Small-Gain Theorem for Safety Verification of Interconnected Systems

Ziliang Lyu [a], Xiangru Xu [b], Yiguang Hong [a]

[a] *Department of Control Science and Engineering, Tongji University, Shanghai, China*

[b] *Department of Mechanical Engineering, University of Wisconsin-Madison, Madison, WI, USA*

Abstract

A small-gain theorem in the formulation of barrier function is developed in this work for safety verification of interconnected systems. This result is helpful to verify input-to-state safety (ISSf) for interconnected systems from the safety information encoded in the individual ISSf-barrier functions. Also, it can be used to obtain a safety set in a higher dimensional space from the safety sets in two lower dimensional spaces.

Key words: Input-to-state safety (ISSf); barrier function; interconnected systems; small-gain theorem.

1 Introduction

Safety is crucial in practical control design, which requires any trajectories of a control system initialized in a prescribed safety set to be kept out of unsafe sets. Applications concerned with safety are ubiquitous in our daily life, ranging from cars in the street to aeroplanes in the air. For example, autonomous vehicles are equipped with lane-keeping modules [23]; a robot team is designed to avoid collision between robots [20]; and aircrafts must satisfy the safety requirement during takeoff and landing [3].

For safety-critical systems, rigorous verification of safety is the first step towards other control tasks (e.g., stabilization and regulation). In general, the techniques for safety verification can be classified into two sorts: model checking [5] and deductive verification [11]. Compared with the former one, deductive verification provides a safety certificate by mathematical inferences rather than exhaustively checking all of the possible system behaviors. The barrier function gives a promising deductive approach for safety verification, analogous to Lyapunov functions for stability; e.g., see [1,2,6,9,15,16,19,21,24] for more details. In [15], barrier functions were used to formulate the verification tasks as convex programming problems. A quadratic program framework was proposed in [1] to balance the conflict between control tasks and safety requirements. In [24], a novel barrier function, called the zeroing barrier function, was proposed for establishing safety and analyzing the robustness of safety sets. Later, [9] redefined the notion of input-to-state safety (ISSf) and provided a sufficient condition in the sense of barrier function to check ISSf, which could be regarded as the counterpart of Sontag's input-to-state stability (ISS) [18] for safety verification.

On the other hand, safety verification for high-dimensional systems is difficult. For example, in [12], safety was verified by the computation of the backward reachable set, which requires solving a Hamilton-Jacobi-Isaacs partial differential equation, whose computational burden increases exponentially as the system dimension grows; in [23], safety was ensured by control barrier functions constructed by the sum-of-squares optimization, which is computationally demanding and only applicable for low-dimensional systems in general. To handle this issue, a promising approach is to treat a high-dimensional system as an interconnected system consisting of lower-dimensional subsystems. The small-gain technique is effective for verifying the stability of an interconnected system by analyzing its less complicated subsystems. In the stability analysis, this technique has

⋆ This work was supported Shanghai Municipal Science and Technology Major Project under grant 2021SHZDZX0100, and the National Natural Science Foundation of China under grants 62173250 and 61733018. This paper was not presented at any IFAC meeting. Corresponding author Y. Hong.

Email addresses: ziliang_lyu@outlook.com (Ziliang Lyu), xiangru.xu@wisc.edu (Xiangru Xu), yghong@iss.ac.cn (Yiguang Hong).

been investigated extensively [7, 8, 10, 13, 25]. For example, the Lyapunov-based small-gain theorem developed in [8] has been found useful to establish ISS for interconnected systems, which has also been extended to switched systems [25] and hybrid systems [13] in recent years.

Considering that the barrier function provides a Lyapunov-like verification approach, it is natural to ask a question: does there exist a small-gain condition such that one can establish safety for the interconnected system based on the individual ISSf-barrier functions of its subsystems? This question is not trivial. First, there is no result about the small-gain theorem in the ISSf setting, even though such an approach has been widely used in checking stability or robustness of interconnected systems. Second, the tools of the traditional small-gain theorems for stability analysis [7, 8, 10, 13, 25] cannot be used to verify safety for interconnected systems, because barrier functions do not have the positive definite property enjoyed by Lyapunov functions.

The objective of this paper is to develop a small-gain theorem based on barrier functions for the safety verification of interconnected systems, in order to establish a higher-dimensional safety set from two lower-dimensional safety sets. The main contributions are summarized as follows. First, in order to handle the interconnections, a set of tools are extended from the traditional small-gain theorem for stability by removing the positive definiteness assumption. Then, based on the ISSf-barrier function, a small-gain theorem for safety verification is established. Such a tool enables us to verify safety in a compositional way.

