $\partial\mathcal{D}_{relaxed} \cap \partial\mathcal{X} = \varnothing$, i.e., (3.4d) holds (with $\mathcal{X} = \mathcal{D}_{relaxed} \cup \mathcal{U}$). □

Remark 3.8. It can be shown that the set of λ_i and κ that satisfy (3.20) is non-empty, i.e., the inequalities in (3.20) are solvable. The following algorithm provide a systematic way to design such λ_i and κ.

A1 For every i choose $\lambda_i > 0$ such that $\lambda_i > \frac{c_2 c_{3i} - c_1 c_{4i}}{\varepsilon_i}$.

A2 Choose κ such that $\kappa \in$

$$\left(\sum_i \lambda_i \varepsilon_i - \min_i \lambda_i \varepsilon_i - c_1 \min_i c_{4i}, \sum_i \lambda_i \varepsilon_i - c_2 \max_i c_{3i} \right).$$

Indeed, if we choose λ_i and κ as in (**A1**) and (**A2**), the conditions (3.20) hold.

3.5 Examples

In order to demonstrate the applicability of the developed methods, we will consider two numerical examples, which are described as follows.

3.5.1 Nonlinear mechanical system

Consider the system described by

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= -s(x_2) - x_1 + u,\end{aligned} \tag{3.23}$$

where $x = [x_1\ x_2]^T \in \mathbb{R}^2$, and $u \in \mathbb{R}$. This example can represent a mechanical system where x_1 describes the displacement, x_2 describes the velocity. In this case, the mass is 1, the damping parameter is described by Stribeck friction model $s(x_2) = (0.8+0.2e^{-100|x_2|})\tanh(10x_2)+x_2$ and spring constant is 1. For this system, $f(x) = \begin{bmatrix} x_2 \\ -s(x_2) - x_1 \end{bmatrix}$ and $g(x) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

It can be checked that the system (3.23) admits $V(x) = x_1^2 + x_1x_2 + x_2^2$ as a CLF, i.e. (2.2) holds and it has small control property. Also, the function

$$B(x) = \begin{cases} e^{-\left(\frac{1}{1-(x_1-2)^2}+\frac{1}{1-x_2^2}\right)} - e^{-4} & \forall x \in \mathcal{X} \\ -e^{-4} & \text{elsewhere,} \end{cases} \tag{3.24}$$

where $\mathcal{X} := (1,3)\times(-1,1)$, defines a CBF for (3.23) with the set of unsafe states as $\mathcal{D} := \{x \in \mathcal{X} | \frac{1}{1-(x_1-2)^2} + \frac{1}{1-x_2^2} < 4\}$. Note that for all $x \in \mathcal{D}$, $B(x) > 0$.

Indeed, by direct evaluation, we have that for all $x \in \mathcal{X}$

$$\frac{\partial B}{\partial x} g(x) = 0 \Rightarrow x_2 = 0.$$

Hence the manifold $\{x | L_gB = 0\}$ is given by $\{x | x_2 = 0\}$, in which case

$$\left.\frac{\partial B}{\partial x} f(x)\right|_{x_2=0} = 0,$$

hence (2.17b) holds.

Let us now construct a CLBF $W(x)$ according to the construction as in Proposition 3.4. It is easy to see that the CLF $V(x)$ satisfies $\frac{1}{2}\|x\|^2 \leqslant V(x) \leqslant \frac{3}{2}\|x\|^2$, $\forall x \in \mathbb{R}^2$, i.e., (3.8) holds with $c_1 = \frac{1}{2}$ and $c_2 = \frac{3}{2}$.

On the other hand, it can be checked that $c_3 = \max_{x\in\partial\mathcal{X}} \|x\|^2 = 10$, $c_4 = \min_{x\in\partial\mathcal{D}} \|x\|^2 = 1.4$ and $\varepsilon = e^{-4}$. Hence, by taking $\lambda = 1000$, the condition $\lambda > \frac{c_2c_3-c_1c_4}{\varepsilon}$ is satisfied. Also, as defined in Proposition 3.4, $\kappa = -c_1c_4 = -0.7$.

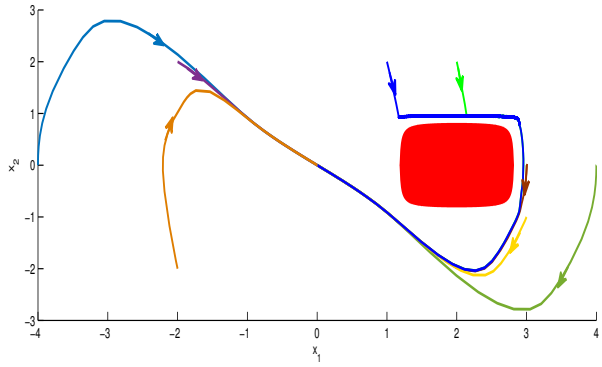

Figure 3.1: *The numerical simulation result of the closed-loop system using our proposed uniting CLBF method. The set of unsafe state $\mathcal{D}$ is shown in red and the plot of closed-loop trajectories are based on eight different initial conditions.*

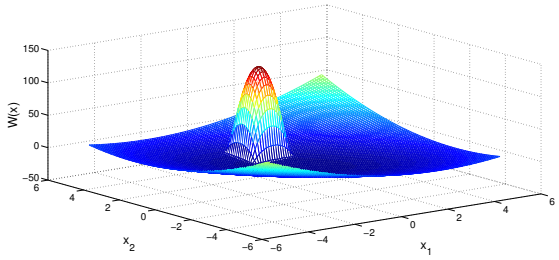

Figure 3.2: *The plot of the resulting Control Lyapunov-Barrier Function $W(x)$ as considered in the numerical simulation for Example 3.5.1.*

Using this constant λ and κ, the CLBF $W(x)$ is given by

$$W(x) = V(x) + \lambda B(x) + \kappa,$$

and the control law for solving the problem of stabilization with guaranteed safety is given by (3.5).

Figure 3.1 shows the numerical simulation of the closed-loop system with the gain $\gamma = 2$. In this plot, eight trajectories are shown with eight different initial states (4 0), (2 2), (-4 0), (-2 2), (-2 -2), (3 0), (3 -1), and (1 2). It can be seen from this figure that all trajectories converges to zero and avoid the unsafe state $\mathcal{D}$.

Figure 3.2 shows the resulting CLBF $W(x)$ where it is shown that for all $x \in \mathcal{D}$, $W(x) > 0$.

3.5.2 Mobile robot

In this example, we consider a simple mobile robot navigation that can be described by the following equations

$$\begin{aligned}\dot{x}_1 &= u_1\\ \dot{x}_2 &= u_2\end{aligned} \tag{3.25}$$

where x_1, x_2 are the positions in a 2D plane, and u_1, u_2 are their velocities, respectively.

This system admits a CLF $V(x) = x_1^2 + x_1x_2 + x_2^2$. We can choose $c_1 = 0.5$ and $c_1 = 2$ such that (3.8) is satisfied. Assume that we have two disjoint sets of unsafe states $\mathcal{D}_1 := \{x \in \mathcal{X}_1 | (x_1 - 3)^2 + x_2^2 < 4\}$ and $\mathcal{D}_2 := \{x \in \mathcal{X}_2 | x_1^2 + (x_2 - 5)^2 < 1\}$. It is easy to verify that the smallest distance between the sets $\mathcal{D}_1$ and $\mathcal{D}_2$, is 2.83, thus according to (3.16), we can enlarge each unsafe sets $\mathcal{D}_1$ and $\mathcal{D}_2$ with the open ball with radius $\mu < 0.7$. According to definition of $\mathcal{D}_1$ and $\mathcal{D}_1$, and by letting $\mathcal{X}_1 = \mathcal{D}_1 + \mathbb{B}_\mu$, $\mathcal{X}_2 = \mathcal{D}_2 + \mathbb{B}_\mu$ with $\mu = 0.3$, we have $c_{31} = 31.36$, $c_{41} = 1$, $c_{32} = 43.56$, $c_{42} = 16$.

We can choose two CBFs $B_1(x) = -((x_1 - 3)^2 + x_2^2) + 8$ and $B_2(x) = -(x_1^2 + (x_2 - 5)^2) + 4$ for $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. It can be checked that $-B_1$ and $-B_2$ are locally-strictly-concave functions. Now, for constructing $\widetilde{B}_1(x)$ and $\widetilde{B}_2(x)$ as in Proposition 3.5, we can choose a $\mathcal{C}^1$ function ρ_i that satisfies

$$\rho_i(z) = \begin{cases} 1 & \forall z \geqslant 0\\ 0 & \forall z \leqslant -\delta_i\\ \frac{1}{2}(\cos(\frac{\pi}{\delta_i}z) + 1) & \forall z \in (-\delta_i, 0)\end{cases}$$

We choose the following parameters $\delta_1 = 1.24$, $\delta_2 = 1.44$ and $\lambda_1 = \lambda_2 = 100$ that satisfy $\lambda_i > \frac{c_2c_{3i} - c_1c_{4i}}{\varepsilon_i}$, with $\varepsilon_i \leqslant \delta_i$, and the feedback gain $\gamma = 3$. Thus by using the control law as in (3.5) with $W(x) = V(x) + \lambda_1\widetilde{B}_1(x) + \lambda_2\widetilde{B}_2(x) + \kappa$, with κ being arbitrarily chosen as in Proposition 3.7.

Figure 3.3 shows the simulation results of the closed-loop system where it can be seen from this figure that all state trajectories with different initial conditions avoid the unsafe sets $\mathcal{D}_1$ and $\mathcal{D}_2$, and all trajectories converge to zero, i.e., the closed loop system is safe and stable.

3.6 Conclusions and discussions

In this chapter, we have proposed a novel control design method for achieving stability with guaranteed safety by merging a Control Lyapunov Function and (multiple) Control Barrier Function(s). Simulation results show the effectiveness

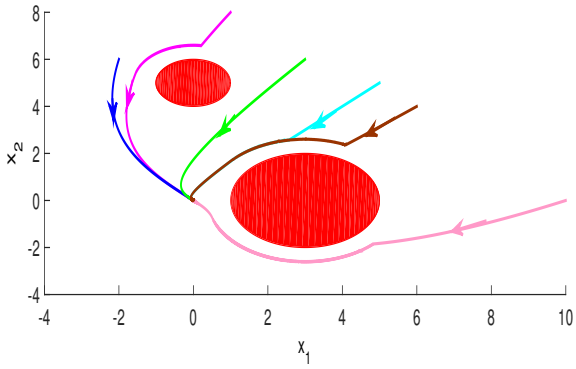

Figure 3.3: *The numerical simulation result of the closed-loop system using our proposed uniting CLF and CBFs method for the mobile robot example in subsection 3.5.2. The set of unsafe state $\mathcal{D}_1$ and $\mathcal{D}_2$ is shown in red and the plot of closed-loop trajectories are based on six different initial conditions (1 8), (-2 6), (5 5), (3 6), (10 0), and (6 4).*

of the control law based on the resulting Control Lyapunov-Barrier Function for solving the stabilization with guaranteed safety. Our proposed approach can simultaneously stabilize the closed-loop systems and guarantee its safety.

Chapter 4

On the new notion of input-to-state safety

Chapter 4
On the new notion of input-to-state safety

In this chapter, we propose a new notion of input-to-state safety (ISSf) which is an adaptation of input-to-state stability (ISS) inequality to the systems' safety case.

We introduce formally the notion of input-to-state safety and the characterization using ISSf barrier function in Section 4.1. In Section 4.3, we present sufficient conditions for a nonlinear system to be input-to-state safe. The sufficient conditions are based on an adaptation of ISS Lyapunov conditions to the barrier certificate. In Section 4.4, we restrict ourselves to the exponential case. In Section 4.5, we combine both concepts of ISS and ISSf in order to provide a robustness analysis tool for stability with guaranteed safety. We also discuss the special case of exponential rate and provide a numerical example of the aforementioned results for a simple mobile robot navigation system in Section 4.6. The works in the chapter is based on our preliminary work in [50] and our works in [51, 54].

4.1 Introduction

With the advent of complex cyber-physical systems (CPS) and industrial internet-of-things, the safety of the integrated cyber-physical systems has become an important design feature that must be incorporated in all software levels [7]. In particular, this feature must also be present in the low-level control systems where both aspects of safety and stability are integrated in the control design.

Despite the appealing idea in the works for guaranteeing stability and safety, it remains unclear on how to analyze the robustness of the closed-loop system in the presence of external (disturbance) input signals. There are many tools available for analyzing the robustness of systems' stability, including, H_∞ and L_2-stability theories [24, 55], absolute stability theory [26], input-to-state stability (ISS) theory [57] and many others. However, analogous tools for systems' safety are still minimal in literature which makes it difficult to carry out robustness analysis to the aforementioned works that deal with the problem of stabilization with guaranteed safety.

The seminal work in [57, 58] on the characterization of input-to-state stability has been one of the most important tools in the stability analysis of nonlinear systems. It has allowed us to study stability of interconnected systems, to quantify

systems' robustness with respect to external disturbances and to provide means for constructing a robustly stabilizing control law. The use of ISS Lyapunov function is crucial in all of these applications. In the following decade, the concept of ISS has been used and/or generalized in various direction with a commonality on the robustness analysis of systems' stability. Safety and constraint aspects have not been considered in this framework. By considering the complement of the set of unsafe state, one might consider to apply recent generalization of ISS to the stability of invariant sets as in [4]. But it may not give us an insightful detail on the influence of external disturbance signals to the state of safety of the system. In this case, the resulting ISS inequality will only provide us information on the effect of external input to the systems' trajectory with respect to the complement set of unsafe state, but not on how far it is from being unsafe.

Instead of the usual ISS inequality where the state trajectory $x(t)$ of the system can be bounded from above by a term that depends on initial condition and decays to zero and another term that depends on the L^∞-norm of the external input signal $u(t)$, we look at the following inequality

$$\sigma(|x(t)|_{\mathcal{D}}) \geqslant \min\{\mu\left(|x(0)|_{\mathcal{D}}, t\right), \delta\} - \phi\left(\|u(t)\|\right) \tag{4.1}$$

where $\mathcal{D}$ is the set of unsafe state, $|x|_{\mathcal{D}}$ denotes the distance of x to $\mathcal{D}$, the function σ is a strictly increasing function, μ is a strictly increasing function in both arguments, $\delta > 0$ and ϕ as the gain function that is dependent on input u, akin to the ISS case. As will be discussed later in Section 3, the inequality (4.1) will be called input-to-state safety (ISSf) inequality.

Roughly speaking, this inequality can be interpreted as follows. When there is no external input signal u, then the state trajectory will never get closer to $\mathcal{D}$. On the other hand, if there is an external input signal then it may jeopardize the systems' safety when the input signal u is taken sufficiently large. The above interpretation serves very well with what we can expect in real systems where external disturbance input can potentially bring the system into the unsafe state.

Complementary to the work of Xu *et al.* in [64], we adapt the ISS framework a' la Sontag to the systems' safety case through the use of ISSf barrier function which implies (4.1).

4.2 Review on barrier certificate

Let consider again Theorem 2.3 in Chapter 2. Although the safety result as in Theorem 2.3 is formulated only for autonomous systems, an extension to the non-autonomous case has also been presented in [44]. For the case where an external input u is considered, e.g., the complete system as in (2.27), the safety condition

(2.15) becomes

$$\frac{\partial B(\xi)}{\partial \xi}\left(f(\xi)+g(\xi)v\right)\leqslant 0 \quad \forall(\xi,v)\in\mathcal{X}\times\mathcal{U} \tag{4.2}$$

where $\mathcal{U}\subset\mathbb{R}^m$ denotes the admissible set of input. However, the condition (4.2) is a very restrictive assumption since it must hold for all $u(t)\in\mathcal{U}$ including the case when the initial condition $x(0)$ is very close to the unsafe set $\mathcal{D}$. It means that when we start very close to the unsafe state, the system must always remain safe for whatever type of input signals u as long as it has values in $\mathcal{U}$. In this case, we can say that such system is very robust with respect to bounded external input signals. In practice, we should expect a certain degree of fragility in the system, in the sense that, if we start very close to the unsafe state, a small external input signal can already jeopardize the systems' safety; a feature that is not captured in (4.2).

