A contract negotiation scheme for safety verification of interconnected systems

Xiao Tan, Antonis Papachristodoulou, and Dimos V. Dimarogonas

Abstract— **This paper proposes a (control) barrier function synthesis and safety verification scheme for interconnected nonlinear systems based on assume-guarantee contracts (AGC) and sum-of-squares (SOS) techniques. It is well-known that the SOS approach does not scale well for barrier function synthesis for high-dimensional systems. In this paper, we show that compositional methods like AGC can mitigate this problem. We formulate the synthesis problem into a set of small-size problems, which constructs local contracts for subsystems, and propose a negotiation scheme among the subsystems at the contract level. The proposed scheme is then implemented numerically on two examples: vehicle platooning and room temperature regulation.**

I. Introduction

In many engineering applications, system states need to be confined to a specific set of safe states. Designing active control to achieve this property and verifying a given closed-loop system regarding this property are known as safety synthesis and verification problems. Many safety-ensuring control approaches have been proposed in the literature, including reachability analysis [1], control barrier functions (CBF) [2], model predictive control [3], prescribed performance control [4] among many others. In particular, when a CBF is shown to exist, safety-ensuring feedback can be constructed, and the safety of the system is certified [5]. Thus, there has been lots of interest in synthesizing valid control barrier functions numerically, by, for example, sum-of-square approaches [6], [7], learning-based approaches [8], [9], and Hamiltonian-Jacobi reachability analysis [10]. However, most of these approaches are limited to dynamical systems of small to moderate size, and will become computationally intractable for large-scale systems.

Many complex, large-scale systems naturally impose an interconnected structure. It is thus essential to exploit this structure to deal with the numerical scalability issue. Along this line of research, the idea of compositional reasoning has been leveraged so that one could establish properties of the interconnected system by reasoning properties on its components. As for system safety/invariance property, [11], [12] propose to synthesize local barrier functions, establish local input-to-state safety properties, and compose the local properties by checking a small-gain-like condition. However, it remains unclear how to adapt local safety properties if the condition fails. On the other hand, [13] certifies the safety property by seeking a Lyapunov function of the interconnected system. Safety is thus certified if a subset of the constructed Lyapunov function has no intersection with the unsafe region. It is worth noting that the search for a Lyapunov function is solved as a centralized semi-definite problem, and is still computationally demanding when the size of the interconnected system becomes larger.

In the literature of formal methods and model checking [14], the composition of system properties is usually approached through the notion of an assume-guarantee contract [15]. In plain words, a contract describes the behavior that a system will exhibit (guarantees) subject to the influence of the environment (assumptions). Originally, the main application domain of a contract in model checking was for discrete space systems. When contracts are applied to certify the safety of complex continuous space systems, circular reasoning of implications might exist. This is not a trivial problem in general, and the AGC framework is always sound only if a hierarchical structure exists [16]. [17] introduces parameterized AGCs, laying the foundation for finding local AGCs that can be composed of. [18] deals with invariance properties of discrete-time linear systems. The authors show that the composition of all local AGCs can be formulated as a linear program when using zonotopic representation to parameterize the constraint set and input set. In [19], the authors consider a finite transition system and propose to determine how safe a state is by applying value iterations. The contracts are iterated locally, yet no completeness guarantee can be asserted.

Recently, there are a few works that apply AGCs to control synthesis problems for continuous-time systems. [20] utilizes behaviour AGC for control design for linear systems, and [21] applies AGCs to design local feedback law under signal temporal logic specifications.

In this work, we provide a tractable safety verification scheme for continuous-time interconnected nonlinear systems, leveraging sum-of-square techniques and assume-guarantee contracts. Our result is built upon [16] on the invariance AGCs for continuous-time systems that circumvent circular reasoning under mild assumptions. Our proposed approach consists of the construction of local AGCs and the search for compatible AGCs. In contrast to [13], [18], we propose to negotiate local contracts only with its neighbors, and thus no central optimization is needed. Once a set of compatible AGCs is returned, the safety of the interconnected system is certified. Moreover, we show that the proposed

This work was supported in part by Swedish Research Council (VR), in part by Horizon Europe SymAware, in part by ERC CoG LEAFHOUND, in part by EU CANOPIES Project, and in part by Knut and Alice Wallenberg Foundation (KAW). Xiao Tan and Dimos V. Dimarogonas are with the School of EECS, Royal Institute of Technology (KTH), 100 44 Stockholm, Sweden. Antonis Papachristodoulou is with the Department of Engineering Science, University of Oxford, Oxford, United Kingdom. Email: {xiaotan, dimos}@kth.se, antonis@eng.ox.ac.uk.

algorithms will terminate in finite steps and find a solution whenever one exists under relevant technical assumptions in the case of acyclic interconnections or for homogeneous systems.

II. Notation and Preliminaries

Notation: $\mathbb{R}^n$ denotes the n-dimensional vector space. A vector $a = (a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ is a column vector unless stated otherwise. For $Z \subseteq \mathbb{R}^n$, we denote by $M(Z)$ the set of continuous-time maps $z : E \to Z$, where $E \in \{[0,a], a \geq 0\} \cup \{[0,a), a > 0\} \cup \{\mathbb{R}_+\}$ is a time interval. Given sets $X_i \subseteq \mathbb{R}^{n_i}$, $i \in \mathcal{I} = \{1, 2, \dots, N\}$, the Cartesian product $X_1 \times X_2 \times \cdots \times X_N$ is denoted by $\Pi_{i\in\mathcal{I}} X_i$. Let $x \in \mathbb{R}^n$ be an independent variable. Denote by $\mathcal{R}[x]$ the set of polynomials in the variable x. We call a polynomial $p \in \mathcal{R}[x]$ sum-of-squares if there exist polynomials $g_1, g_2, \dots, g_N$ in the variable x such that $p = \sum_{i=1}^N g_i^2$. Denote by $\Sigma[x]$ the set of sum-of-squares polynomials in x. Let $\mathcal{R}[x_1, x_2, \dots, x_n], \Sigma[x_1, x_2, \dots, x_n]$ denote the sets of polynomials and SOS polynomials of independent variables $x_1, x_2, \dots, x_n$, respectively. Consider a directed graph $(\mathcal{I}, \mathcal{E}), \mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$. Denote by $N(i) = \{j \in \mathcal{I} : (j,i) \in \mathcal{E}\}$ the set of parent nodes of node i, and $\text{Child}(i) = \{k \in \mathcal{I} : (i,k) \in \mathcal{E}\}$ the set of its child nodes. We call node i a root node if $N(i) = \emptyset$; node i is a leaf node if $\text{Child}(i) = \emptyset$.

We first introduce the definitions of continuous-time systems, their interconnections, and assume-guarantee contracts tailored from [16] for the safety verification problem.

A. Systems and Interconnections

In this work, we consider continuous-time systems formally defined as follows.