Notations and Terminologies. Throughout this paper, '$\circ$' denotes the composition operator, i.e., $f \circ g(s) = f(g(s))$; 'T' denotes the transpose operator; Id denotes the identity function; $|\cdot|$ denotes the Euclidean norm; $|x|_{\mathcal{S}} = \inf_{s\in\mathcal{S}} |x - s|$ denotes the point-to-set distance from a point x to a set $\mathcal{S}$; $\phi'(r)$ denotes the derivative of the continuously differentiable function ϕ at r; $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ denote the set of real numbers and nonnegative real numbers, respectively. For any measurable function $u : \mathbb{R}_{\geq 0} \to \mathbb{R}^m$, $\|u\| = \sup\{|u(t)|, t \geq 0\}$ denotes the L_∞^m norm of u. A continuous function γ: $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\gamma(0) = 0$ is of class $\mathcal{K}$, if it is strictly increasing. Moreover, a class $\mathcal{K}$ function γ is of class $\mathcal{K}_\infty$ if it is unbounded. A continuous function $\gamma : \mathbb{R} \to \mathbb{R}$ with $\gamma(0) = 0$ is of extended class $\mathcal{K}$ if it is strictly increasing. In particular, an extended class $\mathcal{K}$ function γ is of extended class $\mathcal{K}_\infty$ if it is unbounded. A function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{KL}$ if it is of class $\mathcal{K}$ on the first argument and decreases to zero on the second argument.

2 Preliminaries

Consider the system

$$\dot{x} = f(x, u), \quad x(t_0) = x_0 \tag{1}$$

where $x \in \mathbb{R}^n$ is the state, $u : \mathbb{R}_{\geq 0} \to \mathbb{R}^m$ is the locally essentially bounded input that accounts for uncertainty entering the system, and the vector field $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is locally Lipschitz continuous.

We first review some definitions related to safety.

Definition 1 (Robust Forward Invariance [4, pp. 123]) *A set $\mathcal{S} \subseteq \mathbb{R}^n$ is robustly forward invariant, if for all $x_0 \in \mathcal{S}$ and any locally essentially bounded input u, the solution $x(t)$ of system (1) satisfies $x(t) \in \mathcal{S}$ for all $t \geq t_0$.*

Definition 2 (Input-to-State Safety) *The system (1) is input-to-state safe (ISSf) on the set*

$$\mathcal{S} = \{x \in \mathbb{R}^n : h(x) \geq 0\} \tag{2}$$

with respect to the external input u, if the set

$$\mathcal{S}_{\gamma(\|u\|)} = \{x \in \mathbb{R}^n : h(x) + \gamma(\|u\|) \geq 0\} \tag{3}$$

is robustly forward invariant. Herein, $h : \mathbb{R}^n \to \mathbb{R}$ is a continuous function, and γ is a class $\mathcal{K}_\infty$ function. In particular, we say that system (1) is safe on the set $\mathcal{S}$ if there is no external input (i.e., $u \equiv 0$), in which case $\mathcal{S}_{\gamma(\|u\|)} = \mathcal{S}$.

Definition 2 is different from [9, Def. 3] in that h is only required to be continuous, which enables us to handle the nonsmoothness resulting from the composition of individual barrier functions.

Definition 3 (ISSf-Barrier Function) *A continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$ is said to be an ISSf-barrier function for system (1) if for all $x \in \mathbb{R}^n$ and all $u \in \mathbb{R}^m$,*

$$\nabla h(x) f(x, u) \geq -\alpha(h(x)) - \eta(|u|) \tag{4}$$

where α and η are of extended class $\mathcal{K}_\infty$ and of class $\mathcal{K}_\infty$, respectively.

Remark 1 *The ISSf-barrier function (4) is a global version of [9, Def. 4]. A continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$ is an ISSf-barrier function for system (1) if and only if there exist functions σ and ϕ of class K_∞ such that $|h(x)| \geq \sigma(|x|)$ and*

$$|h(x)| \geq \phi(|u|) \Rightarrow \nabla h(x) f(x, u) \geq -\alpha(h(x)).$$

The sufficiency part follows by considering the two cases $|\alpha(h(x))| \geq \eta(|u|)/c$ and $|\alpha(h(x))| < \eta(|u|)/c$ for any constant $c \in (-1, 1)$. For necessity, we can take

$$\eta(r) = -\alpha(-\phi(r)) - \min\{0, \inf_{|h(x)| \leq \phi(r)} \nabla h(x) f(x, r)\},$$

where $-\alpha(-\phi(r))$ is clearly of class $\mathcal{K}_\infty$. Since ϕ is of extended class $\mathcal{K}_\infty$, the set $\{x : |h(x)| \leq \phi(r)\}$ is compact for fixed $r \geq 0$. By combining this with the local Lipschitzness of h and f, $-\min\{0, \inf_{|h(x)| \leq \phi(r)} \nabla h(x) f(x, r)\}$ is well-defined and non-decreasing on $\mathbb{R}_{\geq 0}$. Thus, η is a class $\mathcal{K}_\infty$ function.

The following lemma provides a sufficient condition for establishing ISSf.