Instead of considering the inequality (4.2), we will consider a more restrictive condition on B for our main results later, where the non-increasing assumption of B as in (2.15) is replaced by a strict inequality as follows

$$\frac{\partial B(\xi)}{\partial \xi}f(\xi)\leqslant -\alpha(|x|_{\mathcal{D}}) \tag{4.3}$$

where α is a $\mathcal{K}$ function, and $|x|_{\mathcal{D}}$ is the distance of a point x with respect to the unsafe state $\mathcal{D}$.

In [53, 61], the use of such barrier function B for control design that guarantees safety has been presented. It is shown in these works that the standard Lyapunov-based control design can directly be extended to solving the safety problem by replacing the Lyapunov function with the barrier one. Interested readers are referred to [53] for control design methods that solve the stabilization with guaranteed safety by merging the Control Lyapunov Function with the Control Barrier Function.

4.3 Sufficient condition of input-to-state safety

In this section, we will explore a new notion of input-to-state safety as a tool to analyze the robustness of systems' safety. In particular, we focus our study on extending existing results on barrier certificate to the input-to-state safety framework; akin to the role of Lyapunov stability theory in the input-to-state stability results.

Definition 3. *The system* (2.27) *is called* input-to-state safe *(ISSf) locally in $\mathcal{X}\subset\mathbb{R}^n$ and with respect to the set of unsafe state $\mathcal{D}\subset\mathcal{X}$ if for all $x_0\in\mathbb{R}^n\backslash\mathcal{D}$, there exist*

$\sigma, \phi \in \mathcal{K}$, $\mu \in \mathcal{KK}$ and $\delta > 0$ such that

$$\sigma(|x(t)|_{\mathcal{D}}) \geqslant \min\{\mu(|x_0|_{\mathcal{D}}, t), \delta\} - \phi\left(\|u(t)\|\right) \tag{4.4}$$

holds for almost all $t \in [0, \infty)$ and for all admissible[1] *(x_0, u), where the constant $\delta > 0$ can be dependent on boundary of $\mathcal{X}$.*

If a system is ISSf, we can infer from (4.1) that the system (2.27) may be brought to the unsafe state if the L^∞-norm of u is sufficiently large such that the RHS of (4.1) is negative. Hence one can quantify the robustness of the system's safety with respect to an external input signal using this notion. For instance, if the initial condition x_0 is in the neighborhood of the boundary of unsafe state $\mathcal{D}$ then (4.1) shows that a small external input signal u may steer the state trajectory to enter $\mathcal{D}$; even when the autonomous case is safe. Since the first element on the RHS of (4.1) is a $\mathcal{KK}$ function, it implies that the distance between $x(t)$ and $\mathcal{D}$ is lower-bounded by a strictly increasing function until $x(t)$ leaves $\mathcal{X}$. As this lower-bound of the distance is non-decreasing with time, (4.1) means that the system can eventually withstand larger input signal.

We can also take a different view to the ISSf inequality above. If u is considered to be a disturbance signal with known magnitude, e.g., $\|u\|_{L^\infty} \leqslant k$ with $k > 0$, then (4.1) provides us with information on the admissible x_0 such that the RHS of (4.1) remains positive so that the system under such external disturbance will remain safe.

Let us now investigate the ISS-Lyapunov like condition for input-to-state safety of system (2.27) in the following proposition.

Proposition 4.1. *Consider system* (2.27) *with a given unsafe set $\mathcal{D} \subset \mathcal{X} \subset \mathbb{R}^n$. Suppose that there exists an ISSf barrier function $B \in \mathcal{C}^1(\mathcal{R}^n, \mathbb{R})$ satisfying*

$$-\alpha_1(|\xi|_{\mathcal{D}}) \leqslant B(\xi) \leqslant -\alpha_2(|\xi|_{\mathcal{D}}) \;\; \forall \xi \in \mathbb{R}^n \backslash \mathcal{D} \tag{4.5}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -\alpha_3(|\xi|_{\mathcal{D}}) + \alpha_4(\|v\|) \qquad \forall \xi \in \mathcal{X} \backslash \mathcal{D}, \forall v \in \mathcal{U}, \tag{4.6}$$

where $\alpha_i \in \mathcal{K}_\infty$, i=1,..4. Assume further that the system is ISS.

Then the system is input-to-state safe locally in $\mathcal{X}$ and w.r.t. $\mathcal{D}$. In particular, for any $\theta, \epsilon \in (0, 1)$ and for all $x_0 \in \mathbb{R}^n \backslash \mathcal{D}$, the ISSf inequality (4.1) *holds for all $t \geqslant 0$*

[1] By admissible (x_0, u), we mean that the tuple is such that the RHS of (4.1) is strictly positive for almost all $t \geqslant 0$.

and for all admissible (x_0, u) *where* $\sigma(s) = s$, $\delta = \min\{\epsilon|\xi|_{\mathcal{D}} : \forall \xi \in \partial\mathcal{X}\}$,

$$\mu(s,t) = \epsilon\alpha_1^{-1}(\tilde{\alpha}(\alpha_2(s),t)) \qquad \forall s,t \geqslant 0$$

and

$$\phi(s) = \alpha_2^{-1} \circ \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(s)}{\theta} \qquad \forall s \geqslant 0$$

with $\tilde{\alpha} \in \mathcal{KK}$ *being the solution of the following initial value problem*

$$\dot{y} = (1-\theta)\alpha_3 \circ \alpha_1^{-1}(y), \quad y(0) = s \in \mathbb{R}_+,$$

so that $\tilde{\alpha}(s,t) := y(t)$ *for all* $s \geqslant 0$. □

The main idea of the proof is that we evaluate the evolution of the barrier function B along the trajectory of the state x for a given bounded input signal u. Following a similar derivation of ISS property from an ISS Lyapunov function, we can show that when the input is small then the distance is bounded from below by an increasing function of time and, on the other hand, when the input is large then the distance can be lower bounded by a positive function that depends on input. Finally, we can patch the two lower-bound functions together.

Prior to proving this proposition, a few remarks can be made on the relation between the ISSf barrier function satisfying (4.5)-(4.6) and the barrier certificate satisfying (2.13)-(2.15). First, it is easy to see that the condition (4.5) implies (2.14) where $\mathcal{X}_0$ in (2.14) is $\mathbb{R}^n \backslash \bar{\mathcal{D}}$. Second, when we consider the autonomous case (i.e., $u = 0$), then (4.6) implies the strict version of (2.15) (c.f., (4.3)).

Proof : Let us first evaluate the solution $x(t)$ of (2.27) with $x_0 \in \mathcal{X}\backslash\mathcal{D}$. From (4.5) it follows that $|x(t)|_{\mathcal{D}} \geqslant \alpha_1^{-1}(-B(x(t)))$, thus evaluating the time derivative of $B(x(t))$ gives us

$$\begin{aligned}\dot{B}(x(t)) &\leqslant -\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) + \alpha_4(\|u(t)\|) \\ &= -(1-\theta)\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) \\ &\quad - \theta\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) + \alpha_4(\|u(t)\|), \end{aligned} \tag{4.7}$$

with $\theta \in (0,1)$ which holds whenever $x(t) \in \mathcal{X}\backslash\mathcal{D}$.

Thus for almost all t such that $\|u(t)\| \leqslant \alpha_4^{-1} \circ \theta\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) =: \rho(x(t))$, inequality (4.7) implies that

$$\dot{B}(x(t)) \leqslant -(1-\theta)\alpha_3 \circ \alpha_1^{-1}(-B(x(t)))$$

holds whenever $x(t) \in \mathcal{X}\backslash\mathcal{D}$. By letting $\tilde{B}(x(t)) = -B(x(t))$, the last inequality becomes

$$\dot{\tilde{B}}(x(t)) \geqslant (1-\theta)\alpha_3 \circ \alpha_1^{-1}(\tilde{B}(x(t))). \tag{4.8}$$

Note that function $(1-\theta)\alpha_3 \circ \alpha_1^{-1}(r)$ belongs to $\mathcal{K}$ function and the function $\tilde{B}$ is positive definite. Hence, the RHS of (4.8) is always positive. Now by the comparison lemma,

$$\tilde{B}(x(t)) \geqslant \tilde{\alpha}(\tilde{B}(x_0), t) \tag{4.9}$$

where $\tilde{\alpha} \in \mathcal{KK}$ is the solution $y(t)$ of

$$\dot{y} = (1-\theta)\alpha_3 \circ \alpha_1^{-1}(y), \quad y(0) = s \in \mathbb{R}_+,$$

i.e., $\tilde{\alpha}(s,t) := y(t)$ for any positive initial condition s.

By subtituting (4.9) into the lower bound and upper bound of $B(x)$ in (4.5) it follows that

$$\begin{aligned} &\alpha_1(|x(t)|_{\mathcal{D}}) \geqslant \tilde{\alpha}(\tilde{B}(x_0), t) \geqslant \tilde{\alpha}(\alpha_2(|x_0|_{\mathcal{D}}), t) \\ &\implies |x(t)|_{\mathcal{D}} \geqslant \alpha_1^{-1}\tilde{\alpha}(\alpha_2(|x_0|_{\mathcal{D}}), t) =: \widetilde{\mu}(|x_0|_{\mathcal{D}}, t) \end{aligned} \tag{4.10}$$

which holds for almost all t s.t. $\|u(t)\| \leqslant \rho(x(t))$ and whenever $x(t) \in \mathcal{X}\backslash\mathcal{D}$.

Now, let us consider the other case where $\|u(t)\| > \rho(x(t))$. In this case, it follows immediately that

$$\begin{aligned} &-B(x(t)) \leqslant \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta} \\ &\implies \alpha_2(|x(t)|_{\mathcal{D}}) \leqslant \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta} \\ &\implies |x(t)|_{\mathcal{D}} \leqslant \alpha_2^{-1} \circ \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta} =: \widetilde{\phi}(\|u(t)\|) \end{aligned} \tag{4.11}$$

We will now combine these two cases as follows. Firstly, from (4.10), it follows that

$$-\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) + |x(t)|_{\mathcal{D}} \geqslant (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) - \eta\widetilde{\phi}(\|u(t)\|), \tag{4.12}$$

where $\epsilon, \eta \in (0,1)$. This inequality is obtained by adding both sides of (4.10) by $-\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)$ and substracting the right-hand side of (4.10) by $-\eta\widetilde{\phi}(\|u(t)\|)$ which is non-positive for all $u(t)$. On the other hand, by multiplying both sides of (4.11) by $-\eta$ and then by adding both sides by $(1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)$, we get

$$(1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) - \eta|x(t)|_{\mathcal{D}} \geqslant (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) - \eta\widetilde{\phi}(\|u(t)\|). \tag{4.13}$$

Thus, (4.12) (which holds for $\|u(t)\| \leqslant \rho(x(t))$) and (4.13) (which is true for

$\|u(t)\| > \rho(x(t))$) imply that

$$\begin{aligned}&\max\{-\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}},t)+|x(t)|_{\mathcal{D}},\ (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}},t)-\eta|x(t)|_{\mathcal{D}}\} \\ &\geqslant (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}},t)-\eta\widetilde{\phi}(\|u(t)\|)\end{aligned} \tag{4.14}$$

holds for all $t \geqslant 0$ s.t. $x(t) \in \mathcal{X}\backslash\mathcal{D}$.

Since the state trajectory starts from the safe region, then for a given initial condition x_0 and bounded input u, there exists sufficiently small η, ϵ and $T_1 > 0$ such that the right hand side of (4.14) and each term on the left-hand side are positive for all $t \in [0, T_1)$. Thus, since $\max\{a, b\} \leqslant a + b$ for $a, b \geqslant 0$, (4.14) implies that

$$\begin{aligned}&(1-2\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}},t)+(1-\eta)|x(t)|_{\mathcal{D}} \\ &\quad\geqslant (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}},t)-\eta\widetilde{\phi}(\|u(t)\|) \\ \Leftrightarrow&(1-\eta)|x(t)|_{\mathcal{D}} \geqslant \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}},t)-\eta\widetilde{\phi}(\|u(t)\|) \\ \Leftrightarrow&|x(t)|_{\mathcal{D}} \geqslant \frac{\epsilon}{1-\eta}\widetilde{\mu}(|x_0|_{\mathcal{D}},t)-\frac{\eta}{1-\eta}\widetilde{\phi}(\|u(t)\|)\end{aligned} \tag{4.15}$$

holds for almost all $t \in [0, T_1)$.

We will prove now that we can extend the time interval, where (4.15) is valid, to $[0, T_{1,\max})$ with finite $T_{1,\max} < \infty$ if x leaves the set $\mathcal{X}$ at time $T_{1,\max}$, or $T_{1,\max} = \infty$ when x stays in $\mathcal{X}\backslash\mathcal{D}$ at all time. In particular, we show that we can choose η and ϵ such that both terms on the LHS of (4.14) are positive for almost all $t \in [0, T_{1,\max})$, so that (4.15) holds accordingly.

Firstly, let us show that for any $\epsilon \in (0, 1)$, there exists $\eta \in (0, 1)$ such that

$$|x(t)|_{\mathcal{D}} \leqslant \frac{1-\epsilon}{\eta}\widetilde{\mu}(|x_0|_{\mathcal{D}},t) \qquad \forall t \in [0,\infty). \tag{4.16}$$

Since the system is ISS, there exists $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}_\infty$ such that

$$\begin{aligned}|x(t)| &\leqslant \beta(|x_0|,t)+\gamma(\|u\|_{L^\infty}) \\ &\leqslant \beta(|x_0|,0)+\gamma(\|u\|_{L^\infty}) =: D_1.\end{aligned}$$

By triangular inequality and by denoting $D_2 = \max\{|\xi| \ : \ \forall \xi \in \mathcal{D}\}$, it follows that

$$\begin{aligned}|x(t)|_{\mathcal{D}} &\leqslant D_2 + |x(t)| \leqslant D_1 + D_2 \\ &\leqslant \frac{D_1+D_2}{\widetilde{\mu}(|x_0|_{\mathcal{D}},0)}\widetilde{\mu}(|x_0|_{\mathcal{D}},t),\end{aligned} \tag{4.17}$$

where the last inequality is due to the fact that $\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) \geqslant \widetilde{\mu}(|x_0|_{\mathcal{D}}, 0)$ for all

$t \geqslant 0$. Thus, by taking

$$\eta = \min\left\{0.5, \frac{(1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, 0)}{D_1 + D_2}\right\} \in (0, 0.5], \tag{4.18}$$

the inequality (4.17) implies that (4.16) holds for all $t \geqslant 0$. Hence, the second term on the LHS of (4.14) is always positive for all t.