Definition 1 (Continuous-time system)**.** A continuous-time system G is a tuple

$$G = (U, W, X, Y, X^0, \mathcal{T}),$$

where the sets U, W, X, Y, X^0 represent the external input set, the internal input set, the state set, the output set, and the initial state set, respectively. $u \in U, w \in W, x \in X, y \in Y$ are the external input, internal input, local state, and local output variables. $\mathcal{T} \subseteq M(U \times W \times X \times Y)$ characterizes all the trajectories that are described by a differential equation

$$\dot{x}(t) = f(x,w) + g(x,w)u \tag{1}$$

and $o : x \mapsto y$ is the output function.

To guarantee the existence and uniqueness of the system trajectory, we conveniently assume that the vector field and the output map are locally Lipschitz. Now we formally define an interconnected system.

Definition 2. Given N subsystems $\{G_i\}_{i\in\mathcal{I}}$, $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i), \mathcal{I} = \{1, 2, \dots, N\}$, and a binary connectivity relation $\mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$, we say $\{G_i\}_{i\in\mathcal{I}}$ is *compatible for composition* with respect to $\mathcal{E}$ if $\Pi_{j\in N(i)} Y_j \subseteq W_i$, where $N(i) = \{j : (j,i) \in \mathcal{E}\}$ is the index set of subsystems that influence G_i. G_j (G_i) is referred to as a parent (child) node of G_i (G_j).

In this definition, a set of subsystems is compatible for composition when, for each subsystem, the output space of all parental subsystems is a subset of its internal input space.

When the subsystems $\{G_i\}_{i\in\mathcal{I}}$ are compatible for composition w.r.t. $\mathcal{E}$, the composed system, also referred to as the interconnected system, is denoted by $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle = (U, \{0\}, X, Y, X^0, \mathcal{T})$, where $U = \Pi_{i\in\mathcal{I}} U_i, X = \Pi_{i\in\mathcal{I}} X_i, Y = \Pi_{i\in\mathcal{I}} Y_i, X^0 = \Pi_{i\in\mathcal{I}} X_i^0$. Denote the composed state by x, the composed external input u, and the composed output y. Then $(u(t), 0, x(t), y(t)) \in \mathcal{T}$ if and only if for all $i \in \mathcal{I}$, there exists $(u_i(t), w_i(t), x_i(t), y_i(t)) \in \mathcal{T}_i$ and $w_i(t) = (y_{j_1}(t), y_{j_2}(t), \dots, y_{j_p}(t))$, where $N(i) = \{j_1, j_2, \dots, j_p\}$.

B. Assume-guarantee contracts for invariance

To begin with, we introduce notation that will help us define the set of all continuous trajectories that always stay in a set. Let a nonempty set $S \subseteq \mathbb{R}^n$. Define

$$I_S^E = \{z : E \to \mathbb{R}^n \in M(\mathbb{R}^n) : \forall t \in E, z(t) \in S\}, \tag{2}$$

where E is a time interval. In the following, the superscript E is neglected as it is usually chosen as the maximal time interval of the existence of solutions to the continuous-time system. An invariance assume-guarantee contract (iAGC) is defined as follows:

Definition 3. For a continuous-time system $G = (U, W, X, Y, X^0, \mathcal{T})$, an *invariance assume-guarantee contract* (iAGC) for G is a tuple $C = (I_{\underline{W}}, I_{\underline{X}}, I_{\underline{Y}})$ where $\underline{W} \subseteq W, \underline{X} \subseteq X, \underline{Y} \subseteq Y$. We refer to $I_{\underline{W}}$ as the set of assumptions on the internal inputs, and $I_{\underline{X}}, I_{\underline{Y}}$ as the sets of guarantees on the states and outputs. We say a system G *satisfies a contract* $C = (I_{\underline{W}}, I_{\underline{X}}, I_{\underline{Y}})$, denoted $G \models C$, if there exists a feedback control $k(\cdot,\cdot) : X \times W \to U$ such that for all $t > 0$, for all $w|_{[0,t]} \in I_{\underline{W}}$, the state and output fulfill $x|_{[0,t]} \in I_{\underline{X}}, y|_{[0,t]} \in I_{\underline{Y}}$ for all trajectories $(u(t) = k(x,w), w(t), x(t), y(t)) \in \mathcal{T}$.

A key result that establishes the compositional reasoning of the system property is the following:

Lemma 1 (Compositional reasoning)**.** *Consider an interconnected system $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle = (U, \{0\}, X, Y, X^0, \mathcal{T})$ composed of N subsystems with a compatible binary connectivity relation $\mathcal{E}$. If for each subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$, there exists an invariance assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ such that $G_i \models C_i$ and $\Pi_{j\in N(i)} I_{\underline{Y}_j} \subseteq I_{\underline{W}_i}$, then $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle \models C$ with $C = (\{0\}, \Pi_{i\in\mathcal{I}} I_{\underline{X}_i}, \Pi_{i\in\mathcal{I}} I_{\underline{Y}_i})$.*

This lemma is a special case of [16, Theorem 3] and thus we neglect its proof here. While this lemma may seem intuitive, it is worth highlighting that we can not deduce directly the conclusion due to possible circular reasoning of implications. One such example for systems with non-locally Lipschitz vector fields is shown in [16, Example 6]. The

AGC framework helps to circumvent possible circular reasoning and enables compositional reasoning of the forward invariance property of interconnected systems.

C. System safety and barrier functions

Now we give the formal definition of safety of a continuous-time system. Throughout this work, we refer to a *safe region* as the collection of states that are benign, for example, unoccupied configuration space in robotic applications, and a *safe set* as a subset of the safety region that is also forward invariant.

Definition 4. Given a system $G = (U, W, X, Y, X^0, \mathcal{T})$ and a safe region $\mathcal{Q} \subseteq X$, we say the system G is *safe with respect to an internal input set* $\underline{W}$ if and only if $X^0 \subseteq \mathcal{Q}$, and for all initial states $x_0 \in X^0$ and for all internal input signals $w|_{[0,t]} \in I_{\underline{W}}$, there exists an external input signal $u|_{[0,t]} \in I_U$ such that $x|_{[0,t]} \in I_{\mathcal{Q}}$ for all $t > 0$.

We note that the internal input w is assumed to be known via communication. This is in contrast to the definition of a robust control invariant set where w is treated as disturbance and unknown [22], in which case the qualifier $\exists u$ proceeds $\forall w$. One way to certify the safety of the system is to find a (control) barrier function, also known as a barrier certificate [5], which is given by

Definition 5. A differential function $h : X \to \mathbb{R}$ for system $G = (U, W, X, Y, X^0, \mathcal{T})$ is called a *control barrier function* with respect to an internal input set $\underline{W} \subseteq W$, if there exists a class $\mathcal{K}$ function α such that $\forall w \in \underline{W}, \exists u \in U$ the following inequality holds for all x

$$\nabla h(x) f(x, w) + \nabla h(x) g(x, w) u + \alpha(h(x)) \geq 0. \tag{3}$$

When the external input set is empty, i.e., $U = \emptyset$, h is called a *barrier function* as this system has no active control. When such a (control) barrier function is found, then the set $\mathcal{C} = \{x : h(x) \geq 0\}$ is (controlled) forward invariant, and asymptotically stable when it is compact [2]. If $X^0 \subseteq \mathcal{C} \subseteq \mathcal{Q}$, then system safety is certified [2], [7]. In general, finding an invariant set $\mathcal{C}$ is computationally expensive for large nonlinear systems.