Lemma 1 *Suppose that h is an ISSf-barrier function satisfying (4). Then system (1) is ISSf, namely, the set $\mathcal{S}_{\gamma(\|u\|)}$ defined in (3) is robustly forward invariant with $\gamma(r) := -\alpha^{-1}(-\eta(r))$.*

This lemma can be verified by the arguments used in the proof of [9, Thm. 3].

Remark 2 *Note that the set $\mathcal{S}$ defined in (2) is ISS*[1] *if h is an ISSf-barrier function. To see this, we consider a Lyapunov-like function as in [24]:*

$$V(x) = \begin{cases} 0, & \text{if } x \in \mathcal{S}; \\ -h(x), & \text{if } x \in \mathbb{R}^n \setminus \mathcal{S}. \end{cases}$$

Then it follows from (4) that, for all $x \in \mathbb{R}^n \setminus \mathcal{S}$,

$$\nabla V(x) f(x, u) \leq -\hat{\alpha}(V(x)) + \eta(|u|) \tag{5}$$

where $\hat{\alpha}(r) = -\alpha(-r)$ is of class $\mathcal{K}_\infty$ on $\mathbb{R}_{\geq 0}$. With [17, Thm. 1], the conclusion follows. □

3 Small-Gain Theorem for Safety Verification

Consider the interconnected system

$$\dot{x}_1 = f_1(x_1, x_2, u_1) \tag{6a}$$
$$\dot{x}_2 = f_2(x_1, x_2, u_2) \tag{6b}$$

where, for $i = 1, 2$, x_i takes values in the Euclidean space $\mathbb{R}^{n_i}$, $u_i : \mathbb{R}_{\geq 0} \to \mathbb{R}^{m_i}$ is locally essentially bounded, and $f_i : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \times \mathbb{R}^{m_i} \to \mathbb{R}^{n_i}$ is locally Lipschitz. Let $x = (x_1^{\mathrm{T}}, x_2^{\mathrm{T}})^{\mathrm{T}}$ and $u = (u_1^{\mathrm{T}}, u_2^{\mathrm{T}})^{\mathrm{T}}$.

The small-gain theorem for safety verification of the interconnected system (6) is given as follows.

[1] As introduced in [17], a compact set $\mathcal{S}$ is ISS if there exist functions β of class $\mathcal{KL}$ and γ of class $\mathcal{K}$ such that $|x(t)|_{\mathcal{S}} \leq \beta(|x_0|_{\mathcal{S}}, t - t_0) + \gamma(\|u\|)$ holds for all $t \geq t_0$ and $x \in \mathbb{R}^n$.

Theorem 1 *Consider the interconnected system (6). For $i = 1, 2$, suppose that there exist continuously differentiable function $h_i : \mathbb{R}^{n_i} \to \mathbb{R}$, extended class $\mathcal{K}_\infty$ functions α_i and ψ_i, and class $\mathcal{K}_\infty$ function γ_i such that*

$$\begin{aligned} &\nabla h_1(x_1) f_1(x_1, x_2, u_1) \\ &\qquad \geq -\alpha_1(h_1(x_1)) + \psi_1(h_2(x_2)) - \gamma_1(|u_1|), \end{aligned} \tag{7}$$

$$\begin{aligned} &\nabla h_2(x_2) f_2(x_1, x_2, u_2) \\ &\qquad \geq -\alpha_2(h_2(x_2)) + \psi_2(h_1(x_1)) - \gamma_2(|u_2|). \end{aligned} \tag{8}$$

If the small-gain condition

$$|\phi_1 \circ \phi_2(r)| < |r|, \quad \forall r \in \mathbb{R}, \tag{9}$$

with

$$\phi_i(r) = \alpha_i^{-1} \circ (Id + \varepsilon) \circ \psi_i(r),$$

holds for a suitable $\varepsilon > 0$, then there exists a continuous function

$$h(x) = \min\{\phi(h_1(x_1)), h_2(x_2)\}, \tag{10}$$

where ϕ is an extended class $\mathcal{K}_\infty$ function related to ϕ_1 and ϕ_2, such that the interconnected system (6) is ISSf on the set $\mathcal{S} = \{x \in \mathbb{R}^{n_1+n_2} : h(x) \geq 0\}$, namely, the set

$$\mathcal{S}_{\gamma(\|u\|)} = \{x \in \mathbb{R}^{n_1+n_2} : h(x) + \gamma(\|u\|) \geq 0\} \tag{11}$$

is robustly forward invariant with[2]

$$\begin{aligned} \gamma(r) = &-\phi \circ \alpha_1^{-1}(-(1 + 1/\varepsilon)\gamma_1(r)) \\ &- \alpha_2^{-1}(-(1 + 1/\varepsilon)\gamma_2(r)). \end{aligned} \tag{12}$$