It remains now to check whether

$$|x(t)|_{\mathcal{D}} > \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)$$

for all $t \in [0, T_{1,\max})$. We will show this by contradiction. Suppose that there is a finite $\tau < T_{1,\max}$ that defines the time when $|x(\tau)|_{\mathcal{D}} = \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, \tau)$. In this case, (4.15) still holds and we have that

$$\begin{aligned}
|x(\tau)|_{\mathcal{D}} &\geqslant \frac{\epsilon}{1-\eta}\widetilde{\mu}(|x_0|_{\mathcal{D}}, \tau) - \frac{\eta}{1-\eta}\widetilde{\phi}(\|u(\tau)\|) \\
&= \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, \tau) \\
&\quad + \frac{\eta}{1-\eta}\left(\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, \tau) - \widetilde{\phi}(\|u(\tau)\|)\right).
\end{aligned}$$

Since $\widetilde{\phi}(\|u(t)\|) < \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)$ for all $t \geqslant 0$ (by hypothesis of the proposition on the admissibility of (x_0, u) with $\mu = \epsilon\widetilde{\mu}$ and $\widetilde{\phi} = \phi$), it follows from the above inequality that

$$|x(\tau)|_{\mathcal{D}} > \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, \tau)$$

which is a contradiction. Thus, we have that (4.15) holds for almost all $t \in [0, T_{1,\max})$.

Finally, we will derive the conservative lower bound of (4.15) such that it will no longer depend on η (which is currently dependent on x_0 and u as in (4.18)). By the definition of η in (4.18), it is trivial to check that $0 < \eta < 0.5$,

$$1 < \frac{1}{1-\eta} < 2 \;\text{ and }\; 0 > \frac{-\eta}{1-\eta} > -1.$$

Thus, (4.15) implies that

$$|x(t)|_{\mathcal{D}} \geqslant \epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) - \widetilde{\phi}(\|u(t)\|) \tag{4.19}$$

for almost all $t \in [0, T_{1,\max})$.

On the other hand, by defining $\kappa := \min\{|\xi|_{\mathcal{D}} : \forall \xi \in \partial\mathcal{X}\} > 0$, we have that when $x(t) \notin \mathcal{X}$ (including for the second case when $x_0 \notin \mathcal{X}$),

$$|x(t)|_{\mathcal{D}} \geqslant \kappa \geqslant \kappa - \widetilde{\phi}(\|u(t)\|). \tag{4.20}$$

Once x leaves $\mathcal{X}$ and enters again $\mathcal{X}$ at a later time interval, then we can use again the argument as before where the initial condition is taken in the neighborhood of the boundary of $\mathcal{X}$. Indeed, suppose that x enters again $\mathcal{X}$ at time $T_2 > T_{1,\max}$. Then by following the same argument as before, we get

$$\begin{aligned} |x(t)|_{\mathcal{D}} &\geqslant \epsilon\widetilde{\mu}(|x(T_2)|_{\mathcal{D}}, t - T_2) - \widetilde{\phi}(\|u(t)\|) \\ &\geqslant \epsilon\widetilde{\mu}(\kappa, 0) - \widetilde{\phi}(\|u(t)\|), \end{aligned} \tag{4.21}$$

for almost all $t \in [T_2, T_{2,\max})$ where $T_{2,\max}$ is the maximum time where x remains in $\mathcal{X}$.

Since in all of these cases, $|x(t)|_{\mathcal{D}}$ satisfies either (4.19), (4.20) or (4.21) in different time intervals, we can combine them by taking the minimum of their lower bounds. Thus by defining $\delta := \epsilon\widetilde{\mu}(\kappa, 0)$ with κ as defined before (4.20),

$$\begin{aligned} |x(t)|_{\mathcal{D}} &\geqslant \min\{\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)\,,\, \kappa\,,\, \epsilon\widetilde{\mu}(\kappa, 0)\} - \widetilde{\phi}(\|u(t)\|) \\ &= \min\{\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)\,, \delta\} - \widetilde{\phi}(\|u(t)\|) \end{aligned}$$

holds for almost all $t \in [0, \infty)$.

Hence, we have ISSf with $\mu = \epsilon\widetilde{\mu}$ and $\phi = \widetilde{\phi}$ where $\widetilde{\mu}$ and $\widetilde{\phi}$ are as in (4.10) and (4.11), respectively, and δ as defined above. Note that the choice of $\epsilon \in (0, 1)$ is, in this case, independent of admissible tuple (x_0, u).

□

The ISS assumption in this proposition can be relaxed by weaker conditions that can guarantee the boundedness of $|x(t)|_{\mathcal{D}}$. For instance, we can assume that the system is integral input-to-state stable or it is practically input-to-state stable.

One can see from Proposition 4.1 that the inequalities in (4.5) and (4.6) are reminiscent of those inequalities used in the study of ISS Lyapunov function. In this context, the inequality (4.6) resembles the dissipation inequality in the ISS Lyapunov function and the growth of B as in (4.5) can be likened to the growth of V as in (2.29), albeit they grow with different sign as well as with different metric norm.

We can now combine the notion of input-to-state stability and that of input-to-state safety which allows us to study the robustness of a stable and safe system with respect to an external input signal u.

Definition 4. *System* (2.27) *is called ISS with guaranteed safety (ISS-GS) with respect to $\mathcal{D}$ if there exists $\mathcal{X} \subset \mathbb{R}^n$ such that the system* (2.27) *is both input-to-state stable and input-to-state safe locally in $\mathcal{X}$ and w.r.t. $\mathcal{D} \subset \mathcal{X}$.*

It is trivial to show that if there exist both an ISS Lyapunov function V satisfying

(2.29)–(2.30) and an ISSf barrier function B satisfying (4.5)–(4.6) locally on $\mathcal{X} \subset \mathbb{R}^n$ with $\mathcal{D} \subset \mathcal{X}$ then the system is input-to-state stable with guaranteed safety. Instead of considering two separate functions V and B as suggested before, we can also consider combining the ISS Lyapunov inequality (2.30) and ISSf barrier inequality (4.6) as shown in the following corollary.

Corollary 4.2. *Suppose that there exists $W : \mathbb{R}^n \to \mathbb{R}$ and $\mathcal{D} \subset \mathcal{X} \subset \mathbb{R}^n$ such that*

$$\alpha_1(\|\xi\|) \leqslant W(\xi) \leqslant \alpha_2(\|\xi\|) \quad \forall \xi \in \mathbb{R}^n \tag{4.22}$$

$$-\alpha_3(|\xi|_{\mathcal{D}}) \leqslant W(\xi) - c \leqslant -\alpha_4(|\xi|_{\mathcal{D}}) \quad \forall \xi \in \mathcal{X}\backslash\mathcal{D} \tag{4.23}$$

$$\frac{\partial W(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -\alpha_5(\|\xi\|) - \Xi_{\mathcal{X}}(\xi)\alpha_6(|\xi|_{\mathcal{D}}) + \alpha_7(\|v\|) \tag{4.24}$$

where $\Xi_{\mathcal{X}}$ is an indicator function for $\mathcal{X}$, $c > 0$, the functions $\alpha_i \in \mathcal{K}_\infty$ for $i = 1, ..7$. Then it is ISS with guaranteed safety with respect to $\mathcal{D}$.

Proof : It is trivial to check that $W(x)$ qualifies as an ISS Lyapunov function satisfying (2.29)–(2.30) and as an ISSf barrier function satisfying (4.5)–(4.6) locally in $\mathcal{X}$. The ISS property follows trivially from (4.22) and (4.24) and Theorem 2.8.

Let $B(\xi) = W(\xi) - c$ for all $\xi \in \mathcal{X}\backslash\mathcal{D}$. Subsequently, let the function B be extended smoothly to $\xi \in \mathbb{R}^n\backslash\mathcal{X}$ so that (4.5) holds for all $\mathbb{R}^n\backslash\mathcal{D}$. It follows from (4.24) that

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -\alpha_6(|\xi|_{\mathcal{D}}) + \alpha_7(\|v\|)$$

holds for all $\xi \in \mathcal{X}\backslash\mathcal{D}$ and for all $v \in \mathcal{U}$. By Proposition 4.1, it implies that it is ISSf. □

4.4 The case of exponential rate input-to-state safety

In this section, we will explore exponential rate input-to-state safety as a tool to analyze the robustness of systems' safety. We can boil down definition of ISSf as before in this special case. Instead of using definition (4.1), we use the following definition for the case of exponential rate.

Definition 5. *The system* (2.27) *is called* practically exponentially input-to-state safe *(pISSf) with respect to the set of unsafe state $\mathcal{D}$ if it satisfies*

$$|x(t)|^p_{\mathcal{D}} \geqslant k_1 e^{\lambda_1 t}|x_0|^p_{\mathcal{D}} - k_2 e^{\lambda_2 t}\|u\|^q_{L^\infty} - k_3 e^{\lambda_3 t} \tag{4.25}$$

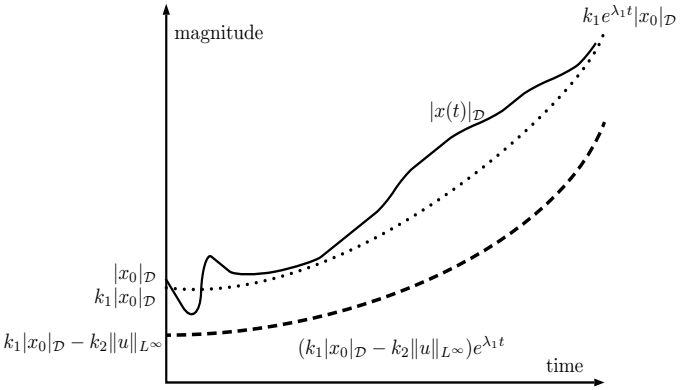

Figure 4.1: *An illustration of the ISSf-inequality* (4.25) *for the exponential rate case as presented in Proposition* (4.3) *with* $\kappa = 0$. *The dotted-line describes the lower-bound of distance to unsafe set that is due to the initial conditions (e.g., the first term on RHS of* (4.25)*) while the dashed-line shows the influence of the bounded external input in decreasing this lower-bound. The solid-line shows a possible time evolution of the distance to the unsafe set following* (4.25). *If the dashed-line crosses the zero line then the system may enter the unsafe set.*

for all t, *where* $k_1, k_2, k_3, \lambda_1, \lambda_2, \lambda_3 > 0$. *Furthermore, if* $k_3 = 0$ *then it is called input-to-state safe (ISSf). In order to guarantee that the RHS is positive, it is implicitly assumed that* $\lambda_1 \geqslant \max\{\lambda_2, \lambda_3\}$.

Figure 4.1 shows an illustration of the ISSf-inequality with an exponential rate as in (4.25) and $k_3 = 0$, i.e., the case of input-to-state safe. In this figure, the evolution of state distance to the unsafe set is always lower-bounded by $k_1 e^{\lambda_1 t}|x_0|_{\mathcal{D}} - k_2 e^{\lambda_2 t}\|u\|_{L^\infty}$, with $\lambda_1 = \lambda_2$. When the lower bound crosses the zero line (for instance, if the input is sufficiently large or the initial distance to the unsafe set is very small) then safety of the system is no longer guaranteed for such input and initial state setting.

In the following proposition, we show a barrier function characterization that gives rise to the input-to-state safety inequality (4.25).

Proposition 4.3. *Consider the nonlinear system in* (2.27) *that is forward complete and let the set of unsafe state be given by a compact set* $\mathcal{D} \subset \mathbb{R}^n$. *Suppose that there exists an ISSf barrier function* $B : \mathbb{R}^n \to \mathbb{R}$ *satisfying*

$$-c_1|\xi|^p_{\mathcal{D}} - \kappa \leqslant B(\xi) \leqslant -c_2|\xi|^p_{\mathcal{D}} \tag{4.26}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -c_3|\xi|^p_{\mathcal{D}} + c_4\|v\|^q \tag{4.27}$$

where $c_i > 0$, $i = 1, 2, 3, 4$ and $\kappa \geqslant 0$. Then the system is practically exponentially input-to-state safe w.r.t. $\mathcal{D}$ where $\alpha(s,t) = \frac{c_2}{c_1} e^{\frac{c_3}{c_1}t} s^p$, $\phi(s,t) = \frac{c_4}{c_3} e^{\frac{c_3}{c_1}t} s^q$ and $\gamma(t) = \frac{\kappa}{c_1} e^{\frac{c_3}{c_1}t}$.

Proof : Let $x(t)$ be the solution of (2.27). Evaluating the time derivative of $B(x(t))$ along the trajectory of x, it follows from (4.26) and (4.27) that

$$\dot{B}(x) \leqslant \frac{c_3}{c_1} B(x) + \frac{\kappa c_3}{c_1} + c_4 \|u\|^q.$$

By the standard application of comparison lemma, the above differential inequality implies immediately that

$$B(x(t)) \leqslant e^{\frac{c_3}{c_1}t} B(x(0)) + \int_0^t e^{\frac{c_3}{c_1}(t-\tau)} \left(\frac{\kappa c_3}{c_1} + c_4 \|u(\tau)\|^q \right) \mathrm{d}\tau.$$

Following a routine computation on the RHS of this inequality, we get

$$\begin{aligned} B(x(t)) &\leqslant e^{\frac{c_3}{c_1}t} B(x(0)) \\ &\quad + \left(\frac{\kappa c_3}{c_1} + c_4 \|u\|_{L^\infty}^q \right) \int_0^t e^{\frac{c_3}{c_1}(t-\tau)} \mathrm{d}\tau \\ &= e^{\frac{c_3}{c_1}t} B(x(0)) + \left(\kappa + \frac{c_4 c_1}{c_3} \|u\|_{L^\infty}^q \right) \left(e^{\frac{c_3}{c_1}t} - 1 \right) \end{aligned}$$

By using the lower bound of $B(x(t))$ in (4.26) into the above inequality, it is easy to see that

$$\begin{aligned} -c_1 |x(t)|_{\mathcal{D}}^p - \kappa &\leqslant e^{\frac{c_3}{c_1}t} B(x(0)) \\ &\quad + \left(\kappa + \frac{c_4 c_1}{c_3} \|u\|_{L^\infty}^q \right) \left(e^{\frac{c_3}{c_1}t} - 1 \right) \\ \Rightarrow -c_1 |x(t)|_{\mathcal{D}}^p &\leqslant -c_2 e^{\frac{c_3}{c_1}t} |x(0)|_{\mathcal{D}}^p \\ &\quad + \frac{c_4 c_1}{c_3} \|u\|_{L^\infty}^q \left(e^{\frac{c_3}{c_1}t} - 1 \right) + \kappa e^{\frac{c_3}{c_1}t} \\ \Rightarrow |x(t)|_{\mathcal{D}}^p &\geqslant \frac{c_2}{c_1} e^{\frac{c_3}{c_1}t} |x(0)|_{\mathcal{D}}^p - \frac{c_4}{c_3} \|u\|_{L^\infty}^q (e^{\frac{c_3}{c_1}t} - 1) \\ &\quad - \frac{\kappa}{c_1} e^{\frac{c_3}{c_1}t} \\ &\geqslant \frac{c_2}{c_1} e^{\frac{c_3}{c_1}t} |x(0)|_{\mathcal{D}}^p - \frac{c_4}{c_3} \|u\|_{L^\infty}^q e^{\frac{c_3}{c_1}t} - \frac{\kappa}{c_1} e^{\frac{c_3}{c_1}t}. \end{aligned}$$

□

As shown in Proposition 4.3, a practical exponential input-to-state safety can be

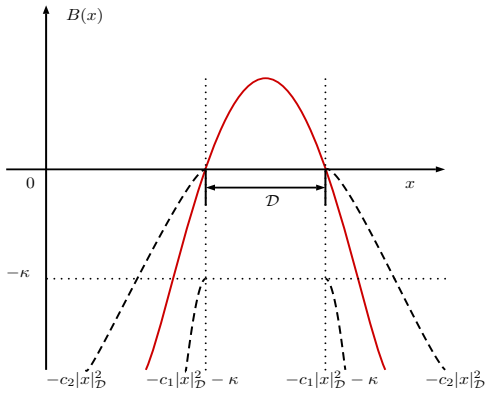

Figure 4.2: *An illustration of a practical ISSf barrier function which takes the form of a quadratic function, e.g.,* $B(x) = -(x - x^*)^T P(x - x^*) + c$ *where* P *is a positive definite matrix,* x^* *is the centroid of the unsafe set* $\mathcal{D}$ *and* c *is a constant that is chosen such that the zero level of* B *is equal to the boundary of* $\mathcal{D}$*. The solid red-line is the plot of* B *and the dashed-line shows the possible lower and upper bound of* B *using the set distance function* $|x|_{\mathcal{D}}$ *and a bias constant* $\kappa > 0$ *as used in Proposition* (4.3)*, c.f.,* (4.26)*.*

shown if there exists B such that the inequalities (4.26) and (4.27) hold. When $\kappa = 0$ then (4.26) & (4.27) $\Rightarrow$ the system (2.27) is input-to-state safe. In the following, we define the function B satisfying (4.26) and (4.27) as pISSf barrier function. Moreover, if $\kappa = 0$ then it is called ISSf barrier function.