D. Sum-of-squares programs

One tractable approach to deal with infinite inequalities as in (3) is via sum-of-squares programming. A standard sum-of-squares (SOS) program takes the following form

$$\begin{aligned} &\min_{p_1,\dots,p_k} \textstyle\sum_{j=1}^{k} a_j p_j \\ &\text{s.t. } b_0(x) + \textstyle\sum_{j=1}^{k} p_i b_j(x) \in \Sigma[x], \end{aligned} \tag{4}$$

where the decision variables $p_1, \dots, p_k \in \mathbb{R}$, constants $a_1, \dots, a_k \in \mathbb{R}$ are the weights, and $b_0, \dots, b_k \in \mathcal{R}[x]$ are given polynomials. This SOS program is a convex optimization problem and can be equivalently transformed into a semi-definite program (SDP). Interested readers are referred to [23], [24] for more details.

E. Problem formulation

In this work, we aim to numerically verify the safety property of interconnected systems. The following sub-problems are considered:

(P1) For a continuous-time subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$ and a given safe region $\mathcal{Q}_i \subseteq X_i$, construct an invariance assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ such that $G_i \models C_i$ and $X_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$;

(P2) For an interconnected system $\langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle = (U, \{0\}, X, Y, X^0, \mathcal{T})$ and a safe region $\mathcal{Q} = \Pi_{i \in \mathcal{I}} \mathcal{Q}_i$, $\mathcal{Q}_i \subseteq X_i$, construct an invariance contract $C = (\{0\}, I_{\underline{X}}, I_{\underline{Y}})$ such that $G \models C$ and $X^0 \subseteq \underline{X} \subseteq \mathcal{Q}$.

If such a $\underline{X}$ is found, then safety of the interconnected system is certified.

Assumption 1. *We assume the following:*

1) *the local feedback law $u_i = k_i(x_i, w_i) \in U_i$ is known, but it does not necessarily render the interconnected system safe;*
2) *The class $\mathcal{K}$ function $\alpha(\cdot)$ in* (3) *is chosen to be a linear function with constant gain a.*
3) *The initial set X_i^0, safe region $\mathcal{Q}_i$, and the internal input set W_i are super-level sets of (possibly vector-valued) differentiable functions, i.e., $X_i^0 = \{x_i : b_i^0(x_i) \geq 0\}, \mathcal{Q}_i = \{x_i : q_i(x_i) \geq 0\}, W_i = \{(y_{j_1}, y_{j_2}, \dots, y_{j_p}) : d^i_{j_k}(y_{j_k}) \geq 0, k = 1, 2, \dots, p\}$, where $N(i) = \{j_1, j_2, \dots, j_p\}$.*
4) *$b_i^0, q_i \in \mathcal{R}[x_i], d^i_{j_k}(y_{j_k}) \in \mathcal{R}[y_{j_k}], f_i, g_i, k_i \in \mathcal{R}[x_i, w_i]$ are polynomials.*
5) *The subsets of $W_i, \mathcal{Q}_i$, i.e., $\underline{W}_i, \underline{\mathcal{Q}}_i$ are chosen in the form of*

$$\begin{aligned} &\underline{\mathcal{Q}}_i = \{x_i : q_i(x_i) \geq \zeta \mathbf{1} \text{ for some } \zeta \geq 0\}, \\ &\underline{W}_i = \{(y_{j_1}, \dots, y_{j_p}) : d^i_{j_k}(y_{j_k}) \geq \delta \mathbf{1} \text{ for some } \delta \geq 0\}. \end{aligned}$$

6) *When searching for non-negative polynomials, we restrict the search to the set of SOS polynomials up to a certain degree.*

These restrictions, even though conservative, will facilitate the convergence and completeness analysis that will be clear later. We note that the first two assumptions are in place to avoid bilinear terms when constructing the SOS programs. Both can be relaxed by considering iterative optimization approaches. See [7] for more details. Assumptions 1.3 and 1.5 help to parameterize the assumption and the guarantee sets by scalar variables δ and ζ, respectively. Assumptions 1.4 and 1.6 are standard in the field of SOS-based system verification.

For notational simplicity, we define the set projection of an internal input set W_i of subsystem G_i with respect to subsystem G_k as $\text{Proj}_k(W_i) = \{y_k : d_k^i(y_k) \geq 0\}$ if $k \in N(i)$, and $\text{Proj}_k(W_i) = \emptyset$ otherwise. For a mapping $o : X \to Y$, let $o^{-1}(\underline{Y}) := \{x : o(x) \in \underline{Y}\}$.

III. Proposed solutions

The proposed approach consists of 1) numerically constructing iAGCs for subsystems by synthesizing local (control) barrier functions, and 2) negotiating iAGCs among subsystems to certify the safety property of the interconnected system. We also discuss the convergence properties of our approach.

A. Local barrier function and AGC construction

In this subsection, we will focus on tackling Problem (P1) for a subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$. Under Assumption 1, the closed-loop subsystem dynamics of (1) are

$$\dot{x}_i(t) = f_i(x_i, w_i) + g_i(x_i, w_i) k_i(x_i, w_i) := F_i(x_i, w_i). \quad (5)$$

In this subsection, for the sake of notation simplicity, we will drop the subscript i when no confusion arises.

First we show the relations between a) finding a control barrier function, b) constructing an invariance assume-guarantee contract, and c) establishing the safety property of a subsystem.

Proposition 1. *Consider a continuous-time system $G = (U, W, X, Y, X^0, \mathcal{T})$, a safe region $\mathcal{Q}$ and an internal input set $\underline{W} \subseteq W$. Consider the following claims:*

① *there exists a CBF h with respect to the internal input set $\underline{W}$. Denote by $\mathcal{C} = \{x : h(x) \geq 0\}$;*
② *the system $G \models C$, where $C = (I_{\underline{W}}, I_{\mathcal{C}}, I_{o(\mathcal{C})})$;*
③ *$X^0 \subseteq \mathcal{C} \subseteq \mathcal{Q}$;*
④ *the system is safe with respect to $\underline{W}$;*

We have ① $\implies$ ②; ② and ③ $\implies$ ④.

Proof. ① $\implies$ ②: ① implies that the set $\mathcal{C}$ is forward invariant when the signal $w(t) \in I_{\underline{W}}$, which implies ② from Definition 3. ② and ③ $\implies$ ④: This is straightforward according to Definition 4. □

Numerically, one can formulate the conditions of ① and ③ of Proposition 1 as a set of SOS constraints, as follows.