Remark 3 *The function ϕ_i serves as the "ISSf gain" of the x_i-subsystem. The small-gain condition (9) is an extension of [7, Cond. (17)] by removing the positive definiteness assumption. Note that ε is used to handle the external input u. If there is no external input (i.e., $u \equiv 0$), ϕ_i can be chosen as $\phi_i(r) = \alpha_i^{-1} \circ \psi_i(r)$.*

Remark 4 *For the case $u \equiv 0$, with (7) and (8),*

$$\begin{aligned} \dot{h}_i &\geq -\alpha_i(h_i) + \psi_i(h_{3-i}) \\ &\geq -\alpha_i(h_i) + \min\{0, \inf_{t \geq t_0} \psi_i(h_{3-i}(s))\}, \quad i = 1, 2. \end{aligned}$$

Then, according to Lemma 1, the set $\hat{\mathcal{S}}_i = \{x_i : h_i(x_i) + d_i \geq 0\}$ is robustly forward invariant, where $d_i = -\min\{0, \inf_{t \geq t_0} \alpha_i^{-1} \circ \psi_i(h_{3-i}(s))\}$. Note that $\hat{\mathcal{S}}_i$ may be larger than the set $\mathcal{S}_i = \{x_i : h_i(x_i) \geq 0\}$, which is used to encode the hard safety constraints that

[2] Note that γ is of class $\mathcal{K}_\infty$ since $\hat{\alpha}_1(r) = -\phi \circ \alpha_1^{-1}(-(1 + 1/\varepsilon)r)$ and $\hat{\alpha}_2(r) = -\alpha_2^{-1}(-(1 + 1/\varepsilon)r)$ are non-negative, continuous, strictly increasing and unbounded on $\mathbb{R}_{\geq 0}$.

should be met. To handle this issue, it needs to impose the small-gain condition (9) on the ISSf gains ϕ_1 and ϕ_2. Then, according to Theorem 1, $x_i(t)$ cannot leave $\mathcal{S}_i$ for all $t \geq t_0$, if $x_1(t_0) \in \mathcal{S}_1$ and $x_2(t_0) \in \mathcal{S}_2$.

Remark 5 *Note that (7) and (8) are different from (4) in that ψ_i is of extended class $\mathcal{K}_\infty$. This modification is necessary, because the interconnection $\psi_i(h_{3-i})$ is helpful to keep safety for the x_i-system if $h_{3-i}(x_{3-i}(t)) > 0$ for all $t \geq t_0$. Such a feature will be used to establish some useful conclusions in the proof of Theorem 1, as detailed in (16) and (22).*

As indicated in (7) and (8), both individual ISSf-barrier functions are coupled with interconnections. It is worth noting that the function ϕ in (10) is helpful to handle these interconnections. However, such a function cannot be constructed by the tools of the traditional small-gain theorems for stability analysis [7,13,25], because barrier functions are not of the positive definiteness enjoyed by Lyapunov functions. To handle this issue, an approach to the construction of ϕ is given below, by extending the tool for ISS on the positive domain in [7, Appendix] to the whole domain.

Lemma 2 *Let $\rho_0 : \mathbb{R} \to \mathbb{R}$ be a continuous function with $\rho_0(0) = 0$, $\rho_0(r) < 0$ for all $r < 0$, and $\rho_0(r) > 0$ for all $r > 0$. Then there exists a continuous function $\rho : \mathbb{R} \to \mathbb{R}$ such that*

- *$\rho_0(r) < \rho(r) < 0$ for all $r < 0$, and $0 < \rho(r) < \rho_0(r)$ for all $r > 0$;*
- *ρ is continuously differentiable on $\mathbb{R}$, and $\rho'(r) < \frac{1}{2}$ for all $r \in \mathbb{R}$.*

Proof. See Appendix A. □

Lemma 3 *Let ϕ_i be of extended class $\mathcal{K}_\infty$ and satisfy (9). Then there exists an extended class $\mathcal{K}_\infty$ function ϕ such that*

- *$\phi_1^{-1}(r) < \phi(r) < \phi_2(r)$ for all $r < 0$, and $\phi_2(r) < \phi(r) < \phi_1^{-1}(r)$ for all $r > 0$;*
- *$\phi(r)$ is continuously differentiable on $\mathbb{R}\backslash\{0\}$, and $\phi'(r) > 0$ for all $r \in \mathbb{R}\backslash\{0\}$.*

Proof. See Appendix B. □

Then it is time to prove Theorem 1.

Proof of Theorem 1. By applying Lemma 3 to the small-gain condition (9), the function ϕ in (10) can be selected as follows

$$\phi_1^{-1}(r) < \phi(r) < \phi_2(r), \ \ \forall r < 0; \tag{13a}$$
$$\phi_2(r) < \phi(r) < \phi_1^{-1}(r), \ \ \forall r > 0. \tag{13b}$$

According to (10), the proof is equivalent to verifying that both of the sets

$$\mathcal{C}_1 = \{x_1 \in \mathbb{R}^{n_1} : \phi(h_1(x_1)) + \gamma(\|u\|) \geq 0\},$$
$$\mathcal{C}_2 = \{x_2 \in \mathbb{R}^{n_2} : h_2(x_2) + \gamma(\|u\|) \geq 0\}$$

are robustly forward invariant. In the following, we show this by contradiction.