The constant κ is introduced in (4.26) to accomodate a polynomial function B of x as typically considered in the construction of a barrier certificate via sum-of-squares programming (for the safety analysis of an autonomous system). The gradient of such function B on the boundary of $\mathcal{D}$ may be non-zero. For example, in Figure 4.2, the red-line depicts a quadratic function B that has values larger than zero in the unsafe set $\mathcal{D}$ and is less than zero otherwise. Since the gradient of B on $\partial\mathcal{D}$ is non-zero, it cannot be lower bounded only by using $-c_1|x|_{\mathcal{D}}$ whose gradient on $\partial\mathcal{D}$ is equal to zero. In this case, by taking an arbitrary small $\kappa > 0$, we can find a sufficiently large $c_1 > 0$ such that the lower bound in (4.26) holds. Note that an arbitrary large c_1 will give us a conservative estimate in the growth of the bound in the ISSf inequality.

An example of an ISSf barrier function that satisfies (4.26) with $\kappa = 0$ is shown in Figure (4.3). In this figure, the ISSf barrier function is constructed directly using the set distance function $|x|_{\mathcal{D}}$.

One can observe that in the standard barrier certificate result as given in Theorem 2.3, the condition (2.15) is imposed so that the barrier certificate B is non-increasing along the trajectory of $x(t)$ which is similar to the Lyapunov stability analysis. However, we cannot use such B as an ISSf barrier function for

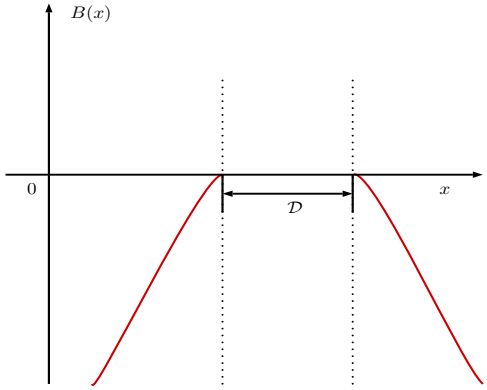

Figure 4.3: *The plot of an ISSf barrier function* $B(x) = -c|x|^2_{\mathcal{D}}$ *with* $c > 0$.

the non-autonomous system (2.27). If we consider a barrier certificate B which satisfies (4.3) instead, then we may be able to use it as a candidate for an ISSf barrier function.

Corollary 4.4. *Consider a forward complete system* (2.27) *with bounded* g *and let the set of unsafe state be given by a compact set* $\mathcal{D} \subset \mathbb{R}^n$. *Suppose that there exists a barrier certificate* $B : \mathbb{R}^n \to \mathbb{R}$ *such that*

$$-c_1|\xi|^p_{\mathcal{D}} - \kappa \leqslant B(\xi) \leqslant -c_2|\xi|^p_{\mathcal{D}} \tag{4.28}$$

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leqslant -c_3|\xi|^p_{\mathcal{D}} \tag{4.29}$$

$$\left\| \frac{\partial B(\xi)}{\partial \xi} \right\| \leqslant c_4 \|\xi\|^q \tag{4.30}$$

where $c_i > 0$, $i = 1, 2, 3, 4$ *and* $\kappa \geqslant 0$. *Then the system is practically input-to-state safe w.r.t.* $\mathcal{D}$ *with an exponential rate.*

The proof of this corollary is straightforward and is therefore omitted.

Similar to this corollary, one can also easily show that if the system admits a Control Barrier Function B with the strict version of the Artstein's like condition, e.g.,

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leqslant -c|\xi|^p_{\mathcal{D}} \qquad \forall \xi \text{ s.t. } \frac{\partial B(\xi)}{\partial \xi} g(\xi) = 0,$$

then we may use B to design a control law (for instance, via the Sontag's universal control law) such that the closed-loop system is pISSf or ISSf which depends on (4.26).

4.5 Exponential rate input-to-state stability with guaranteed safety

Equipped with the result on input-to-state safety from the previous section, we can now combine the notion of input-to-state stability and that of input-to-state safety that allows us to study the robustness of a stable and safe system with respect to external input u.

Definition 6. *System* (2.27) *is called ISS with guaranteed safety (ISS-GS) with respect to $\mathcal{D}$ if it is both input-to-state stable and input-to-state safe with respect to $\mathcal{D}$.*

Since ISS is a global property, combining both notions of ISS and ISSf can be counteractive. For instance, consider again the exponential rate case for both ISS and ISSf. The ISS notion implies that the state trajectories will converge to a ball close to the origin where the ball size is determined by the input. Since the distance between the origin and $\mathcal{D}$ is finite, it follows then that the evolution of distance to $\mathcal{D}$ will also converge to a finite value which contradicts the ISSf inequality in (4.25). Thus, one needs to either impose ISSf only locally or to allow the $\mathcal{KK}$ functions α, ϕ and γ in (4.1) to have a bounded range or saturation.

It is trivial to show that if there exist both a quadratic ISS Lyapunov function V satisfying (2.29)–(2.30) and an ISSf barrier function B satisfying (4.26)–(4.27) locally on $\Xi \subset \mathbb{R}^n$ with $\kappa = 0$ and $\mathcal{D} \subset \Xi$ then the system is input-to-state stable with guaranteed safety. Instead of considering two separate functions V and B as suggested before, we can also consider combining the ISS Lyapunov inequality (2.30) and ISSf barrier inequality (4.27) as given in the following proposition.

Proposition 4.5. *Suppose that there exists $W : \mathbb{R}^n \to \mathbb{R}$ and $\mathcal{D} \subset \Xi \subset \mathbb{R}^n$ such that*

$$c_1\|\xi\|^p \leqslant W(\xi) \leqslant c_2\|\xi\|^p \quad \forall \xi \in \mathbb{R}^n \tag{4.31}$$

$$-c_3|\xi|_{\mathcal{D}}^p - \kappa \leqslant W(\xi) \leqslant -c_4|\xi|_{\mathcal{D}}^p \quad \forall \xi \in \Xi \tag{4.32}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leqslant -c_5\|\xi\|^p - c_6\chi_\Xi(\xi)|\xi|_{\mathcal{D}}^p + c_7\|v\|^q \tag{4.33}$$

where χ_Ξ is an indicator function for Ξ, the constants $c_i > 0, \quad i = 1, 2, ..$ and $\kappa > 0$. Then it is ISS with guaranteed safety with respect to $\mathcal{D}$.

Proof : It is trivial to check that $W(x)$ qualifies as an ISS Lyapunov function satisfying (2.29)–(2.30) and as an ISSf barrier function satisfying (4.26)–(4.27) locally in Ξ. Indeed, from (4.33), we have that

$$\dot{W}(x(t)) \leqslant -c_5\|x(t)\|^p + c_7\|u(t)\|^q.$$

Using a standard result from ISS and using (4.31), it follows immediately that

$$\|x(t)\|^p \leqslant \frac{c_2}{c_1} e^{-\frac{c_5}{c_1}t} \|x_0\|^p + \frac{c_7}{c_5} \|u\|^q_{L^\infty}$$

which shows the robustness of systems' stability. On the other hand, from (4.33), it follows that in Ξ

$$\dot{W}(x(t)) \leqslant -c_6 \|x(t)\|^p_{\mathcal{D}} + c_7 \|u(t)\|^q.$$

Hence, as shown before, together with (4.32) it implies that

$$|x(t)|^p_{\mathcal{D}} \geqslant \frac{c_4}{c_3} e^{\frac{c_6}{c_3}t} |x(0)|^p_{\mathcal{D}} - \frac{c_7}{c_6} \|u\|^q_{L^\infty} e^{\frac{c_6}{c_3}t} - \frac{\kappa}{c_3} e^{\frac{c_6}{c_3}t}$$

holds for all $x(t) \in \Xi$, i.e., it is safe. □

4.6 Simulation result on mobile robot navigation

In this section, we consider an example of a simple mobile robot navigation described by the following equations

$$\begin{aligned} \dot{x}_1 &= v_1 + u_1 \\ \dot{x}_2 &= v_2 + u_2 \end{aligned} \tag{4.34}$$

where $x = [x_1, x_2]^T$ is the position in a 2D plane, $v = [v_1, v_2]^T$ is its velocity which is used as a feedback control input, and $u = [u_1, u_2]^T \in L^\infty$ is external disturbance signal.

Example 4.1. (*Input-to-state safety*). Consider system (4.34) with a given unsafe set $\mathcal{D} := \{x \in \mathbb{R}^2 | (x_1 - 4)^2 + (x_2 - 6)^2 < 4\}$. We can construct an ISSf barrier function $B(x) = -(x_1 - 4)^2 - (x_2 - 6)^2 + 4$. Consider a gradient-based control law for (4.34) using $B(x)$, i.e., $\left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right] = -\nabla_x B(x) = -\frac{\partial^T B}{\partial x}$.

It can be checked that this ISSf barrier function B fulfills all hypotheses in Proposition 4.3. In this example, the function $B(x)$ can be lower-bounded by $-c_1|x|^2_{\mathcal{D}} - \kappa$, with $c_1 = 1.2, \kappa = 0.1$ and can be upper-bounded by $-c_2|x|^2_{\mathcal{D}}$, with $c_2 = 0.8$. Thus it satisfies (4.26). It remains for us to check whether (4.27) holds.

A routine computation shows that

$$\dot{B} = \frac{\partial B}{\partial x}(-\frac{\partial^T B}{\partial x} + u) \tag{4.35}$$

$$\leqslant -\left\|\frac{\partial B}{\partial x}\right\|^2 + \left\|\frac{\partial B}{\partial x}\right\| \|u\| \tag{4.36}$$

$$\leqslant -c_3|x|^2_{\mathcal{D}} + c_4\|u\|^2 \tag{4.37}$$

with $c_3 = 2$, and $c_4 = 0.5$ which satisfies (4.27).

Figure 4.4 shows the time plots of $\|x(t)\|$ and $|x(t)|^2_{\mathcal{D}}$ started from an initial condition $x_0 = (2, 2)$. The infinity norm of disturbance $u(t)$ is given by $\|u\|_{L^\infty} = 2.5112$. The dashed curve shows $\frac{c_2}{c_1}e^{\frac{c_3}{c_1}t}|x_0|^2_{\mathcal{D}} - \frac{c_4}{c_3}\|u\|^2_{L^\infty}e^{\frac{c_3}{c_1}t} - \frac{\kappa}{c_1}e^{\frac{c_3}{c_1}t}$, which is the lower-bound of $|x(t)|^2_{\mathcal{D}}$ such that the safety of (4.34) still preserved in the presence of disturbance.

Example 4.2. (*Input-to-state stability with guaranteed safety*)

Let us consider the same system (4.34) and the same unsafe set as in Example 4.1. We consider a disturbance signal u whose norm is given by $\|u\|_{L^\infty} = 2.6638$. In addition to ensuring the safety of the system, we also consider now the stabilization problem of the origin. The system (4.34) admits a ISS Lyapunov function $V(x) = x_1^2 + x_1x_2 + x_2^2$ that can be lower-bounded and upper-bounded by $0.5\|x\|^2$ and $2\|x\|^2$ respectively, so that (4.32) holds. As discussed in Proposition 4.5, we need to define ISSf barrier function locally in $\mathbb{B}(0)_{0.5}$ neighborhood of unsafe state $\mathcal{D}$, i.e., $\mathcal{X} := \mathcal{D} + \mathbb{B}(0)_{0.5} = \{x \in \mathbb{R}^2 | (x_1 - 4)^2 + (x_2 - 6)^2 < 9\}$. Since the ISSf barrier function $B(x)$ discussed in Example 1 is not lower-bounded so we can not define it locally, we can construct a lower-bounded one $\widetilde{B}(x)$ by following construction procedure in [53] instead. The lower-bounded ISSf barrier function is given as follows

$$\widetilde{B}(x) = B(\omega) + \oint_{\Gamma} 0.5\left(\cos\left(\frac{\pi}{\delta}B(\sigma)\right) + 1\right)\frac{\partial B(\sigma)}{\partial x}d\sigma \quad \forall x \in \mathcal{X}$$

where $\omega \in \partial\mathcal{D}$ is any point in the boundary of $\mathcal{D}$, Γ is any path from point ω to any point $\phi \in \mathcal{X}$, and $\delta = -B(\partial\mathcal{X}) = 5$. For $x \in \mathbb{R}^2 \setminus \mathcal{X}$, $\widetilde{B}(x)$ is defined as negative constant, i.e. $-\delta = -5$.

Following the same procedure discussed in [53] for achieving the stability and the safety of a system simultaneously, we then merge the ISS Lyapunov function and the ISSf barrier function into $V(x) + k_1\widetilde{B}(x) + k_2$, with $k_1 = 100$, $k_2 = -10$ such that the equations (4.31)-(4.33) are satisfied.

In this example, we use also the gradient of $W(x)$ as a control law for (4.34), i.e., $v = -\nabla_x W(x) = -\frac{\partial^T W}{\partial x}$. An explicit form of this gradient-based control law is

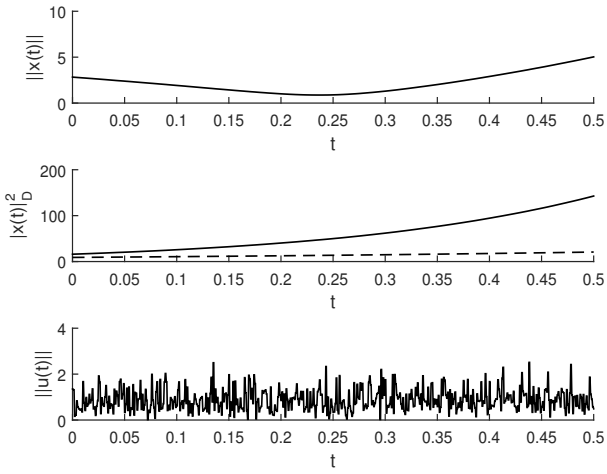

Figure 4.4: *The time plots of* $\|x(t)\|$, $|x(t)|^2_{\mathcal{D}}$, *and* $\|u(t)\|$ *with initial state* $x_0 = (2, 2)$. *The dashed curve in the middle plot shows the lower-bound of* $|x(t)|^2_{\mathcal{D}}$ *such that the safety of* (4.34) *is still preserved in the presence of disturbance* u.

given by

$$v = \begin{cases} -\nabla_x V(x) - k_1 \nabla_x \widetilde{B}(x) & \forall x \in \mathcal{X} \\ -\nabla_x V(x) & \forall x \in \mathbb{R}^2 \setminus \mathcal{X}. \end{cases} \tag{4.38}$$

Figure 4.5 shows the evolution of state x_1 and x_2 starting from four different initial conditions. Under the influence of bounded disturbance, the state trajectories converge to origin and avoid the unsafe state. Thus the system is input-to-state stable with guaranteed safety.