Proposition 2. *Consider a continuous-time system $G = (U, W, X, Y, X^0, \mathcal{T})$ and a safe region $\mathcal{Q}$. If there exist SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[x, y_k], k = 1, 2, \ldots, p$, polynomial $h \in \mathcal{R}(x)$, and positive ϵ, a, δ such that*

$$h(x) - \sigma_{init} b^0(x) \in \Sigma[x]; \quad (6a)$$

$$-h(x) + \sigma_{safe} q(x) \in \Sigma[x]; \quad (6b)$$

$$\nabla h(x) F(x, y_1, \ldots, y_p) + a h(x) - \sum_{k=1}^{p} \sigma_k (d_k(y_k) - \delta) - \epsilon \in \Sigma[x, y_1, \ldots, y_p]. \quad (6c)$$

then, letting $\underline{W} = \{(y_1, \ldots, y_k \ldots, y_p) : d_k(y_k) \geq \delta\}$, ①, ②, ③, ④ in Proposition 1 hold.

Proof. (6c) is a SOS polynomial and thus $\nabla h(x) F(x, w) + a h(x) \geq 0, \forall w \in \underline{W}$. This shows that claim ① holds. Based on non-negativeness of SOS polynomials, (6a) and (6b) imply that $\forall x, b^0(x) \geq 0 \implies h(x) \geq 0$, and $\forall x, h(x) \geq 0 \implies q(x) \geq 0$, respectively. That is, $X_i^0 \subseteq \mathcal{C} \subseteq \mathcal{Q}$. Thus ③ holds. Following Proposition 1, we conclude the proof. □

Even though (6) is only a sufficient condition for system safety, it is a condition we can verify numerically (and efficiently when the system size is small). For this reason, we say that G is *certified to be safe* in $\mathcal{Q}$ w.r.t. $\underline{W}$ if condition (6) holds. We introduce the following special sets that are useful for contract composition later. In what follows, we take $0 < \epsilon << 1$ and a in (6) to be positive constants.

1) Maximal internal input set: To quantify the largest internal input set a subsystem can tolerate while still remaining safe, we propose the following optimization problem:

$$\begin{aligned} &\min \delta \\ &\text{s.t. } (6a), (6b), (6c), \delta \geq 0, \end{aligned} \quad (7)$$

where the decision variables include SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[y_k], k = 1, 2, \ldots, p$, polynomials $h \in \mathcal{R}(x)$, and a scalar δ. It should be noted that although (7) contains a bilinear term $\sigma_{input}\delta$, this can be solved efficiently by bisection as δ is a scalar. If (7) is feasible, denote the optimal value by $\delta^\star$ and the corresponding internal input set $\underline{W}^\star$. We call $\underline{W}^\star$ the *maximal internal input set* for a given subsystem G and safe region $\mathcal{Q}$.

2) Minimal safe region: Given a subsystem G with an internal input set $\underline{W}$, to quantify the least impact on its child subsystem, we propose the following optimization problem:

$$\begin{aligned} &\max \zeta \\ &\text{s.t. } (6a), (6c), \zeta \geq 0 \\ &\quad - h(x) + \sigma_{safe}(q(x) - \zeta) \in \Sigma[x]; \end{aligned} \quad (8)$$

where the decision variables include SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[y_k], k = 1, 2, \ldots, p$, polynomials $h \in \mathcal{R}(x)$, and a scalar ζ. We take ϵ, a to be positive constants. δ in (6c) is known as we assume $\underline{W}$ is given. It should be noted that although (8) contains a bilinear term $\sigma_{safe}\zeta$, this can be solved efficiently by bisection as ζ is a scalar. If (8) is feasible, denote the optimal value by $\zeta^\star$ and the corresponding safe region $\underline{\mathcal{Q}}^\star$. We call $\underline{\mathcal{Q}}^\star$ the *minimal safe region* for a given $\underline{W}$.

We have the following properties about the maximal internal input set $\underline{W}^\star$ and the corresponding minimal safe region $\underline{\mathcal{Q}}^\star$.

Proposition 3. *Under Assumption 1, for a continuous-time system $G = (U, W, X, Y, X^0, \mathcal{T})$ and a safe region $\mathcal{Q}$, the following results hold:*

1) *If (7) is feasible for some $\delta' \geq 0$, then (7) is also feasible for $\delta'', \delta'' \geq \delta'$. If (8) is feasible for some $\zeta' > 0$, then (8) is also feasible for $\zeta'', 0 \leq \zeta'' \leq \zeta'$.*
2) *Consider two safe regions $\underline{\mathcal{Q}}' \subseteq \underline{\mathcal{Q}}'' \subseteq \mathcal{Q}$. If (7) is feasible for the safe region $\underline{\mathcal{Q}}'$, then (7) is also feasible for $\underline{\mathcal{Q}}''$. Denoting the respective optimal values by δ', δ'' and the corresponding internal input sets $\underline{\mathcal{W}}', \underline{\mathcal{W}}''$, then $\delta'' \leq \delta'$ and $\underline{\mathcal{W}}' \subseteq \underline{\mathcal{W}}'' \subseteq \mathcal{W}$.*

3) *Consider two internal input sets* $\underline{\mathcal{W}}' \subseteq \underline{\mathcal{W}}'' \subseteq \mathcal{W}$*. If* (8) *is feasible with the internal input set* $\underline{\mathcal{W}}''$*, then* (8) *is also feasible for* $\underline{\mathcal{W}}'$*. Denoting the respective optimal values by* ζ', ζ'' *and the corresponding safe regions* $\underline{\mathcal{Q}}', \underline{\mathcal{Q}}''$*, then* $0 \leq \zeta'' \leq \zeta'$ *and* $\underline{\mathcal{Q}}' \subseteq \underline{\mathcal{Q}}'' \subseteq \mathcal{Q}$*.*
4) *If* (7) *is feasible, then* $\underline{W}^{\star}$ *is the largest internal input set w.r.t. which* G *is certified to be safe; if infeasible, then there exists no* $\underline{W} \subseteq W$ *w.r.t. which* G *can be certified to be safe.*
5) *If* (7) *is feasible, letting* $\underline{W} = \underline{W}^{\star}$*, then* (8) *is feasible and* $\underline{\mathcal{Q}}^{\star}$ *is the smallest safe region in which* G *is safe w.r.t.* $\underline{W}^{\star}$*.*

Proof. Claim 1) holds since one verifies that, when $\delta'' \geq \delta'$, any feasible decision variables $\sigma_{init}, \sigma_{safe}, \sigma_k, k = 1, 2, \dots, p, h$ to (7) for δ' are also feasible for the case of δ''. Similarly, when $0 \leq \zeta'' \leq \zeta'$, any feasible decision variables to (8) for ζ' are also feasible for the case of ζ''.