Suppose that at least one of the sets $\mathcal{C}_1$ and $\mathcal{C}_2$ is not robustly forward invariant. Denote the first time instant when $x_i(t)$ leaves the set $\mathcal{C}_i$ by τ_i, namely, for any real number $\delta > 0$,

$$\tau_1 := \inf\{t \geq t_0 : \phi(h_1(x_1(t))) \leq -\gamma(\|u\|) - \delta\}, \tag{14a}$$
$$\tau_2 := \inf\{t \geq t_0 : h_2(x_2(t)) \leq -\gamma(\|u\|) - \delta\}. \tag{14b}$$

Note that τ_i will be infinite if $\mathcal{C}_i$ is forward invariant. Without loss of generality, we assume that τ_i is finite. Then we have the following three cases.

Case 1: $\tau_1 < \tau_2$. In this case, we have

$$\phi(h_1(x_1(\tau_1))) = -\gamma(\|u\|) - \delta < h_2(x_2(\tau_1)). \tag{15}$$

As ϕ is continuous but not necessarily differentiable at zero, we first consider the situation when $\|u\| = 0$. According to (15), $h_1(x_1(\tau_1)) = \phi^{-1}(-\delta) < 0$. Besides, as δ is an arbitrary real number larger than zero, we have $h_2(x_2(\tau_1)) \geq 0$. Thus, according to (7),

$$\begin{aligned}\nabla h_1(x_1(\tau_1)) & f_1(x_1(\tau_1), x_2(\tau_1), u_1(\tau_1)) \\ & \geq -\alpha_1(h_1(x_1(\tau_1))) + \psi_1(h_2(x_2(\tau_1))) > 0\end{aligned} \tag{16}$$

which implies that there exists a t in (t_0, τ_1) such that $h_1(x_1(t)) \leq h_1(x_1(\tau_1))$, and thus, $\phi(h_1(x_1(t))) \leq \phi(h_1(x_1(\tau_1)))$ since ϕ is of extended class $\mathcal{K}_\infty$. This contradicts the minimality of τ_1.

Next, we consider the situation when $\|u\| \neq 0$. By combining (12) and (15), we have

$$\phi(h_1(x_1(\tau_1))) < -\gamma(\|u\|) \leq \phi \circ \alpha_1^{-1}(-(1 + 1/\varepsilon)\gamma_1(|u_1(\tau_1)|)),$$

and thus,

$$\frac{\varepsilon}{1+\varepsilon}\alpha_1(h_1(x_1(\tau_1))) < -\gamma_1(|u_1(\tau_1)|). \tag{17}$$

Besides, as $h_1(x_1(\tau_1)) < 0$, it follows from (13a) and (15) that

$$\phi_1^{-1}(h_1(x_1(\tau_1))) < \phi(h_1(x_1(\tau_1))) < h_2(x_2(\tau_1)),$$

which implies

$$\frac{1}{1+\varepsilon}\alpha_1(h_1(x_1(\tau_1))) < \psi_1(h_2(x_2(\tau_1))). \tag{18}$$

By combining (7), (17), (18) and the fact that $\phi'(h_1(x_1(\tau_1))) > 0$, we have

$$\phi'(h_1(x_1(\tau_1)))\nabla h_1(x_1(\tau_1))f_1(x_1(\tau_1), x_2(\tau_1), u_1(\tau_1)) > 0.$$

Thus, there exists some t in (t_0, τ_1) such that $\phi(h_1(x_1(t))) \leq \phi(h_1(x_1(\tau_1)))$, contradicting the minimality of τ_1.

Case 2: $\tau_1 > \tau_2$. In this case,

$$h_2(x_2(\tau_2)) = -\gamma(\|u\|) - \delta < \phi(h_1(x_1(\tau_2))), \quad (19)$$

and thus, similar to the derivation of (17), we have

$$\frac{\varepsilon}{1+\varepsilon}\alpha_2(h_2(x_2(\tau_2))) < -\gamma_2(|u_2(\tau_2)|). \quad (20)$$

Thus, by applying (20) to (8),

$$\begin{aligned}&\nabla h_2(x_2(\tau_2))f_2(x_2(\tau_2), x_2(\tau_2), u_1(\tau_2)) \\ &\quad > -\frac{1}{1+\varepsilon}\alpha_2(h_2(x_2(\tau_2))) + \psi_2(h_1(x_1(\tau_2))).\end{aligned} \quad (21)$$