Figure 4.6 shows the time plots of $\|x(t)\|$ and $|x(t)|_{\mathcal{D}}$ started from $x_0 = (5, 8)$. From the figure we can conclude that the system is robustly stable and safe with respect to the disturbance $u(t)$.

4.7 Conclusion

In this chapter, we have presented a new notion of input-to-state safety for nonlinear systems which is complementary to the well-known input-to-state stability notion and provides safety certification for the system under the influence of external disturbance signals. We present also sufficient conditions for a nonlinear system to be ISSf by using a barrier certificate/function satisfying a dissipation inequality that resembles the ISS Lyapunov function.

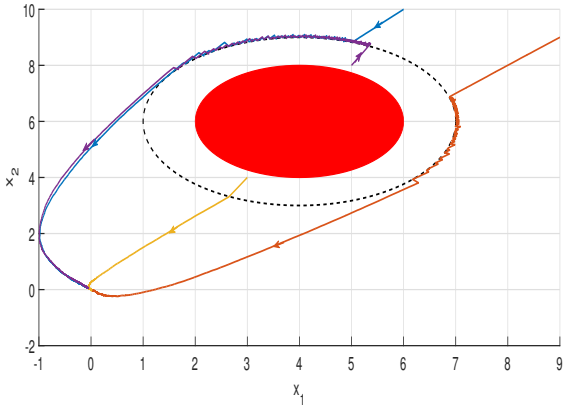

Figure 4.5: *State trajectories $x(t)$ discussed in Example 2, starting from four different initial conditions. The set of unsafe state $\mathcal{D}$ is shown in red area, and the boundary of $\mathcal{X}$ is shown by dashed line.*

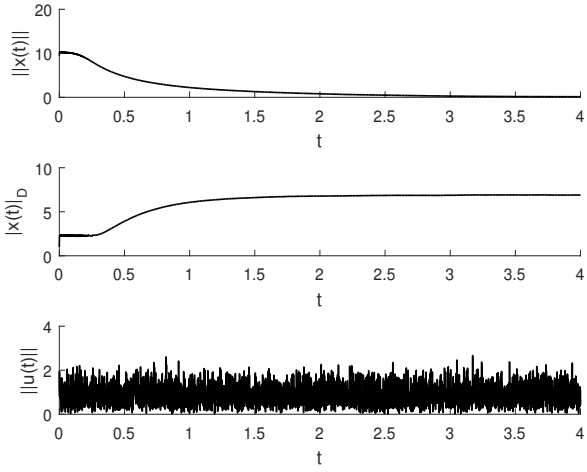

Figure 4.6: *The time plots of $\|x(t)\|$ and $|x(t)|_{\mathcal{D}}$ started from $x_0 = (5, 8)$, and disturbance signal $u(t)$ as discussed in Example 2.*

Chapter 5

Passivity based control with guaranteed safety

Chapter 5

Passivity based control with guaranteed safety

In this chapter, we study a Passivity-Based Control (PBC) design that solves asymptotic stability with guaranteed safety problem via Interconnection and Damping Assignment (IDA) approach. Firstly, we review the problem of stabilization with guaranteed safety in Section 5.2. Akin to the classical IDA-PBC method, we present in Section 5.3, our IDA-PBC approach for safety control systems where the original system is transformed via a state-feedback to a port-Hamiltonian system such that the corresponding interconnection and damping matrices and the energy function are shaped according to the given set of unsafe states and to the desired equilibrium point. By embedding it in a hybrid control framework, we show in Section 5.4 how the global results can also be obtained. We illustrate the efficacy of our proposed method on a nonlinear second-order system. The results in this chapter are based on our work in [52].

5.1 Introduction

Energy-based modeling and control design framework has become an indispensable tool for analyzing and controlling complex multi-domain physical systems. It enables one to gain insight and to control such complex systems through the use of the classical concept of energy and the exchange thereof between different physical entities. For example, the analysis and control of systems described by Euler-Lagrange equation have been investigated and discussed thoroughly in [38]. The concept has found many control applications in electro-mechanical systems, such as, robotics, and power systems (see e.g., [19, 27, 30, 39, 41]).

Another well-known energy-based modeling and control design framework is the port-Hamiltonian framework which is closely related to the Euler-Lagrange framework (through the use of Legendre transformation) and has a nice structure in the state equations. The energy exchange between physical elements and the dissipated energy is encapsulated in the interconnection and damping matrices in the vector field. We refer interested readers on the port-Hamiltonian framework to the textbook of [55] and to the articles in [40, 41, 42]. Control design methods that are based on port-Hamiltonian framework have recently been proposed, such as,

the Interconnection and Damping Assignment Passivity-Based Control (IDA-PBC) which will be the main focus of this paper, and the Energy-Balancing Passivity-Based Control in [28].

Generally speaking, the IDA-PBC method concerns with the design of a state feedback control law such that the closed-loop system has a desirable port-Hamiltonian structure (i.e., it has desired interconnection and damping matrices, as well as, a desired energy function). By an appropriate design of these interconnection and damping matrices and of the energy function, the stabilization of a desired equilibrium can be achieved. A generalization of IDA-PBC method has appeared in [8] where the interconnection and damping matrices are lumped.

In this chapter, we investigate the generalization of IDA-PBC to solve the problem of stabilization with guaranteed safety. Here, safety means that all admissible state trajectories do not violate system constraints or enter a set of unsafe states. In practical applications, especially in advanced instrumentations, robotics and complex systems, it is common that the system has state constraints or set of unsafe states, i.e. the subset of state domain that must be avoided. In this regards, the notion of safety must be also considered as an integral part in the control design process in addition to stability and robustness consideration.

The incorporation of safety aspect into the stabilization of the closed-loop system has been considered before in [1, 37, 49, 53, 60]. In [1, 49, 53], the well-known Control Lyapunov Function-based control method is combined with the Control Barrier Function-based control method which is proposed in [61] to solve the problem. The proposed control method does not impose unboundedness of energy function on the boundary of the set of unsafe states as imposed in [37, 60].

As an alternative to the aforementioned methods for solving stabilization with guaranteed safety problem, we propose in this chapter an energy-based method for solving this problem that offers a nice energy interpretation. The main approach behind our proposed method (as presented later in Proposition 5.2) is to assign a desired energy function such that it has a minimum at the desired equilibrium point and has local maxima in the set of unsafe states. Thus with an appropriate interconnection and damping matrices, the closed-loop system will converge to the minima (that includes the desired one) while avoiding the region of concavity where the unsafe state belongs to.

Although the proposed method can ensure that all admissible trajectories are safe, the method may not give a global stability result. This is due to the existence of multiple minima in the desired energy function.

In our second result (as given later in Proposition 5.4), we propose a hybrid control strategy that combines the global stability result of IDA-PBC with respect to the set of equilibria and another state-feedback controller that can steer the system from the set of undesired equilibria to the desired one. Hence, global stability with guaranteed safety is achieved.

5.2 Problem of stabilization with guaranteed safety

As we discussed in Chapter 2, the IDA-PBC is mainly focused on the stabilization of a point without taking into account the safety of the closed-loop system.

Before we discuss the inclusion of the safety aspect into the IDA-PBC design, let us first recall the problem of stabilization with guaranteed safety which has been studied recently in [49] and [53].

We denote $\mathcal{X}_0 \subset \mathbb{R}^n$ as the set of initial conditions, $\mathcal{D} \subset \mathbb{R}^n$ as the set of unsafe states where $\mathcal{D} \cap \mathcal{X}_0 = \varnothing$. Moreover, we always assume that $x^* \in \mathcal{X}_0$.

Definition 7 (Safety)**.** *Consider an autonomous system*

$$\dot{x} = f(x), \qquad x(0) \in \mathcal{X}_0, \tag{5.1}$$

where $x(t) \in \mathbb{R}^n$, the system is called safe *if for all $x(0) \in \mathcal{X}_0$ and for all $t \in \overline{\mathbb{R}}_+$, $x(t) \notin \mathcal{D}$.*

Stabilization with guaranteed safety control problem: Consider the system in (2.5) with a given set of initial conditions $\mathcal{X}_0 \subset \mathbb{R}^n$ and set of unsafe state $\mathcal{D} \subset \mathbb{R}^n$, design a feedback law $u = \beta(x)$ such that the closed loop system is safe and x^* is asymptotically stable, i.e. for all $x(0) \in \mathcal{X}_0$, we have that $x(t) \notin \mathcal{D}$ for all t and $\lim_{t\to\infty} \|x(t)\| = x^*$. Moreover, when $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$ we call it the *global stabilization with guaranteed safety control problem*.

Note that in the latter definition, there is a slight modification to the one used in [49, 53]. Instead of stabilizing the origin as considered in these papers, we consider here the stabilization of arbitrary admissible equilibra x^*. Here, *the set of admissible equilibria* is given by $\mathcal{E} = \{x \in \mathbb{R}^n | g^\perp(x) f(x) = 0\}$.

Let us now recall the result of stabilization of the origin with guaranteed safety as discussed in [49, Proposition 1].

Proposition 5.1. *Consider the autonomous system* (5.1) *with a given set of unsafe state $\mathcal{D}$ which is assumed to be open. Suppose that there exists a proper and lower-bounded $\mathcal{C}^1$ function $W : \mathbb{R}^n \to \mathbb{R}$ such that*

$$W(x) > 0 \qquad \forall x \in \mathcal{D} \tag{5.2a}$$

$$L_f W(x) < 0 \qquad \forall x \in \mathbb{R}^n \setminus (\mathcal{D} \cup \{0\}) \tag{5.2b}$$

$$\mathcal{U} := \{x \in \mathbb{R}^n | W(x) \leqslant 0\} \neq \varnothing \tag{5.2c}$$

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing \tag{5.2d}$$

then the system is safe with $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$ and the origin is asymptotically stable.

The function W that satisfies the hypotheses in Proposition 5.1 is called Lyapunov-Barrier function. In comparison to the related barrier function as used in

[37] and [60], the Lyapunov-Barrier function is not necessarily unbounded on the boundary of the unsafe state set.

5.3 Stabilization with guaranteed safety via IDA-PBC

As a first step towards the inclusion of safety aspect into the IDA-PBC design, we consider the problem of stabilization of a desired equilibrium x^* with guaranteed safety by combining the standard IDA-PBC with the result in Proposition 5.1 as follows.

Proposition 5.2. *Given a set of unsafe state $\mathcal{D}$ which is open, suppose that there exist H_d, J_d, R_d such that* (2.6) *holds and satisfy*

$$H_d(x) > 0 \qquad \forall x \in \mathcal{D} \tag{5.3a}$$

$$\mathcal{U} := \{x \in \mathbb{R}^n | H_d(x) \leqslant 0\} \neq \varnothing \tag{5.3b}$$

$$\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})} \cap \overline{\mathcal{D}} = \varnothing. \tag{5.3c}$$

Then the control law $u = \beta(x)$ where β as in (2.7) *solves stabilization of x^* with guaranteed safety control problem. Moreover, if x^* is the unique minimum of H_d and H_d is proper, then the result holds globally (i.e., $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$).*

Proof : By the assumption of (2.6a), the substitution of control law (2.7) into the system (2.5) results in a closed-loop system that is in the port-Hamiltonian structure as in (2.8). For the sake of simplicity, we denote the right hand side of (2.8) by $F(x)$.

It is easy to verify that

$$\dot{H}_d = \nabla^\top H_d(x(t))(J_d(x(t)) - R_d(x(t)))\nabla H_d(x(t)) \leqslant 0. \tag{5.4}$$

for all $x(t) \in \mathbb{R}^n \setminus \mathcal{D}$.

First, we prove that the closed-loop system is globally safe, i.e., for all $x(0) \in \mathbb{R}^n \setminus \mathcal{D}$, the corresponding state trajectory $x(t)$ never enters $\mathcal{D}$.

If $x(0) \in \mathcal{U}$ (i.e. $H_d(x(0)) \leqslant 0$ by the definition of $\mathcal{U}$) then it follows from (5.4), that H_d is non-increasing along the trajectory $x(t)$ satisfying $\dot{x} = F(x)$, thus $H_d(x(t)) - H_d(x(0)) \leqslant 0$ for all $t \in \mathbb{R}_+$. Hence, it implies that $H_d(x(t)) \leqslant 0$ for all $t \in \mathbb{R}_+$. In other words, the set $\mathcal{U}$ is forward invariant and $\lim\limits_{t\to\infty} x(t) \in \mathcal{U}$. Moreover by (5.3a) and the fact that $\mathcal{D} \cap \mathcal{U} = \varnothing$, the state trajectory $x(t) \notin \mathcal{D}$ for all $t \in \mathbb{R}_+$.

It remains now to show that for all $x(0) \in \mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$, we also have the property that $x(t) \notin \mathcal{D}$ for all $t \in \mathbb{R}_+$. In this case, we note that $H_d(x(0)) > 0$ and, as before, H_d is non-increasing along the trajectory of x for all t.

Since the set $\overline{\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})}$ does not intersect with the set $\overline{\mathcal{D}}$, it implies that the trajectory $x(t)$ will not enter $\mathcal{D}$ before it first reaches the boundary of $\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$, in which case, $H_d(x) = 0$. Once the trajectory $x(t)$ is on the boundary of $\mathbb{R}^n \setminus (\mathcal{D} \cup \mathcal{U})$, by the fact that $H_d(x(t)) - H_d(x(0)) \leqslant 0$, the state trajectory $x(t)$ will remain in $\mathcal{U}$ for the remaining t. Thus the closed-loop system is globally safe with the admissible set of initial conditions $\mathcal{X}_0 = \mathbb{R}^n \setminus \mathcal{D}$.

We will now prove the asymptotic stability of x^*. By the local convexity of H_d in the neighborhood of x^* (c.f. the assumption (2.6b)) and by (5.4) we can use H_d as a Lyapunov function to show the stability of x^*.

In this case, we define $\mathcal{X}_0$ as the largest domain of convexity of H_d around x^* excluding $\mathcal{D}$. By the convexity of H_d in $\mathcal{X}_0$ and by (5.4), it follows that $\mathcal{X}_0$ is forward invariant.

In particular, for all $x(0) = \mathcal{X}_0$, $x(t)$ is bounded for all t and by the application of La-Salle invariance principle, $x(t)$ converges to the largest invariance set contained in $\mathcal{M} := \{x \in \mathcal{X}_0 | \nabla^\top H_d(x) R_d(x) \nabla H_d(x) = 0\}$. By the strict convexity of H_d in $\mathcal{X}_0$, such an invariant set is given by $\{x^*\}$. In combination with the global safety property as proven above, we achieve the (local) stability of x^* with guaranteed safety.

Finally, if x^* is the unique minimum of H_d and H_d is proper then the global results holds by the use of La-Salle invariance principle. □

It is easy to observe that instead of finding J_d and R_d separately as in Proposition 5.2, we can simultaneously design them as pursued in [8] where we need to find $F_d(x)$ such that (2.9) and (2.10) hold. Note that this relaxed condition does not change our previous result on the stability, neither on the safety of the closed-loop system. It only relaxes the solvability of the PDE in the expense of port-Hamiltonian structure. More precisely, we state it in the following corollary.