For $\underline{\mathcal{Q}}' \subseteq \underline{\mathcal{Q}}''$ (the corresponding $\zeta' \geq \zeta'' \geq 0$), if (7) is feasible for ζ', then the feasible decision variables are also feasible for the case of ζ''. As (7) minimizes over δ and the feasible set of the case ζ' is a subset of that of ζ'', then $\delta'' \leq \delta'$, proving Claim 2).

Similar argument applies for Claim 3). For $\underline{\mathcal{W}}' \subseteq \underline{\mathcal{W}}'' \subseteq \mathcal{W}$ (with the corresponding $\delta' \geq \delta'' \geq 0$), if (8) is feasible for δ'', then the feasible decision variables are also feasible for the case of δ'. As (8) maximizes over ζ and the feasible set of the case δ'' is a subset of that of δ', then $\zeta' \geq \zeta''$, proving Claim 3).

Claim 4) is true since $\underline{W}'' \subseteq \underline{W}'$ if and only if the corresponding $\delta'' \geq \delta'$, and the program in (7) minimizes δ. We note that the condition $\delta \geq 0$ comes from the condition $\underline{W} \subseteq W$. If (7) is feasible, then the feasible decision variables for $\delta = \delta^{\star}$ are also feasible for (8) when $\zeta = 0$. Further noting that $\underline{Q}'' \subseteq \underline{Q}'$ if and only if the corresponding $\zeta'' \geq \zeta'$ and (8) maximizes ζ, thus Claim 5) is deduced. □

Proposition 3's items 2 and 3 show a monotonic relation between the internal input sets and the safe regions. Intuitively, with a larger safe region, the system can tolerate a larger disturbance (internal input set); with a larger disturbance (internal input set), the most confined safe region will become larger. Proposition 3's items 4 and 5 further state that, for a given safe region, $\underline{W}^{\star}$ is the largest internal input set that a system can bear while remaining safe; for a given internal input set, $\underline{\mathcal{Q}}^{\star}$ is the most confined influence a system has for its child subsystems. When (7) and (8) are feasible for a subsystem G_i, denoting the corresponding sets as $\underline{W}_i^{\star}, \underline{\mathcal{Q}}_i^{\star}$, then we construct a local contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, where $\underline{W}_i = \underline{W}_i^{\star}, \underline{X}_i = \underline{\mathcal{Q}}_i^{\star}$, and $\underline{Y}_i = o_i(\underline{X}_i)$.

B. Contract composition and negotiation

In this section, we consider the interconnected system $G = \langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$, $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$ with safe region $\mathcal{Q}_i \subseteq X_i$. We have the following results on the safety properties of the interconnected system.

Proposition 4. *If, for each subsystem* G_i*, an iAGC* $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ *exists such that* $X_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$ *and*

$$\Pi_{j \in N(i)} \underline{Y}_j \subseteq \underline{W}_i, \tag{9}$$

then the interconnected system $\langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$ *is safe.*

Proof. From Lemma 1, $\langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle \models C$ with $C = (\{0\}, \Pi_{i \in \mathcal{I}} I_{\underline{X}_i}, \Pi_{i \in \mathcal{I}} I_{\underline{Y}_i})$. Note that $\Pi_{i \in \mathcal{I}} \underline{X}_i^0 \subseteq \Pi_{i \in \mathcal{I}} \underline{X}_i \subseteq \Pi_{i \in \mathcal{I}} \mathcal{Q}_i$, thus $\langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$ is safe. □

We refer to the condition (9) as the *contract compatibility condition* as it indicates whether the contract of a subsystem agrees with that of its parent subsystems. In the general case, the contracts $C_i, i \in \mathcal{I}$ found locally may not satisfy this condition, and we have to refine them so that (9) holds. We call this refinement process *negotiation*. In what follows, we consider three cases and propose several different algorithms. We note that all algorithms are sound, but differ in finite-step termination and completeness guarantees.

1) Acyclic connectivity graph: In this case, we assume that there exists no cycle in the connectivity graph $(\mathcal{I}, \mathcal{E})$. In this case, the hierarchical tree structure resembles a client-contractor relation model. For $k \in \text{Child}(i)$, we could view G_k as a client with an iAGC $(I_{\underline{W}_k}, I_{\underline{X}_k}, I_{\underline{Y}_k})$, who gives specifications on the behaviour of its parent node G_i (viewed as contractors) by $\underline{W}_k$. Based on this interpretation, we propose Algorithm 1.

In Algorithm 1, $\mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_{-1}$ represent the index sets of ready-to-update, to-be-updated, and updated subsystems, respectively. The algorithm starts with the local contract construction for the leaf nodes. Following a bottom-up traversal along the connectivity graph, for each subsystem G_i in $\mathcal{I}_0$, Algorithm 1 first updates its safe region $\mathcal{Q}_i$ such that it agrees with all its child nodes. This is explicitly conducted in Algorithm 2, while no operation is needed for leaf nodes. The set intersection in Algorithm 2 is again cast as a SOS program, as follows:

$$\begin{aligned} &\min_{\zeta \geq 0} \zeta \\ \text{s.t. } & q_i(x_i) - \zeta - \sigma_k(d_i^k \circ o_i(x_i) - \delta^k) \\ & \qquad \in \Sigma[x_i], \forall k \in \text{Child}(i), \end{aligned} \tag{10}$$

where the decision variables include $\sigma_k \in \Sigma[x_i], k \in \text{Child}(i)$, and a scalar ζ. Recall here o_i is the output map of subsystem G_i, $\text{Proj}_i(\underline{W}_k) = \{y_i : d_i^k(y_i) \geq \delta^k\}$. Denoting the optimal value by ζ' and $\mathcal{Q}_i' = \{x : q_i(x_i) \geq \zeta'\}$, $\mathcal{Q}_i'$ is then the largest inner-approximation of $\bigcap_{k \in \text{Child}(i)} o_i^{-1}(\text{Proj}_i(\underline{W}_k)) \cap \mathcal{Q}_i$. Recall that the subset of $\mathcal{Q}_i$ is parameterized by ζ from Assumption 1.5.

After updating the safe region, Algorithm 1 calculates the maximal internal input set $\underline{W}_i^{\star}$ (Line 6), which can be seen as the least requirement on its parent nodes as discussed in Proposition 3. Algorithm 3 then moves G_i to $\mathcal{I}_{-1}$, and checks for every to-be-updated subsystems whether all their child subsystems have been updated. If yes, then that subsystem is moved to the set of ready-to-update subsystems $\mathcal{I}_0$ and will be updated accordingly.