If $h_1(x_1(\tau_2)) \geq 0$, then

$$\nabla h_2(x_2(\tau_2))f_2(x_2(\tau_2), x_2(\tau_2), u_1(\tau_2)) > 0, \quad (22)$$

which implies that there is a t in (t_0, τ_2) such that $h_2(x_2(t)) \leq h_2(x_2(\tau_2))$, contradicting the minimality of τ_2. We then consider $h_1(x_1(\tau_2)) < 0$. According to (13a),

$$h_2(x_2(\tau_2)) < \phi(h_1(x_1(\tau_2))) < \phi_2(h_1(x_1(\tau_2))),$$

and thus,

$$\frac{1}{1+\varepsilon}\alpha_2(h_2(x_2(\tau_2))) < \psi_2(h_1(x_1(\tau_2))). \quad (23)$$

By substituting this into (21), it can be verified that the minimality of τ_2 is also violated.

Case 3: $\tau_1 = \tau_2$. For notational convenience, we take $\tau = \tau_1 = \tau_2$. Similar to the derivation of (17), we have

$$\frac{\varepsilon}{1+\varepsilon}\alpha_i(h_i(x_i(\tau)) < -\gamma_i(|u_i(\tau)|), \quad i = 1, 2. \quad (24)$$

Then, according to (13a) and $\phi(h_1(x_1(\tau))) = h_2(x_2(\tau))$, we have

$$\phi_1^{-1}(h_1(x_1(\tau))) < h_2(x_2(\tau)) < \phi_2(h_1(x_1(\tau))),$$

and thus, for $i = 1, 2$,

$$\frac{1}{1+\varepsilon}\alpha_i(h_i(x_i(\tau))) < \psi_i(h_{3-i}(x_{3-i}(\tau))). \quad (25)$$

By combining (7), (8), (24) and (25), we have

$$\begin{aligned}&\phi'(h_1(x_1(\tau)))\nabla h_1(x_1(\tau))f_1(x_1(\tau), x_2(\tau), u_1(\tau)) > 0, \\ &\nabla h_2(x_2(\tau))f_2(x_1(\tau), x_2(\tau), u_2(\tau)) > 0,\end{aligned}$$

contradicting to the minimality of τ.

By summarizing the three cases above, the assumption that at least one of the sets $\mathcal{C}_1$ and $\mathcal{C}_2$ is not robustly forward invariant does not hold, and thus, the proof is completed. □

The following example demonstrates how to apply Theorem 1 in the output-constrained control of second-order systems.

Example 1. Consider the system

$$\begin{aligned}\dot{x}_1 &= f_1(x_1, x_2), \\ \dot{x}_2 &= f_2(x_1, x_2) + u\end{aligned} \quad (26)$$

where $f_1(x_1, x_2) = -x_1^3/2 + x_2$ and $f_2(x_1, x_2) = x_1^3 + x_2$. The system output is $y = x_1$. The objective of this example is to design a controller such that the system output $y(t)$ does not violate the hard constraint $y(t) \geq 0$ for all $y(t_0) \geq 0$ and all $t \geq t_0$. Take $h_1 = x_1$. Obviously, the barrier condition (7) is satisfied with $\alpha_1(r) = r^3/2$ and $\psi_1(r) = r$. Let $h_2 = x_2$ and $u = -x_2 - \alpha_2(x_2)$, where $\alpha_2(r)$ is used to assign the ISSf gain ϕ_2. Clearly, the barrier condition (8) is also satisfied with $\psi_2(r) = r^3$. Let $\alpha_2(r) = cr$ with $c > 0$, and one can select a sufficient large c to guarantee that the small-gain condition (9) is satisfied, where $\phi_1(r) = \sqrt[3]{2r}$ and $\phi_2(r) = r^3/c$. Thus, there exists an extended class $\mathcal{K}_\infty$ function ϕ satisfying (13). According to Theorem 1, $h(x(t)) = \min\{\phi(h_1(x_1(t))), h_2(x_2(t))\} \geq 0$ for all $t \geq t_0$, if $h_1(x_1(t_0)) \geq 0$ and $h_2(x_2(t_0)) \geq 0$, and thus, $y(t) = x_1(t) \geq 0$ for all $t \geq t_0$ by noting that ϕ is of extended class $\mathcal{K}_\infty$.

Remark 6 *As can be seen in Example 1, the ISSf gain ϕ_2 can be assigned by tuning the function α_2, which is explicitly involved in the controller u. Thus, the control engineers should assign the ISSf gain carefully so as to meet the small-gain condition (9). Such an approach differs from [14, 22] in that it does not require the barrier functions to be of the exponential form.*

4 Conclusion

We have developed a small-gain theorem based on ISSf-barrier functions for safety verification. It has been shown that an interconnected system with two ISSf subsystems is again ISSf if the absolute value of the composition of ISSf gains of two subsystems is smaller than that of the identity function. The proposed result has provided a relationship between the whole system and its subsystems in the safety sense, though how to effectively apply it to practical control design still needs to be explored in the future.