Corollary 5.3. *Given a set of unsafe state $\mathcal{D}$ which is open, suppose that there exist H_d and F_d such that* (2.6b)*,* (2.9)*,* (2.10) *hold and satisfy* (5.3)*. Then the control law $u = \beta(x)$ as in* (2.11) *solves stabilization of x^* with guaranteed safety control problem.* △

Example 5.1. In order to illustrate the main result in Proposition 5.2, let us consider the following system.

$$\begin{aligned} \dot{x}_1 &= -x_1^3 + 2.25 x_1 x_2^2 + 3.5 x_2^3 - 1500 x_2 \\ \dot{x}_2 &= u. \end{aligned} \tag{5.5}$$

It can be shown that the origin can be made globally-asymptotically stable (GAS) using a simple control law $u = -k x_2$ with $k > 0$. First, we note that the x_1-

subsystem is input-to-state stable (ISS) with respect to x_2 (for example, using $V(x_1) = \frac{1}{2}x_1^2$ as the ISS Lyapunov function). Hence, if we let $u = -kx_2$, the x_2-subsystem converges exponentially to zero, and this implies that, by the ISS property of x_1-subsystem, $x_1(t)$ converges also to zero.

We will now consider the problem of stabilization of (5.5) with guaranteed safety via IDA-PBC. Assume that the set of unsafe state is defined by $\mathcal{D} = \{x \in \mathbb{R}^n | (x_1 - 2)^2 + (x_1 - 2)x_2 + x_2^2 < 10\}$. For simplicity, we consider the following $H_d : \mathbb{R}^2 \to \mathbb{R}$

$$H_d = \begin{pmatrix} x_1^2 & x_1x_2 & x_2^2 \end{pmatrix} \begin{pmatrix} 1 & 0.5 & -0.125 \\ 0.5 & 1 & 0.5 \\ -0.125 & 0.5 & 1 \end{pmatrix} \begin{pmatrix} x_1^2 \\ x_1x_2 \\ x_2^2 \end{pmatrix} - 1000 \begin{pmatrix} x_1 - 2 & x_2 \end{pmatrix} \begin{pmatrix} 1 & 0.5 \\ 0.5 & 1 \end{pmatrix} \begin{pmatrix} x_1 - 2 \\ x_2 \end{pmatrix} + 10000$$

which is proper and has minima at the desired equilibrium $x^* = (-18.6467, -17.8454)^\top$ and at other equilibria $x_{u1} = (-26.948, 25.532)^\top$, $x_{u2} = (16.7688, 17.7117)^\top$, $x_{u3} = (24.3953, -26.0258)^\top$. The contour plot of this H_d is shown in Figure 5.1.

Now, in order to design the controller as in Corollary 5.3, we need to solve the PDE (2.10) where in this case, $g^\perp(x) = \begin{pmatrix} g_1(x) & 0 \end{pmatrix}$, with $g_1 : \mathbb{R}^2 \to \mathbb{R}$ and $F_d(x) = \left(\begin{smallmatrix} a(x) & b(x) \\ c(x) & d(x) \end{smallmatrix}\right)$ that must be designed and also satisfy (2.9). It follows directly from (2.10) that we need to satisfy

$$-x_1^3 + 2.25x_1x_2^2 + 3.5x_2^3 - 1500x_2 = a(x)\nabla_{x_1}H_d(x) + b(x)\nabla_{x_2}H_d(x). \qquad (5.6)$$

A possible solution to this equation is to let $a(x) = -0.5$ and $b(x) = 1$. In order to fulfill (2.9), we can take $c(x) = -1$ and $d(x) = c_1$ with $c_1 \leqslant 0$. Using these numerical values, the simulation results of the closed-loop system with several different initial conditions are shown in Figure 5.2. It can be seen from this figure that we achieve the (local) stabilization with guaranteed safety at the desired equilibrium point x^*. One can also notice from the simulation that there exists other attractive equilibrium points x_{u1}, x_{u2}, x_{u3}. Moreover, we achieve global stabilization with guaranteed safety with respect to $\mathcal{E} = \{x^*, x_{u1}, x_{u2}, x_{u3}\}$. $\triangle$

As shown in Example 5.1, the region-of-attraction of the desired equilibrium point can rather be restrictive. For this example, we plot in Figure 5.3 the numerically-estimated region-of-attraction (RoA) for every equilibria in $\mathcal{E}$. In this plot, the RoA for x^* is shown in yellow, while that for the other equilibria x_{u1}, x_{u2} and x_{u3} are shown in red, blue, and green, respectively.

In fact, the region-of-attraction is influenced by the choice of F_d, particularly,

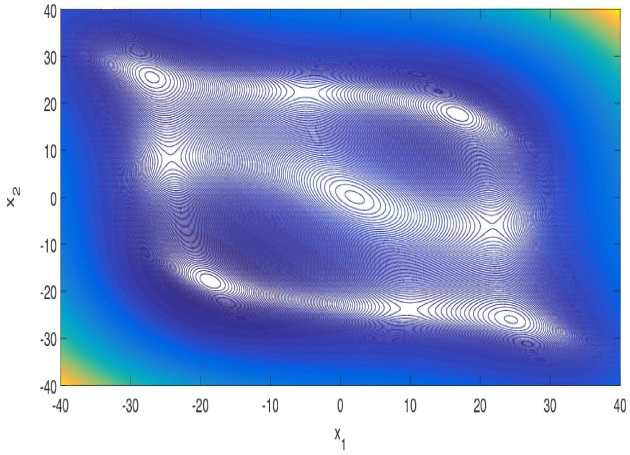

Figure 5.1: *The contour of the desired energy function H_d as used in Example 5.1. The function H_d has four minima, one maximum, and four saddle-points.*

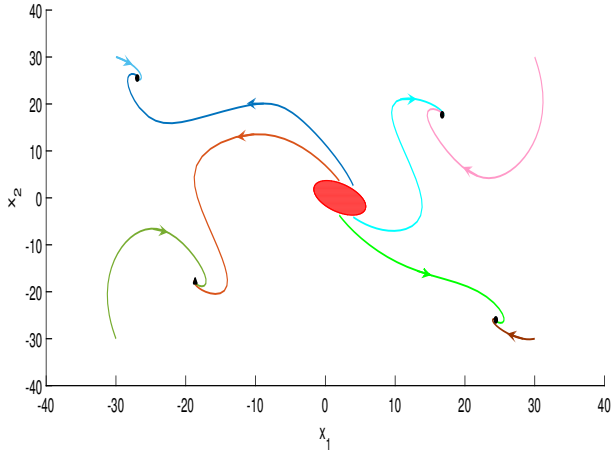

Figure 5.2: *The numerical simulation result of the closed-loop system using IDA-PBC method in Example 5.1 from eight different initial conditions. The desired equilibrium is shown in triangle while the other equilibria are shown in circle. The set of unsafe states $\mathcal{D}$ is shown in the red elliptic-parabolic. All trajectories converge to the equilibria and avoid $\mathcal{D}$*

the damping part. In Figure 5.4 we show the different region-of-attraction for different damping element by varying the value of c_1. In this figure, the RoA of x^* has gained additional area on the upper side, as well as on the lower-right side.

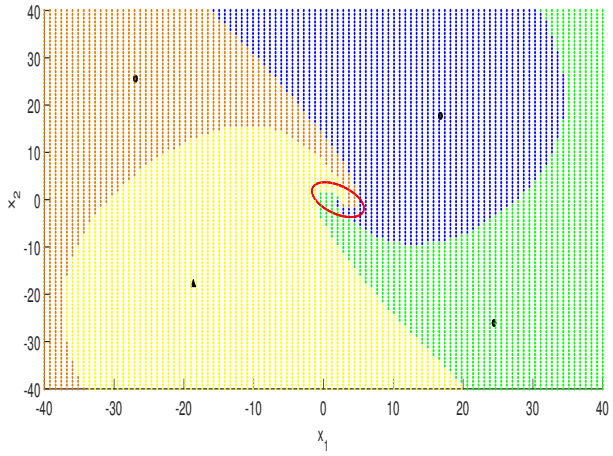

Figure 5.3: *The numerical estimation of region-of-attraction (RoA) of the closed-loop system in Example 5.1 for every equilibria with $c_1 = -1$. The RoA of the desired equilibrium point x^* is shown in yellow, while that for the other equilibria x_{u1}, x_{u2} and x_{u3} are shown in red, blue, and green, respectively. The boundary of $\mathcal{D}$ is shown in red line.*

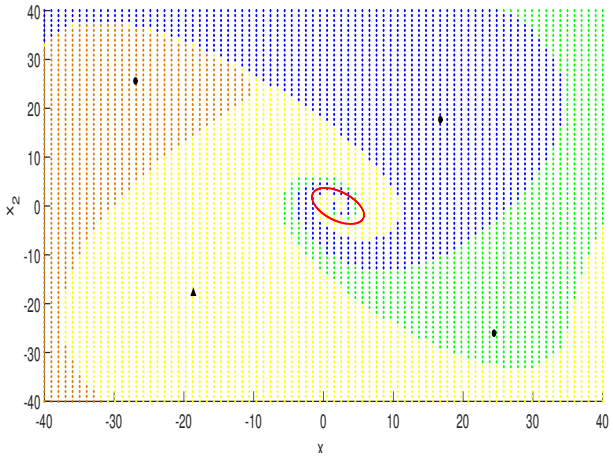

Figure 5.4: *The numerical estimation of the region-of-attraction (RoA) of the closed-loop system in Example 5.1 for every equilibria with $c_1 = 0$. The rest of the information is the same as that in Fig.5.3.*

However, the RoA near the set of unsafe state is reduced.

In the following section we will discuss a hybrid strategy for achieving global

stabilization with guaranteed safety.

5.4 Global stabilization with guaranteed safety

As has been shown before, the IDA-PBC approach has allowed us to achieve local stabilization of a desired equilibrium with guaranteed safety. At the same time, it may also introduce undesired equilibrium points that prevent us from achieving a global stabilization with guaranteed safety. Despite this, if one is interested only in the safety aspect, the aforementioned proposed control can, in fact, guarantee the global safety, i.e., for all admissible initial condition $\mathbb{R}^n \backslash \mathcal{D}$, the state trajectory will never enter the set of unsafe state $\mathcal{D}$. Indeed, in our previous example, we have shown that the state trajectory from any initial condition converges to the set of equilibrium points $\mathcal{E}$ without entering $\mathcal{D}$.

In this section, we propose a simple hybrid control strategy where we combine the IDA-PBC based state feedback that achieves set asymptotic stabilization with guaranteed global safety and other feedback controllers that can steer the system trajectories from the neighborhood of $\mathcal{E}_u$ to the desired equilibrium point x^*. As will be shown later, this hybrid strategy provides a simple solution to the global stabilization with guaranteed safety.

Prior to describing our proposed hybrid controller, let us recall the following definitions on hybrid automaton as discussed in [33].

Let a hybrid automaton be described by the tuple $(Q, X, F, Q_0 \times X_0, Dom, E, \mathcal{G}, \mathcal{R})$ where $Q \subset Z_+$ is a finite set of discrete variables, $X \in \mathbb{R}^n$ is the set of continuous variables, $F : Q \times X \to X$ defines the vector field of the continuous variables, $Q_0 \times X_0$ is the set of initial conditions, $Dom : Q \to X$ defines the domain of each discrete variable $q \in Q$, $E \subset Q \times Q$ denotes the set of edges that describe different transitions/jumps between different discrete state. The set $\mathcal{G} : E \to X$ defines the guard conditions that can initiate the transition or jump to another discrete state. The maps $\mathcal{R} : E \times X \to X$ defines the resetting of the continuous variables following a transition/jump.

Using the above notion of hybrid automaton, we consider hybrid automaton as shown in Figure 5.5 as our proposed hybrid strategy. In this setting, $Q = \{1, 2\}$, $X = \mathbb{R}^n$, the set of initial condition is given by $Q_0 \times X_0 = \{1\} \times \mathbb{R}^n \backslash \mathcal{D}$. For $q = 1$, $F(1, x)$ is a vector field of the closed-loop system using the IDA-PBC method, i.e., $F(1, x) = (J_d(x) - R_d(x)) \nabla H_d(x)$. On the other hand, $F(2, x)$ is a vector field of the closed-loop system using another state-feedback control law $u = k(x)$ that can steer the system trajectories from the neighborhood of $\mathcal{E}_u$ to the desired one x^* without entering $\mathcal{D}$. If the latter state-feedback controller exists then the global stabilization with guaranteed safety problem is solvable by combining it with the IDA-PBC control via hybrid automaton as in Figure 5.5. In this case, the guards

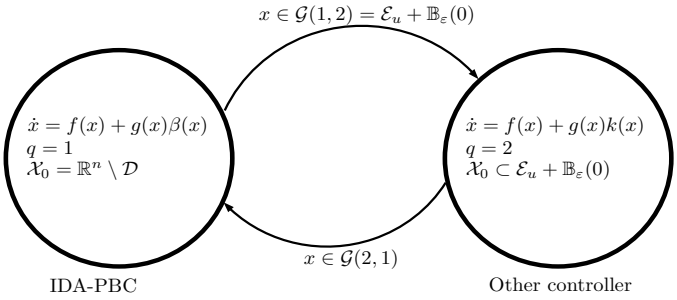

Figure 5.5: *Hybrid automaton used in Proposition 4 for solving global stabilization with guaranteed safety by using IDA-PBC and another local stabilizing feedback controller.*

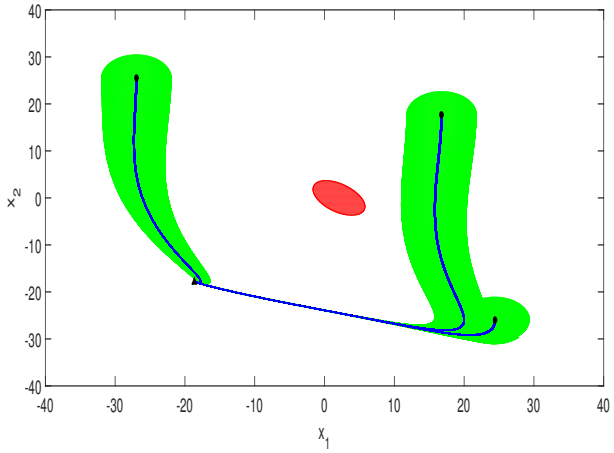

Figure 5.6: *The plot of positively invariant set $\Omega(x(0))$ for the system in Example 5.1 using a state feedback $u = -K(x - x^*)$, with $K = [1339.0 \quad 4673.4]$. The plot of $\Omega(\mathcal{E}_u + \mathbb{B}_5(0))$ is shown in green while the plot of $\Omega(\mathcal{E}_u + \mathbb{B}_{0.1}(0))$ is shown in blue.*

$\mathcal{G}(1,2)$ and $\mathcal{G}(2,1)$ are defined by the neighborhood of $\mathcal{E}_u$ and the boundary of the positive invariant set due to the application of $u = k(x)$ that contains the neighborhood of $\mathcal{E}_u$, respectively. The jump map $\mathcal{R}$ is simply given by an identity.

We note that the existence of the second state-feedback control law $u = k(x)$ is a mild assumption. For this controller to exist, we need only to assume that x^* is reachable from any point in the neighborhood of $\mathcal{E}_u$ without entering $\mathcal{D}$.

Proposition 5.4. *Assume the system as in Proposition 5.2 with the given control law $u = \beta(x)$ and a proper H_d. Suppose that there exist a constant $\delta > 0$ and a control law $u = k(x)$ such that for all $x_0 \in \mathcal{E}_u + \mathbb{B}_\delta(0)$ the corresponding state trajectory*

converges to x^* and is safe, i.e., the positive invariant set $\Omega\big(\mathcal{E}_u + \mathbb{B}_\delta(0)\big) =: \Phi$ does not intersect $\mathcal{D}$. Then the global stabilization with guaranteed safety problem is solvable using hybrid control as in Figure 5.5 with $\mathcal{G}(1,2) = \mathcal{E}_u + \mathbb{B}_\epsilon(0)$, $0 < \epsilon < \delta$, $\mathcal{G}(2,1) = \partial\Phi$ and $\mathcal{R} = Id$.

Proof : As assumed in the proposition, the hybrid automaton is initialized with the first mode $q = 1$.