Proposition 5. *Consider an interconnected system with an acyclic connectivity graph $(\mathcal{I}, \mathcal{E})$. Algorithm 1 has the following properties:*

1) *Algorithm 1 terminates in finite steps and returns either* `True` *or* `False`*.*
2) *If Algorithm 1 returns* `True`*, then iAGCs $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$ satisfy the conditions in Proposition 4.*
3) *If Algorithm 1 returns* `False`*, then there exist no iAGCs $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$ that satisfy the conditions in Proposition 4 under Assumption 1.*

Proof. For every iteration of Algorithm 1, it will either terminate due to `infeasibility` or increase the cardinality of $\mathcal{I}_{-1}$ by 1. Since $|\mathcal{I}_{-1}|$ is upper bounded by $|\mathcal{I}|$, we know it has to terminate in finite steps. This proves Claim 1).

When Algorithm 1 returns `True`, each subsystem has gone through Step 4 - Step 10 and computed an iAGC $(I_{\underline{W}_i^\star}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ in a bottom-up transverse. As Step 4 reduces the safe region of subsystem G_i, and from (7), we have $X_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i' \subseteq \mathcal{Q}_i$. Moreover, for any $k \in \text{Child}(i)$, based on Algorithm 2, $\underline{Y}_i = o_i(\underline{X}_i) \subseteq o_i(\mathcal{Q}_i') \subseteq \text{Proj}_i(\underline{W}_k)$, which proves that the contract compatibility condition (9) holds. Following Proposition 4, we thus certify the safety of the interconnected systems. This proves Claim 2).

We show claim 3) by contradiction. Suppose that there exist iAGCs $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$ that satisfy the conditions in Proposition 4. Denote the safe regions with which such iAGCs are obtained by $\mathcal{Q}_i', i \in \mathcal{I}$, i.e., the functions defining those sets fulfill the SOS constraints in (8) (but not necessarily minimize the size of the safe region) and the sets fulfill the compatibility condition (9). Thanks to the tree structure, we can start our argumentation from the leaf nodes and iteratively reason about the nodes that are one level above, and end at the root node. From Proposition 3, for G_i being the leaf nodes, we have $\underline{W}_i \subseteq \underline{W}_i^\star$, the set obtained from (7). For G_j being the nodes one level above the leaf nodes, from Algorithm 2, we know $\mathcal{Q}_j' \subseteq \mathcal{Q}_j'^\star$, for that $\mathcal{Q}_j'^\star$ is the largest inner-approximation of all safe regions and that $\underline{W}_i \subseteq \underline{W}_i^\star$. Following Proposition 3 item 2, we know $\underline{W}_j \subseteq \underline{W}_j^\star$, where $\underline{W}_j^\star$ is the set obtained by solving (7) with $\mathcal{Q}_j'^\star$. Recursively, we thus obtain that $(I_{\underline{W}_i^\star}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$ exists. This contradicts with the premise that Algorithm 1 returns `False`. Thus Claim 3) is proven. □

2) Homogeneous interconnected system: In this case, we consider the homogeneous interconnected system in the following sense.

Definition 6. An interconnected system $\langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$ is called homogeneous if $G_i = G_j$ and $\mathcal{Q}_i = \mathcal{Q}_j, \forall i, j \in \mathcal{I}$.

Algorithm 4 starts with solving for one subsystem the maximal internal input set and the corresponding minimal safe region. If the compatibility condition is met, then we have verified the safety of the interconnected system; otherwise, we will reduce the safe region by taking the set intersection in Algorithm 2 and start the same process with the updated safe region $\mathcal{Q}_i'$.

Algorithm 1 `Contract construction for acyclic graph`

```
Require: $G_i$, $\mathcal{Q}_i, \forall i \in \mathcal{I}$
 1: $\mathcal{I}_0 \leftarrow$ set of leaf nodes, $\mathcal{I}_1 \leftarrow \mathcal{I} \setminus \mathcal{I}_0$, $\mathcal{I}_{-1} \leftarrow \emptyset$.
 2: while $\mathcal{I}_0 \neq \emptyset$ do
 3:     for each subsystem $G_i, i \in \mathcal{I}_0$ do
 4:         $\mathcal{Q}_i' \leftarrow$ update the local safe region $\mathcal{Q}_i$ by Alg. 2;
 5:         try
 6:             calculate $\delta_i^\star$ by solving (7) with safe region $\mathcal{Q}_i'$;
 7:             compute the corresp. iAGC $(I_{\underline{W}_i^\star}, I_{\underline{X}_i}, I_{\underline{Y}_i})$
 8:         catch infeasible
 9:             return False;
10:         end try
11:         update $\mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_{-1}$ by Alg. 3.
12:     end for
13: end while
14: return True.
```

Algorithm 2 `Update safe region`

```
Require: Safe region $\mathcal{Q}_i$ and iAGCs $(I_{\underline{W}_k}, I_{\underline{X}_k}, I_{\underline{Y}_k})$ for all $k \in \text{Child}(i)$.
 1: $M_i \leftarrow \bigcap_{k \in \text{Child}(i)} o_i^{-1}(\text{Proj}_i(\underline{W}_k)) \cap \mathcal{Q}_i$
 2: $\mathcal{Q}_i' \leftarrow$ largest inner-approximation of $M_i$ by (10)
 3: return $\mathcal{Q}_i'$.
```

We have the following results in this case:

Proposition 6. *Consider a homogeneous interconnected system as per Definition 6. Assume that $\{x_i : q_i(x_i) \geq a\} \subseteq X_i^0$ for some $a > 0$. Algorithm 4 has the following properties:*

1) *Algorithm 4 returns either* `True` *or* `False` *eventually.*
2) *If Algorithm 4 returns* `True`*, then iAGCs $C_i = (I_{\underline{W}_i^\star}, I_{\underline{X}_i^\star}, I_{\underline{Y}_i^\star})$, $i \in \mathcal{I}$ satisfy the conditions in Proposition 4.*
3) *If Algorithm 4 returns* `False`*, then there exists no common contract $C_0 = (I_{\underline{W}_0}, I_{\underline{X}_0}, I_{\underline{Y}_0})$ such that $G_i \models C_0, i \in \mathcal{I}$ and that the conditions in Proposition 4 are satisfied under Assumption 1.*

Proof. Consider the case when X_i^0 is a subset of the local safe region $\mathcal{Q}_i$ (otherwise, (7) yields `infeasible` in Step 2). There are three possibilities: 1) (7) is infeasible, for which the algorithm terminates with `False`; 2) the contract compatibility condition is satisfied, for which the algorithm terminates with `True`; 3) the algorithm starts a new iteration. For the third scenario, the local safe region $\mathcal{Q}_i$ is updated at every iteration, and at each iteration, the set size gets smaller. In particular, as the set size is parameterized by a scaler ζ, which is monotonically increasing, we know it has to converge to some number smaller than a (in which case we found compatible local contracts and the algorithm terminates with `True`) or becomes larger than a (in which case (7) yields `infeasible`). In either case, the algorithm will return `True` or `False` if the iteration goes to infinite.