References

[1] Ames, A. D., Grizzle, J. W., & Tabuada, P. (2014). Control barrier function based quadratic programs with application to adaptive cruise control. In *IEEE conference on decision and control* (pp. 6271–6278).

[2] Ames, A. D., Xu, X., Grizzle, J. W., & Tabuada, P. (2017). Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8), 3861–3876.

[3] Balachandran, S., Ozay, N., & Atkins, E, M. (2016). Verification guided refinement of flight safety assessment and management system for takeoff. *Journal of Aerospace Information Systems*, 13(9), 357–369.

[4] Blanchini, F., & Miani, S. (2015). *Set-theoretic methods in control.* (2nd ed.). Springer.

[5] Clarke, E.M., Grumberg, O., Kroening, D., Peled, D., & Veith, H. (2018). *Model Checking.* MIT Press.

[6] Coogan, S., & Arcak, M. (2014). A dissipativity approach to safety verification for interconnected systems. *IEEE Transactions on Automatic Control*, 60(6), 1722–1727.

[7] Jiang, Z. P., Mareels, I. M. Y, & Wang, Y. (1996). A Lyapunov formulation of the nonlinear small-gain theorem for interconnected ISS systems. *Automatica*, 32(8), 1211–1215.

[8] Jiang, Z. P., Teel, A. R., & Praly, L. (1994). Small-gain theorem for ISS systems and applications. *Mathematics of Control, Signals and Systems*, 7(2), 95–120.

[9] Kolathaya, S., & Ames, A. D. (2018). Input-to-state safety with control barrier functions. *IEEE Control Systems Letters*, 3(1), 108–113.

[10] Long, L., & Zhao, J. (2013). A small-gain theorem for switched interconnected nonlinear systems and its applications. *IEEE Transactions on Automatic Control*, 59(4), 1082–1088.

[11] Manna, Z., & Pnueli A. (2012). *Temporal verification of reactive systems: safety.* Springer Science & Business Media.

[12] Mitchell, I. M., Bayen, A. M., & Tomlin, C. J. (2005). A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50(7), 947–957.

[13] Nesic, D., & Teel, A. R. (2008). A Lyapunov-based small-gain theorem for hybrid ISS systems. In *IEEE conference on decision and control* (pp. 3380–3385).

[14] Nguyen, Q., & Sreenath, K. (2016). Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In *American control conference* (pp. 322–328).

[15] Prajna, S., Jadbabaie, A., & Pappas, G. J. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8), 1415–1428.

[16] Romdlony, M. Z., & Jayawardhana, B. (2016). On the new notion of input-to-state safety. In *IEEE conference on decision and control* (pp. 6403–6409).

[17] Sontag, E. D., & Wang, Y. (1995). On characterizations of input-to-state stability with respect to compact sets. In *proceedings of IFAC non-linear control systems design symposium* (pp. 203–208).

[18] Sontag, E. D., & Wang, Y. (1995). On characterizations of the input-to-state stability property. *Systems and Control Letters*, 24(5), 351–360.

[19] Tee, K. P., Ge S. S., & Tay, E. H. (2009). Barrier Lyapunov functions for the control of output-constrained nonlinear systems. *Automatica*, 45(4), 918–927.

[20] Wang, L., Ames, A. D., & Egerstedt, M. (2017). Safety barrier certificates for collisions-free multirobot systems. *IEEE Transactions on Robotics*, 33(3), 661–674.

[21] Wieland, P., & Allgöwer, F. (2007). Constructive safety using control barrier functions. *IFAC Proceedings Volumes*, 40(12), 462–467.

[22] Xu, X. (2018). Constrained control of input–output linearizable systems using control sharing barrier functions. *Automatica*, 87, 195–201.

[23] Xu, X., Grizzle, J. W., Tabuada, P., & Ames, A. D. (2017). Correctness guarantees for the composition of lane keeping and adaptive cruise control. *IEEE Transactions on Automation Science and Engineering*, 15(3), 1216–1229.

[24] Xu, X., Tabuada, P., Grizzle, J. W., & Ames, A. D. (2015). Robustness of control barrier functions for safety critical control. *IFAC-PapersOnLine*, 48(27), 54–61.

[25] Yang, G., & Liberzon, D. (2015). A Lyapunov-based small-gain theorem for interconnected switched systems. *Systems & Control Letters*, 78, 47–54.