Following the same proof as in Proposition 5.2, the properness of H_d along with inequality (5.4) implies that the state trajectories x asymptotically converges to $\mathcal{E}$. It has also been proven in Proposition 5.2 that the control law $u = \beta(x)$ with a proper H_d guarantees global safety property of the closed-loop system. It remains to show that $x(t) \to x^*$ for the hybrid system.

By the global attractivity of $\mathcal{E}$, x converges to x^* or to $\mathcal{E}_u$. If for some $x(0)$, x converges to x^* then the transition to $q = 2$ will never happen and we obtain our result. Otherwise, there exists $T > 0$ such that $x(T) \in \partial(\mathcal{E}_u + \mathbb{B}_\epsilon(0))$ which will initiate the jump to $q = 2$. During the jump, we have $x^+(T) = x(T) =: x_T$ by our assumption and the closed-loop system will be described by

$$\dot{x} = f(x) + g(x)k(x), \qquad x(T) = x_T \in \mathcal{E}_u + \mathbb{B}_\epsilon(0).$$

By our assumption on $k(x)$, the state trajectory x will remain in the positively invariant set $\Omega(\mathcal{E}_u + \mathbb{B}_\epsilon(0))$ and in particular, will never jump to $q = 1$. Thus x converges to x^* as desired. This proves our claim. □

The proposed approach provides a practical solution to the global stabilization with guaranteed safety. In this case, in addition to the IDA-PBC conditions, we need to find stabilizing controllers for only a finite and arbitrary small set of initial conditions. Hence, we may not need to design a large number of switched controllers defined on different polytope/manifold which can be numerically intractable for higher-order systems.

Let us now consider again the same system as in Example 5.1 where the IDA-PBC based controller is designed with $c_1 = -1$. One can evaluate directly that by applying $u = -K(x - x^*)$ where $K = [1339.0 \quad 4673.4]$, it can steer the system trajectories from any initial condition in $\mathcal{E}_u + \mathbb{B}_5(0)$. Indeed, Figure 5.6 shows the positively invariant set of the closed-loop system for initial condition in $\mathcal{E}_u + \mathbb{B}_5(0)$ (shown in green) and in $\mathcal{E}_u + \mathbb{B}_{0.1}(0)$ (shown in blue). Equipped with this simple controller, we implement the hybrid control strategy as described in Proposition 5.4 and the simulation results are shown in Figure 5.7 where we use the same initial conditions as those used in Figure 5.2. In comparison to the results in Figure 5.2, we have now the global convergence of x to x^* using the hybrid control.

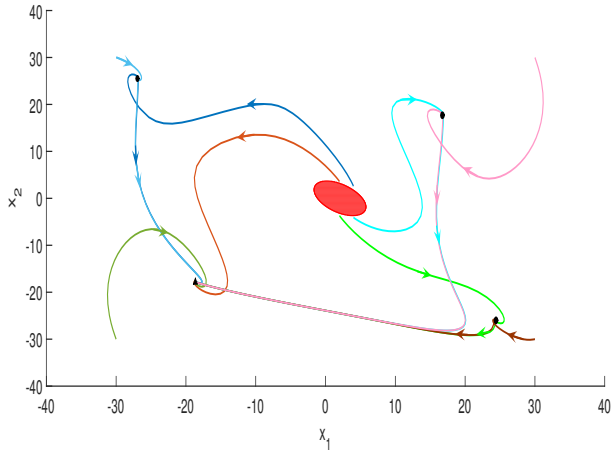

Figure 5.7: *The numerical simulation result of the closed-loop system in Example 5.1 using hybrid control method as in Proposition 5.4. The closed-loop trajectories are based on the same initial conditions as those used in Fig. 5.2 and all trajectories converge to x^* without entering $\mathcal{D}$ (shown in red).*

5.5 Conclusions

The use of energy-based control design has been shown to be applicable for solving the problem of stabilization with guaranteed safety. The avoidance of unsafe state is achieved by an appropriate design of the energy function which may result into the existence of attractive undesired equilibria. By adopting a hybrid control framework, we can obtain the global result with less restrictive conditions on the other mode.

Chapter 6

Conclusions and Future Work

Chapter 6
Conclusions and Future Work

Conclusions

In this thesis, we have presented a body of works that are relevant to the design of control systems with guaranteed safety. Firstly, we propose several control design techniques that can stabilize the plant while providing a guarantee or certificate on the safety of the closed-loop system. Secondly, we propose a novel robustness analysis tool that can be used to quantify the margin of safety (or the fragility) of the closed-loop system.

We have presented in Chapter 3 a novel method to achieve our control goal by merging a classical Control Lyapunov Function with (multiple) Control Barrier Function(s) where the merged function becomes a Control Lyapunov-Barrier Function. We show in Proposition 3.4 that the merging is simply based on a suitable linear combination of CLF and a compactly supported CBF. By suitable linear combination, we mean that there is a gain in the linear combination which is lower bounded by a term that depends on the bound of CLF and the boundary of the unsafe state. When the CBF is not compactly supported, then we provide the method to merge both CLF and CBF as discussed in Proposition 3.5. In this proposition, we propose a method to modify the original CBF into a compactly supported CBF and then combine it with CLF as in Proposition 3.4. Further extension of Proposition 3.4 is given in Proposition 3.7 where we can combine directly a CLF with multiple CBFs. The combination is again based on a linear combination of these functions. As before, there are lower bounds on the gains in this combination. Consequently, the application of Sontag's universal control law using the resulting Control Lyapunov-Barrier Function gives us the desired control law. On the other hand, in Chapter 5, we explore another design method where we solve the problem of stabilization with guaranteed safety using control laws that are motivated by the popular IDA-PBC approach. In Proposition 5.2, we have shown that under similar IDA-PBC equations with additional constraints on the desired Hamiltonian (but not on the interconnection and damping matrices) we can apply the same control law as in IDA-PBC for solving the stabilization with guaranteed safety problem. However, as shown in the simple Example 5.1, if we are interested only in the stabilization of a desired point, the proposed IDA-PBC method may give rise to undesirable attractive multiple equilbria. In this case, we may only achieve local

stabilization. In order to circumvent this problem, we may use a hybrid control strategy with, at least, two automata. In Proposition 5.4, we present sufficient conditions for global stabilization using only two automata.

We have introduced a novel concept of input-to-state safety in Chapter 4. It complements the popular notion of input-to-state stability and is very relevant for quantifying the margin of safety of a closed-loop safety control system. In Proposition 4.1, we present sufficient conditions for a system to be input-to-state safe using an ISSf barrier function, akin to the ISS Lyapunov function for characterizing input-to-state stability of nonlinear systems. We further study the exponential case of input-to-state safety in Proposition 4.3. Here, we show that if we have quadratic ISSf barrier function then the system is ISSf with an exponential rate. We discuss as well the combination of standard ISS property with our proposed ISSf in nonlinear systems. In particular, we present in Proposition 4.5 the merged ISS-ISSf Lyapunov-barrier function that can guarantee the ISS and ISSf properties of the system.

Future Work

In Chapter 3, we have discussed ways to combine a Control Lyapunov Function with multiple Control Barrier Functions. This enables us to incorporate a number of sets of unsafe state in the final control design by defining a different CBF for each set. However, if, in addition to the stabilization and safety guarantee, there are other control requirements such as multiple LQR functions for different domain in state space then we need to find ways to combine multiple CLFs and multiple CBFs at the same time. This remains currently an open problem.

It is also interesting to combine the results in Chapter 3 and Chapter 4 for designing control laws that work in event-triggered fashion. For a stabilizing controller, it is known in literature that an event-triggered stabilizing control law can be designed by a simple algebraic manipulation of the ISS Lyapunov inequality. In particular, if there is a simple stabilizing control law such that the closed-loop system is ISS with respect to the measurement error then there is an event-triggered control law. In a similar fashion, we can ask ourselves whether it is possible to design an event-triggered control law for stabilizing a plant with guaranteed safety when there is a continuous-time control law that achieves input-to-state safety with respect to the measurement error.

When we focus on our contribution in Chapter 3, we have presented sufficient conditions for stability with guaranteed safety, namely, through the existence of a Lyapunov-Barrier function. The converse to this result is still an open problem. However, recent work in [62] on the converse result for barrier certificate may shed light on this problem.

Similar to the above mentioned problem, the converse result for input-to-state safety is also an interesting topic to be addressed in the future.

Finally, we have not addressed yet in this thesis the analysis of interconnected safety control systems. For ISS systems, one can already employ small-gain conditions to analyze the stability of interconnected ISS systems. It is interesting to investigate further whether we can define a 'small-gain' condition that can guarantee that the interconnection of ISSf systems will remain ISSf.

Bibliography

[1] A. D. Ames, J. W. Grizzle, and P. Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *53rd IEEE Conference on Decision and Control*, pages 6271–6278, Dec 2014. doi: 10.1109/CDC.2014.7040372.

[2] V. Andrieu and C. Prieur. Uniting two control lyapunov functions for affine systems. *IEEE Transactions on Automatic Control*, 55(8):1923–1927, Aug 2010. ISSN 0018-9286. doi: 10.1109/TAC.2010.2049689.

[3] V. Andrieu, B. Jayawardhana, and L. Praly. On transverse exponential stability and its use in incremental stability, observer and synchronization. In *52nd IEEE Conference on Decision and Control*, pages 5915–5920, Dec 2013. doi: 10.1109/CDC.2013.6760822.

[4] D. Angeli and D. Efimov. Characterizations of input-to-state stability for systems with multiple invariant sets. *IEEE Transactions on Automatic Control*, 60(12):3242–3256, Dec 2015. ISSN 0018-9286. doi: 10.1109/TAC.2015.2418676.

[5] Zvi Artstein. Stabilization with relaxed controls. *Nonlinear Analysis: Theory, Methods & Applications*, 7(11):1163 – 1173, 1983. ISSN 0362-546X. doi: http://dx.doi.org/10.1016/0362-546X(83)90049-4. URL `http://www.sciencedirect.com/science/article/pii/0362546X83900494`.

[6] A. Balestrino, A. Caiti, and E. Crisostomi. Logical composition of lyapunov functions. *International Journal of Control*, 84(3):563–573, 2011. doi: 10.1080/00207179.2011.562549. URL `http://dx.doi.org/10.1080/00207179.2011.562549`.

[7] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta. Ensuring safety, security, and sustainability of mission-critical cyber physical

systems. *Proceedings of the IEEE*, 100(1):283–299, Jan 2012. ISSN 0018-9219. doi: 10.1109/JPROC.2011.2165689.

[8] Carles Batlle, Arnau Dria-Cerezo, Gerardo Espinosa-Prez, and Romeo Ortega. Simultaneous interconnection and damping assignment passivity-based control: the induction machine case study. *International Journal of Control*, 82(2):241–255, 2009. doi: 10.1080/00207170802050817. URL http://www.tandfonline.com/doi/abs/10.1080/00207170802050817.

[9] A. Bemporad. Reference governor for constrained nonlinear systems. *IEEE Transactions on Automatic Control*, 43(3):415–419, Mar 1998. ISSN 0018-9286. doi: 10.1109/9.661611.

[10] A. Bemporad, A. Casavola, and E. Mosca. Nonlinear control of constrained linear systems via predictive reference management. *IEEE Transactions on Automatic Control*, 42(3):340–349, Mar 1997. ISSN 0018-9286. doi: 10.1109/9.557577.

[11] A. Bemporad, F. Borrelli, and M. Morari. Model predictive control based on linear programming - the explicit solution. *IEEE Transactions on Automatic Control*, 47(12):1974–1985, Dec 2002. ISSN 0018-9286. doi: 10.1109/TAC.2002.805688.

[12] Guido Blankenstein, Romeo Ortega, and Arjan J. Van Der Schaft. The matching conditions of controlled lagrangians and ida-passivity based control. *International Journal of Control*, 75(9):645–665, 2002. doi: 10.1080/00207170210135939. URL http://dx.doi.org/10.1080/00207170210135939.

[13] Fernando Castaos and Romeo Ortega. Energy-balancing passivity-based control is equivalent to dissipation and output invariance. *Systems & Control Letters*, 58(8):553 – 560, 2009. ISSN 0167-6911. doi: http://dx.doi.org/10.1016/j.sysconle.2009.03.007. URL http://www.sciencedirect.com/science/article/pii/S0167691109000565.

[14] Fernando Castaos, Romeo Ortega, Arjan van der Schaft, and Alessandro Astolfi. Asymptotic stabilization via control by interconnection of port-hamiltonian systems. *Automatica*, 45(7):1611 – 1618, 2009. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2009.03.015. URL http://www.sciencedirect.com/science/article/pii/S0005109809001393.

[15] Francis Clarke. Lyapunov functions and discontinuous stabilizing feedback. *Annual Reviews in Control*, 35(1):13 – 33, 2011. ISSN 1367-5788. doi: http://dx.doi.org/10.1016/j.arcontrol.2011.03.001. URL http://www.sciencedirect.com/science/article/pii/S1367578811000022.

[16] D. V. Dimarogonas and K. J. Kyriakopoulos. A feedback stabilization and collision avoidance scheme for multiple independent nonholonomic non-point agents. In *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005.*, pages 820–825, June 2005. doi: 10.1109/.2005.1467120.

[17] K. D. Do. Bounded controllers for formation stabilization of mobile agents with limited sensing ranges. *IEEE Transactions on Automatic Control*, 52(3): 569–576, March 2007. ISSN 0018-9286. doi: 10.1109/TAC.2007.892382.

[18] Vincent Duindam, Alessandro Macchelli, Stefano Stramigioli, and Herman Bruyninckx. *Modeling and Control of Complex Physical Systems: The Port-Hamiltonian Approach*. Springer Publishing Company, Incorporated, 2014. ISBN 3642420753, 9783642420757.

[19] Elosa Garca-Canseco, Dimitri Jeltsema, Romeo Ortega, and Jacquelien M.A. Scherpen. Power-based control of physical systems. *Automatica*, 46(1): 127 – 132, 2010. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2009.10.012. URL `http://www.sciencedirect.com/science/article/pii/S0005109809004737`.

[20] E. G. Gilbert and I. Kolmanovsky. A generalized reference governor for nonlinear systems. In *Decision and Control, 2001. Proceedings of the 40th IEEE Conference on*, volume 5, pages 4222–4227 vol.5, 2001. doi: 10.1109/.2001.980851.

[21] E. G. Gilbert and K. T. Tan. Linear systems with state and control constraints: the theory and application of maximal output admissible sets. *IEEE Transactions on Automatic Control*, 36(9):1008–1020, Sep 1991. ISSN 0018-9286. doi: 10.1109/9.83532.

[22] S. Grammatico, F. Blanchini, and A. Caiti. Control-sharing and merging control lyapunov functions. *IEEE Transactions on Automatic Control*, 59(1): 107–119, Jan 2014. ISSN 0018-9286. doi: 10.1109/TAC.2013.2281479.

[23] Eugene P. Ryan Hartmut Logemann. Asymptotic behaviour of nonlinear systems. *The American Mathematical Monthly*, 111(10):864–889, 2004. ISSN 00029890, 19300972. URL `http://www.jstor.org/stable/4145095`.

[24] B. Jayawardhana and G. Weiss. State convergence of passive nonlinear systems with an l^2 input. *IEEE Transactions on Automatic Control*, 54(7): 1723–1727, July 2009. ISSN 0018-9286. doi: 10.1109/TAC.2009.2020661.

[25] B. Jayawardhana, E. P. Ryan, and A. R. Teel. Bounded-energy-input convergent-state property of dissipative nonlinear systems: An iiss approach.

IEEE Transactions on Automatic Control, 55(1):159–164, Jan 2010. ISSN 0018-9286. doi: 10.1109/TAC.2009.2033754.