If Algorithm 4 returns `True`, from Step 9, the contract

Algorithm 3 `Update` $\mathcal{I}_0$,$\mathcal{I}_1$ `and` $\mathcal{I}_{-1}$

```
Require: Subsystem $G_i$, $\mathcal{I}_0$,$\mathcal{I}_1$ and $\mathcal{I}_{-1}$.
 1: $\mathcal{I}_0 \leftarrow \mathcal{I}_0 \setminus \{i\}, \mathcal{I}_{-1} \leftarrow \mathcal{I}_{-1} \cup \{i\}$,
 2: for each subsystem $G_k$, $k \in \mathcal{I}_1$ do
 3:     if Child$(k) \subseteq \mathcal{I}_{-1}$ then
 4:         $\mathcal{I}_0 \leftarrow \mathcal{I}_0 \cup \{k\}, \mathcal{I}_1 \leftarrow \mathcal{I}_1 \setminus \{k\}$,
 5:     end if
 6: end for
```

Algorithm 4 `Contract construction for homogeneous systems`

```
Require: $G_i, \mathcal{Q}_i$
 1: try
 2:     calculate $\delta_i^\star$ by solving (7)
 3:     calculate $\zeta_i^\star$ by letting $\delta_i = \delta_i^\star$ and solving (8)
 4:     compute the corresp. iAGC $C_i = (I_{\underline{W}_i^\star}, I_{\underline{X}_i^\star}, I_{\underline{Y}_i^\star})$
 5: catch infeasible
 6:     return False
 7: end try
 8: Assign all subsystem $G_j, j \in \mathcal{I}$ with an iAGC $C_j = (I_{\underline{W}_j^\star}, I_{\underline{X}_j^\star}, I_{\underline{Y}_j^\star})$ with $\underline{W}_j^\star = \underline{W}_i^\star, \underline{X}_j^\star = \underline{X}_i^\star, \underline{Y}_j^\star = \underline{Y}_i^\star$.
 9: if $\underline{Y}_j^\star \subseteq \text{Proj}_j(\underline{W}_i^\star)$ for all $j \in N(i)$ then
10:     return True
11: else
12:     $\mathcal{Q}_i' \leftarrow$ update the local safe region $\mathcal{Q}_i$ by Alg. 2;
13:     Goto Step 1 with updated safe region $\mathcal{Q}_i'$
14: end if
```

compatibility condition holds for subsystem G_i. Noting that each subsystem has the same number of parent nodes (implicit from the fact that each subsystem has the same output set $Y_i = Y_j$ and the same internal input set $W_i = W_j$) and the same assumption and guarantee sets (Step 8), we know this compatibility condition also holds for all subsystems. Thus, Claim 2) is shown.

We show Claim 3) by contradiction. Suppose that a common local contract $C_0 = (I_{\underline{W}_0}, I_{\underline{X}_0}, I_{\underline{Y}_0})$ exists and the compatibility condition (9) holds. Denote the safe region with which such an iAGC is obtained by $\mathcal{Q}_0$. That is, the functions defining these sets fulfill the SOS constraints in (8) (but not necessarily minimize the size of the safe region) and

$$o(\mathcal{Q}_0) \subseteq \text{Proj}_i(\underline{W}_0). \tag{11}$$

Trivially, we know $X_i^0 \subseteq \mathcal{Q}_0 \subseteq \mathcal{Q}_i$. Let the sequence of the updated safe regions of Algorithm 4 be $Q^1 = \mathcal{Q}_i, Q^2, \ldots, Q^M$ (it is a finite sequence of sets with shrinking size following Claim 1)). Without loss of generality, assume $\mathcal{Q}^{r+1} \subsetneqq \mathcal{Q}_0 \subseteq \mathcal{Q}^r$. Following Proposition 3 items 2 and 4, we know $\underline{W}_0 \subseteq \underline{W}^\star\big|_{\mathcal{Q}_0} \subseteq \underline{W}^\star\big|_{\mathcal{Q}^r}$, where $\underline{W}^\star\big|_{\mathcal{Q}}$ represents the maximal internal input set given safe region $\mathcal{Q}$. Recall Q^{r+1} is obtained from Alg. 2, i.e., Q^{r+1} is the largest safe region such that $o(\mathcal{Q}^{r+1}) \subseteq \text{Proj}_i(\underline{W}^\star\big|_{\mathcal{Q}^r})$. However, from (11), we know $o(\mathcal{Q}_0) \subseteq \text{Proj}_i(\underline{W}_0) \subseteq \text{Proj}_i(\underline{W}^\star\big|_{\mathcal{Q}^r})$ and $\mathcal{Q}^{r+1} \subsetneqq \mathcal{Q}_0$. This yields a contradiction, which thus proves Claim 3). □

A common practice to bound the total number of iterations is to add extra termination conditions, e.g., Algorithm 4 terminates if the updated safe region $\mathcal{Q}_i'$ in Line 9 (with its level value ζ') is close in size compared to the original one $\mathcal{Q}_i$ (with its level value ζ), i.e., $\zeta' - \zeta < \epsilon$ for some small positive constant ϵ. Other termination conditions include the maximal number of iterations allowed. When the algorithm is terminated due to these conditions, we do not have a definite conclusion about the existence of compatible contracts.

3) General case: In the following, we provide a constructive approach for safety verification of interconnected systems with general connectivity graphs and dynamics.

Algorithm 5 `Contract construction for general systems`

```
Require: Subsystem $G_i$ and its safe region $\mathcal{Q}_i, i \in \mathcal{I}$ and connectivity graph $(\mathcal{I}, \mathcal{E})$
 1: run Algorithm 1;
 2: for each $G_i \in \mathcal{I}_1$ do
 3:     try
 4:         calculate $\delta_i^\star$ by solving (7);
 5:         calculate $\zeta_i^\star$ by letting $\delta_i = \delta_i^\star$ and solving (8)
 6:         compute the corresp. iAGC $(I_{\underline{W}_i^\star}, I_{\underline{X}_i^\star}, I_{\underline{Y}_i^\star})$
 7:     catch infeasible
 8:         return False;
 9:     end try
10: end for
11: if contract compatibility condition (9) does not hold then
12:     update $\mathcal{Q}_i$ for all $i \in \mathcal{I}_1$ by Alg. 2
13:     Goto Step 2
14: end if
15: return True.
```

Proposition 7. *For the general case, if Algorithm 5 returns* `True`*, then iAGCs $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$ satisfies the conditions in Proposition 4.*

The proof is straightforward and omitted. We note that Algorithm 5 simplifies to Algorithm 1 in the case of acyclic connectivity graph, and becomes Algorithm 4 for homogeneous interconnected systems. Proposition 7 only provides sufficient conditions on the existence of compatible contracts. We will explore how to provide completeness guarantees for Algorithm 5 or design other algorithms with such guarantees in our future work.