A Proof of Lemma 2

Suppose $-\frac{1}{2} \leq \rho_0(r) < 0$ for all $r < 0$ and $0 < \rho_0(r) \leq \frac{1}{2}$ for all $r > 0$. Otherwise, we take

$$\hat{\rho}(r) = \begin{cases} \max\{-\frac{1}{2}, \rho_0(r)\}, & \text{if } r < 0 \\ 0, & \text{if } r = 0 \\ \min\{\frac{1}{2}, \rho_0(r)\}, & \text{if } r > 0 \end{cases}$$

to replace $\rho_0(r)$. Let $\rho_1(0) = 0$ and

$$\rho_1(r) = \begin{cases} \rho_1^-(r), & \text{if } r < 0 \\ \rho_1^+(r), & \text{if } r > 0 \end{cases} \tag{A.1}$$

with

$$\rho_1^-(r) = \begin{cases} \max_{s\in[-2,r]} \rho_0(s) & \text{if } -1 \leq r < 0; \\ \max_{s\in[r-1,-1]} \rho_0(s) & \text{if } r < -1; \end{cases}$$

$$\rho_1^+(r) = \begin{cases} \min_{s\in[r,2]} \rho_0(s) & \text{if } 0 < r \leq 1; \\ \min_{s\in[1,r+1]} \rho_0(s) & \text{if } r > 1. \end{cases}$$

Since $\rho_0(r) < 0$ for $r \in [-2, 0)$,

$$\lim_{r\to 0^-} \rho_1(r) = \max_{s\in[-2,0]} \rho_0(s) = 0;$$

and analogously,

$$\lim_{r\to 0^+} \rho_1(r) = \min_{s\in[r,2]} \rho_0(s) = 0.$$

Therefore, ρ_1 is continuous at zero. Moreover, because ρ_1 is continuous at $r = -1$ and at $r = 1$, ρ_1 is continuous on $\mathbb{R}$.

To get a desired function ρ satisfying the condition given in Lemma 2, we take

$$\rho(r) = \begin{cases} \int_r^{r+1} \rho_1(s)\mathrm{d}s, & \text{if } r < -1; \\ \int_r^0 \rho_1(s)\mathrm{d}s, & \text{if } -1 \le r < 0; \\ \int_0^r \rho_1(s)\mathrm{d}s, & \text{if } 0 \le r \le 1; \\ \int_{r-1}^r \rho_1(s)\mathrm{d}s & \text{if } r > 1. \end{cases} \tag{A.2}$$

With the help of the proof of [7, Lemma A.2], we obtain that ρ meets the first requirement of Lemma 2. Furthermore, since ρ_1 is a continuous function, ρ is continuously differentiable on $\mathbb{R}$. Note that $\rho_0(r) \le \rho_1(r) < 0$ for $r < 0$, and $0 < \rho_1(r) \le \rho_0(r)$ for $r > 0$. As a result, it is easy to see that $\rho'(r) \le |\rho_1(r)| \le \frac{1}{2}$ for all $r \in \mathbb{R}$. The second requirement given in Lemma 2 is met.

B Proof of Lemma 3

Define

$$\rho_0(r) = \frac{1}{2}[r - \phi_1 \circ \phi_2(r)]. \tag{B.1}$$

According to (9),

$$\begin{aligned} &\phi_1 \circ \phi_2(r) > r - \rho_0(r), \quad \text{if } r < 0, \\ &\phi_1 \circ \phi_2(r) < r - \rho_0(r), \quad \text{if } r > 0; \end{aligned}$$

and hence,

$$\begin{aligned} &\phi_2(r) > \phi_1^{-1}(r - \rho_0(r)), \quad \forall r < 0, \\ &\phi_2(r) < \phi_1^{-1}(r - \rho_0(r)), \quad \forall r > 0. \end{aligned}$$

By Lemma 2, there exists a continuously differentiable function $\rho : \mathbb{R} \to \mathbb{R}$ with $\rho'(r) \le \frac{1}{2}$ such that $\rho_0(r) < \rho(r) < 0$ for each $r < 0$, and $0 < \rho(r) < \rho_0(r)$ for each $r > 0$. Without loss of generality, we assume $|\rho(r)| < |r|$. Let $\phi(0) = 0$ and

$$\phi(r) = \frac{1}{\rho(r)} \int_{r-\rho(r)}^{r} \phi_1^{-1}(s)\mathrm{d}s, \quad \forall r \ne 0, \tag{B.2}$$

which yields $\phi_1^{-1}(r) < \phi(r) < \phi_1^{-1}(r - \rho(r)) < \phi_2(r)$ for all $r < 0$, and $\phi_2(r) < \phi_1^{-1}(r - \rho(r)) < \phi(r) < \phi_1^{-1}(r)$ for all $r > 0$. Because $\phi_1^{-1}(0) = 0$ and ϕ_1^{-1} is continuous on $\mathbb{R}$, $\lim_{r\to 0^+} \phi(r) = \lim_{r\to 0^-} \phi(r) = 0$, which further implies that $\phi(r)$ is continuous at zero, and consequently, $\phi(r)$ is continuous on $\mathbb{R}$ as well. Since ρ is continuously differentiable on $\mathbb{R}$, ϕ is continuously differentiable on $\mathbb{R}\backslash\{0\}$. Moreover, with the proof of [7, Lemma A.1], $\phi'(r) > 0$ for all $r \in \mathbb{R}\backslash\{0\}$.