[26] B. Jayawardhana, H. Logemann, and E. P. Ryan. The circle criterion and input-to-state stability. *IEEE Control Systems*, 31(4):32–67, Aug 2011. ISSN 1066-033X. doi: 10.1109/MCS.2011.941143.

[27] Bayu Jayawardhana and George Weiss. Tracking and disturbance rejection for fully actuated mechanical systems. *Automatica*, 44(11):2863 – 2868, 2008. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2008.03.030. URL http://www.sciencedirect.com/science/article/pii/S0005109808002525.

[28] Dimitri Jeltsema, Romeo Ortega, and Jacquelien M.A. Scherpen. An energy-balancing perspective of interconnection and damping assignment control of nonlinear systems. *Automatica*, 40(9):1643 – 1646, 2004. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2004.04.007. URL http://www.sciencedirect.com/science/article/pii/S0005109804001256.

[29] Z. P. Jiang, A. R. Teel, and L. Praly. Small-gain theorem for iss systems and applications. *Mathematics of Control, Signals and Systems*, 7(2):95–120, Jun 1994. ISSN 1435-568X. doi: 10.1007/BF01211469. URL https://doi.org/10.1007/BF01211469.

[30] P. Kotyczka and B. Lohmann. Parametrization of ida-pbc by assignment of local linear dynamics. In *Control Conference (ECC), 2009 European*, pages 4721–4726, Aug 2009.

[31] Miroslav Krstic, Petar V. Kokotovic, and Ioannis Kanellakopoulos. *Nonlinear and Adaptive Control Design*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 1995. ISBN 0471127329.

[32] J. La Salle. *The Stability of Dynamical Systems*. Society for Industrial and Applied Mathematics, 1976. doi: 10.1137/1.9781611970432. URL http://epubs.siam.org/doi/abs/10.1137/1.9781611970432.

[33] J. Lygeros, K. H. Johansson, S. N. Simic, Jun Zhang, and S. S. Sastry. Dynamical properties of hybrid automata. *IEEE Transactions on Automatic Control*, 48 (1):2–17, Jan 2003. ISSN 0018-9286. doi: 10.1109/TAC.2002.806650.

[34] J.M. Maciejowski. *Predictive Control: With Constraints*. Pearson Education. Prentice Hall, 2002. ISBN 9780201398236. URL https://books.google.nl/books?id=HV_Y58c7KiwC.

[35] A. Mehra, W. L. Ma, F. Berg, P. Tabuada, J. W. Grizzle, and A. D. Ames. Adaptive cruise control: Experimental validation of advanced controllers on scale-model cars. In *2015 American Control Conference (ACC)*, pages 1411–1418, July 2015. doi: 10.1109/ACC.2015.7170931.

[36] Manfred Morari and Jay H. Lee. Model predictive control: past, present and future. *Computers & Chemical Engineering*, 23(45):667 – 682, 1999. ISSN 0098-1354. doi: http://dx.doi.org/10.1016/S0098-1354(98)00301-9. URL http://www.sciencedirect.com/science/article/pii/S0098135498003019.

[37] K. B. Ngo, R. Mahony, and Zhong-Ping Jiang. Integrator backstepping using barrier functions for systems with multiple state constraints. In *Proceedings of the 44th IEEE Conference on Decision and Control*, pages 8306–8312, Dec 2005. doi: 10.1109/CDC.2005.1583507.

[38] R. Ortega, J.A.L. Perez, P.J. Nicklasson, and H. Sira-Ramirez. *Passivity-based Control of Euler-Lagrange Systems: Mechanical, Electrical and Electromechanical Applications*. Communications and Control Engineering. Springer London, 1998. ISBN 9781852330163. URL https://books.google.nl/books?id=GCVn0oRqP9YC.

[39] R. Ortega, A. J. Van Der Schaft, I. Mareels, and B. Maschke. Putting energy back in control. *IEEE Control Systems*, 21(2):18–33, Apr 2001. ISSN 1066-033X. doi: 10.1109/37.915398.

[40] R. Ortega, A. van der Schaft, F. Castanos, and A. Astolfi. Control by interconnection and standard passivity-based control of port-hamiltonian systems. *IEEE Transactions on Automatic Control*, 53(11):2527–2542, Dec 2008. ISSN 0018-9286. doi: 10.1109/TAC.2008.2006930.

[41] Romeo Ortega and Elosa Garca-Canseco. Interconnection and damping assignment passivity-based control: A survey. *European Journal of Control*, 10(5):432 – 450, 2004. ISSN 0947-3580. doi: http://dx.doi.org/10.3166/ejc.10.432-450. URL http://www.sciencedirect.com/science/article/pii/S094735800470391X.

[42] Romeo Ortega, Arjan van der Schaft, Bernhard Maschke, and Gerardo Escobar. Interconnection and damping assignment passivity-based control of port-controlled hamiltonian systems. *Automatica*, 38(4):585 – 596, 2002. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/S0005-1098(01)00278-3. URL http://www.sciencedirect.com/science/article/pii/S0005109801002783.

[43] Stephen Prajna. *Optimization-based methods for nonlinear and hybrid systems verification*. Dissertation (Ph.D.). California Institute of Technology, 2005. URL http://resolver.caltech.edu/CaltechETD:etd-05272005-144358.

[44] Stephen Prajna and Ali Jadbabaie. *Hybrid Systems: Computation and Control: 7th International Workshop, HSCC 2004, Philadelphia, PA, USA, March 25-27, 2004. Proceedings*, chapter Safety Verification of Hybrid Systems Using Barrier Certificates, pages 477–492. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004. ISBN 978-3-540-24743-2. doi: 10.1007/978-3-540-24743-2_32. URL http://dx.doi.org/10.1007/978-3-540-24743-2_32.

[45] L. Praly, R. Ortega, and G. Kaliora. Stabilization of nonlinear systems via forwarding mod LgV. *IEEE Transactions on Automatic Control*, 46(9):1461–1466, Sep 2001. ISSN 0018-9286. doi: 10.1109/9.948478.

[46] C. Prieur and L. Praly. Uniting local and global controllers. In *Decision and Control, 1999. Proceedings of the 38th IEEE Conference on*, volume 2, pages 1214–1219 vol.2, 1999. doi: 10.1109/CDC.1999.830096.

[47] Christophe Prieur. Uniting local and global controllers with robustness to vanishing noise. *Mathematics of Control, Signals and Systems*, 14(2):143–172, 2001. ISSN 1435-568X. doi: 10.1007/PL00009880. URL http://dx.doi.org/10.1007/PL00009880.

[48] James A. Primbs, Vesna Nevisti, and John C. Doyle. Nonlinear optimal control: A control lyapunov function and receding horizon perspective. *Asian Journal of Control*, 1(1):14–24, 1999. ISSN 1934-6093. doi: 10.1111/j.1934-6093.1999.tb00002.x. URL http://dx.doi.org/10.1111/j.1934-6093.1999.tb00002.x.

[49] M. Z. Romdlony and B. Jayawardhana. Uniting control lyapunov and control barrier functions. In *53rd IEEE Conference on Decision and Control*, pages 2293–2298, Dec 2014. doi: 10.1109/CDC.2014.7039737.

[50] M. Z. Romdlony and B. Jayawardhana. On the new notion of input-to-state safety. In *2016 IEEE 55th Conference on Decision and Control (CDC)*, pages 6403–6409, Dec 2016. doi: 10.1109/CDC.2016.7799254.

[51] M. Z. Romdlony and B. Jayawardhana. On the sufficient conditions for input-to-state safety. In *2017 13th IEEE International Conference on Control Automation (ICCA)*, pages 170–173, July 2017. doi: 10.1109/ICCA.2017.8003054.

[52] Muhammad Zakiyullah Romdlony and Bayu Jayawardhana. Passivity-based control with guaranteed safety via interconnection and damping assignment.

IFAC-PapersOnLine, 48(27):74 – 79, 2015. ISSN 2405-8963. doi: http://dx.doi.org/10.1016/j.ifacol.2015.11.155. URL http://www.sciencedirect.com/science/article/pii/S2405896315024131. Analysis and Design of Hybrid Systems ADHSAtlanta, GA, USA, Oct. 14-16, 2015.

[53] Muhammad Zakiyullah Romdlony and Bayu Jayawardhana. Stabilization with guaranteed safety using control lyapunovbarrier function. *Automatica*, 66:39 – 47, 2016. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2015.12.011. URL http://www.sciencedirect.com/science/article/pii/S0005109815005439.

[54] Muhammad Zakiyullah Romdlony and Bayu Jayawardhana. Robustness analysis of systems' safety through a new notion of input-to-state safety. *CoRR*, abs/1702.01794, 2017. URL http://arxiv.org/abs/1702.01794.

[55] Arjan van der Schaft. *L2-Gain and Passivity in Nonlinear Control*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2nd edition, 1999. ISBN 1852330732.

[56] E. Sontag. Notions of integral input-to-state stability. In *Proceedings of the 1998 American Control Conference. ACC (IEEE Cat. No.98CH36207)*, volume 5, pages 3210–3214 vol.5, Jun 1998. doi: 10.1109/ACC.1998.688455.

[57] E. D. Sontag and Yuan Wang. New characterizations of input-to-state stability. *IEEE Transactions on Automatic Control*, 41(9):1283–1294, Sep 1996. ISSN 0018-9286. doi: 10.1109/9.536498.

[58] Eduardo D. Sontag. A universal construction of artstein's theorem on nonlinear stabilization. *Syst. Control Lett.*, 13(2):117–123, July 1989. ISSN 0167-6911. doi: 10.1016/0167-6911(89)90028-5. URL http://dx.doi.org/10.1016/0167-6911(89)90028-5.

[59] Duan M. Stipanovi, Peter F. Hokayem, Mark W. Spong, and Dragoslav D. iljak. Cooperative avoidance control for multiagent systems. *J. Dyn. Sys., Meas., Control.*, pages 699–707, 2007. doi: 10.1115/1.2764510.

[60] Keng Peng Tee, Shuzhi Sam Ge, and Eng Hock Tay. Barrier lyapunov functions for the control of output-constrained nonlinear systems. *Automatica*, 45 (4):918 – 927, 2009. ISSN 0005-1098. doi: http://dx.doi.org/10.1016/j.automatica.2008.11.017. URL http://www.sciencedirect.com/science/article/pii/S0005109808005608.

[61] Peter Wieland and Frank Allgower. Constructive safety using control barrier functions. *IFAC Proceedings Volumes*, 40(12):462 – 467, 2007. ISSN 1474-6670. doi: http://dx.doi.org/10.3182/20070822-3-ZA-2920.

00076. URL http://www.sciencedirect.com/science/article/pii/S1474667016355690. 7th IFAC Symposium on Nonlinear Control Systems.

[62] R. Wisniewski and C. Sloth. Converse barrier certificate theorem. In *52nd IEEE Conference on Decision and Control*, pages 4713–4718, Dec 2013. doi: 10.1109/CDC.2013.6760627.

[63] J. Wolff and M. Buss. Invariance control design for constrained nonlinear systems. *IFAC Proceedings Volumes*, 38(1):37 – 42, 2005. ISSN 1474-6670. doi: http://dx.doi.org/10.3182/20050703-6-CZ-1902.00660. URL http://www.sciencedirect.com/science/article/pii/S1474667016366721. 16th IFAC World Congress.

[64] Xiangru Xu, Paulo Tabuada, Jessy W. Grizzle, and Aaron D. Ames. Robustness of control barrier functions for safety critical control**this work is partially supported by the national science foundation grants 1239055, 1239037 and 1239085. *IFAC-PapersOnLine*, 48(27):54 – 61, 2015. ISSN 2405-8963. doi: http://dx.doi.org/10.1016/j.ifacol.2015.11.152. URL http://www.sciencedirect.com/science/article/pii/S2405896315024106. Analysis and Design of Hybrid Systems ADHS.

Summary

This thesis discusses the incorporation of safety into control design. In this control problem, safety refers to a behaviour of the closed-loop system where its state trajectories starting from an admissible set of initial states avoid a set of unsafe states. Such problem of achieving stability and safety simultaneously for the closed-loop system is termed as the ”stabilization with guaranteed safety” problem. This thesis also discusses how to measure the robustness of safety of the closed-loop system in the presence of external disturbances.

We propose various control design strategies that solve the stabilization with guaranteed safety problem for nonlinear systems. Firstly, a novel method of merging the classical Control Lyapunov Function (CLF) with the Control Barrier Function (CLBF) is introduced. The merged function is termed Control Lyapunov Barrier Function (CLBF). We also handle the case where there are multiple unsafe sets in the state by involving several CBFs with a single CLF.

Secondly, energy-based control design via interconnection and damping assignment passivity-based control (IDA-PBC) is shown to be applicable for solving the problem of stabilization with guaranteed safety. We can achieve local stabilization with guaranteed safety by using IDA-PBC, while for a global result, we combine IDA-PBC with another feedback control using an hybrid control method.

We also propose a novel robustness analysis tool that can be used to quantify the margin of safety (or the fragility) of the closed-loop system. As a complement to the well-known input-to-state stability (ISS) notion for analyzing systems' stability robustness, we introduce an input-to-state safety (ISSf) notion which can be used for the robustness analysis of systems' safety in the presence of external disturbance signals.

Samenvatting

In dit proefschrift wordt het aspect van veiligheid opgenomen in het ontwerp van besturingsmechanismen. Veiligheid refereert hierbij naar het gedrag van het gesloten lus systeem waarbij het tijdspad van de toestandsvariabelen, welke gestart zijn in een toegestane verzameling van initiële waarden, de verzameling van onveilige toestanden vermijdt. Het probleem van het tegelijkertijd garanderen van stabiliteit en veiligheid van het gesloten lus systeem wordt "stabilisatie met gegarandeerde veiligheid" genoemd. Verder behandelt dit proefschrift ook hoe men de robuustheid van veiligheid van het gesloten systeem kan meten in de aanwezigheid van externe storingssignalen.

We dragen verschillende regelstrategieën voor welke een oplossing bieden voor het "stabilisatie met gegarandeerde veiligheid" probleem in niet-lineaire systemen. Ten eerste, een nieuwe manier wordt geïntroduceerd voor het samenvoegen van de klassieke 'Control Lyapunov Functie' (CLF) met de 'Control Barrier Functie' (CBF). De samengevoegde functie wordt aangeduid als 'Control Lyapunov Barrier Functie' (CLBF). Het scenario van verschillende verzamelingen van onveilige toestanden is ook bekeken. Hierbij worden verschillende CBF functies samengevoegd met een enkele CLF.

Ten tweede, het is aangetoond dat de koppeling en demping toekenning passiviteits besturingsmethode (IDA-PBC), welke een op energie gebaseerde besturingsmechanisme is, gebruikt kan worden voor het oplossen van het "stabilisatie met gegarandeerde veiligheid" probleem. We zijn geslaagd in het bereiken van lokale stabilisatie met gegarandeerde veiligheid door toepassing van de IDA-PBC methode. Voor het bereiken van globale stabilisatie wordt de IDA-PBC methode gecombineerd met een ander terugkoppelingsregeling middels een hybride besturingsmethode.

We stellen ook een nieuwe robuustheidsanalyse methode voor welke gebruikt kan worden voor het kwantificeren van de veiligheidsspeling (of veiligheids fragiliteit) van het gesloten lus systeem. Als aanvulling op de welbekende input-to-state stabiliteitsinterpretatie (ISS) voor de robuustheidsanalyse van de stabiliteit van een

systeem introduceren we de input-to-state veiligheidsinterpretatie (ISSf), welke gebruikt kan worden voor de robuustheidsanalyse van de veiligheid van een systeem wanneer er externe storingssignalen aanwezig zijn.