Remark 1 (Meaning of `False`)**.** It is worth highlighting that our completeness results are established under Assumption 1, and that the algorithm returning `False` does not mean that the interconnected system is unsafe. It simply means that we can not certify the safety of the interconnected systems under the restrictions in Assumption 1. When a `False` is encountered, one can group two or several subsystems

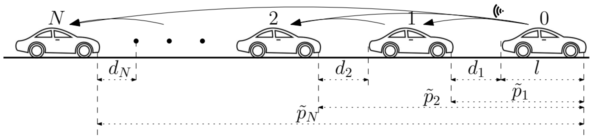


Fig. 1: Platooning scenario

together and run the algorithms again by taking a group of subsystems as a single one.

IV. Examples

A. Vehicular platooning: an acyclic example

Consider a vehicular platooning scenario adapted from [25] where $N+1$ autonomous vehicles are moving on a single-lane road. We assume that each vehicle has the same length l, and has access to the state information of its proceeding vehicle and the leading vehicle (hereafter referred to as the leader). The dynamics relative to the leader is

$$\begin{aligned} \dot{\tilde{p}}_i &= \tilde{v}_i, \\ \dot{\tilde{v}}_i &= \tilde{u}_i - (\tilde{v}_i - \tilde{v}_{i-1})^3, \end{aligned} \tag{12}$$

where $\tilde{p}_i(t) = p_0(t) - p_i(t), \tilde{v}_i = v_0(t) - v_i(t), \tilde{u}_i(t) = u_0(t) - u_i(t)$, $i = 1, 2, \ldots, N, k_0 > 0$. Here $p_i, v_i, u_i, \tilde{p}_i, \tilde{v}_i, \tilde{u}_i$ denote the absolute position, the absolute velocity, the absolute control, the relative position, the relative velocity, and the relative control of vehicle i, respectively. We conveniently let $\tilde{v}_0 = 0$ for ease of notation.

Instead of looking at the relative dynamics in (12), we introduce a new coordinate $x_i = (d_i, \tilde{v}_i)$ associated with vehicle i, where $d_i = \tilde{p}_i - \tilde{p}_{i-1} - l$ denotes the distance between the front of the i-th vehicle and the rear of its proceeding vehicle. See Figure 1 for an illustration. The dynamics of this new state are given by

$$\begin{aligned} \dot{d}_i &= \tilde{v}_i - \tilde{v}_{i-1} \\ \dot{\tilde{v}}_i &= -(\tilde{v}_i - \tilde{v}_{i-1})^3 + \tilde{u}_i \end{aligned} \tag{13}$$

From the analysis above, we can model the vehicular platooning system as an interconnected system. Each subsystem $G_i, i \in \mathcal{I} = \{1, 2, \ldots, N\}$, is a continuous-time system

$$G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$$

with $(d_i, \tilde{v}_i)$ as the state vector, and $U_i = \mathbb{R}, W_i = \left\{ \begin{smallmatrix} \emptyset, & i=1; \\ \mathbb{R}, & i\geq 2, \end{smallmatrix} \right.$, $X_i = \mathbb{R}^2, Y_i = \left\{ \begin{smallmatrix} \mathbb{R}, & i\leq N-1; \\ \emptyset, & i=N, \end{smallmatrix} \right.$, $X_i^0 \subset X_i, \mathcal{T}_i$ characterizes all the trajectories satisfying (13), and the output map o_i : $\left\{ \begin{smallmatrix} (d_i,\tilde{v}_i)\mapsto\tilde{v}_i & i\leq N-1 \\ (d_i,\tilde{v}_i)\mapsto\emptyset & i=N \end{smallmatrix} \right.$. The binary connectivity relation $\mathcal{E}$ is defined that $(j, i) \in \mathcal{E}$ if and only if $j = i-1, i = 2, 3, \ldots, N$. One verifies that $\{G_i\}_{i\in\mathcal{I}}$ is compatible for composition with respect to $\mathcal{E}$. In the following analysis, we assume all the subsystems have the same initial state set X_i^0 and safe region $\mathcal{Q}_i$, which are $X_i^0 = \{x_i : -x_i^\top Q x_i + q^\top x_i - 899 \geq 0\}$, and the safe region $\mathcal{Q}_i = \{x_i : -x_i^\top Q x_i + q^\top x_i - 800 \geq 0\}$. where $Q = \left[\begin{smallmatrix} 100 & 30 \\ 30 & 50 \end{smallmatrix} \right]$ and $q = (600, 180)$. The initial state set and the safe region are depicted in Fig.2(a). Each subsystem applies a local controller

$$\tilde{u}_i = -(\tilde{v}_i - \tilde{v}_{i-1}) - (d_i - 3) - (d_i - 3)^3, i \in \mathcal{I}.$$

Our task is to verify safety of the interconnected system $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E} \rangle$. In this scenario, we consider 4 vehicles ($N = 3$). Algorithm 1 will be used for this example. We will fix the form of $d_{j_k}^i$ in $\mathrm{Proj}_k(W_i)$ as in $d_{j_k}^i(x_{i-1}) = a^2 - (\tilde{v}_{i-1} - b)^2$ to denote a bounded interval, where a and b are determined accordingly.

Consider the vehicle 3, which is the leaf node in the graph. One calculates $d_2^3(x_2) = 2.439 - \tilde{v}_2^2$ by projecting $\mathcal{Q}_2$ to the $\tilde{v}_2$ coordinate. By solving (7) and (8), one obtains $\delta^\star = 1.704$ and $\zeta^\star = 1.1147$. That is to say, a local contract $C_3 = (I_{\underline{W}_3}, I_{\underline{X}_3}, I_{\underline{Y}_3})$ for vehicle 3 is constructed with

$$\underline{W}_3 = \{\tilde{v}_2 : 0.735 - \tilde{v}_2^2 \geq 0\}, \tag{14a}$$

$$\underline{X}_3 = \{x_3 : -x_3^\top Q x_3 + q^\top x_3 - 801.115 \geq 0\}\}, \tag{14b}$$

$$\underline{Y}_3 = o_3(\underline{X}_3). \tag{14c}$$

$\underline{W}_3$ can be seen as the requirement from vehicle 3 to vehicle 2. Following Algorithm 2 (and also by solving (10)), the updated safe region for vehicle 2 is $\mathcal{Q}_2' = \{x_2 : -x_2^\top Q x_2 + q^\top x_2 - 869.85 \geq 0\}$. The initial set and the guarantee set of vehicle 3 as well as the updated safe region of vehicle 2 are illustrated in Figure 2(b). We thus follow the same procedures for vehicles 2 and 1, and obtain the results in Figure 2(c) and Figure 2(d). Moreover, we calculate the assumption set $\underline{W}_1 = \{\tilde{v}_0 : 0.019 - \tilde{v}_0^2 \geq 0\}$, which holds true since $\tilde{v}_0(t) = 0$ for all t. Thus, we have constructed compatible local contracts for each vehicle. Following Proposition 4, we conclude that the platooning system is safe.

B. Room temperature: a homogeneous example

In the second example, we consider a room temperature regulation problem [26] in a ring-shaped building as illustrated in Fig. 3. Each room has its temperature x_i, which is affected by neighboring rooms, the heater, and the environment as follows

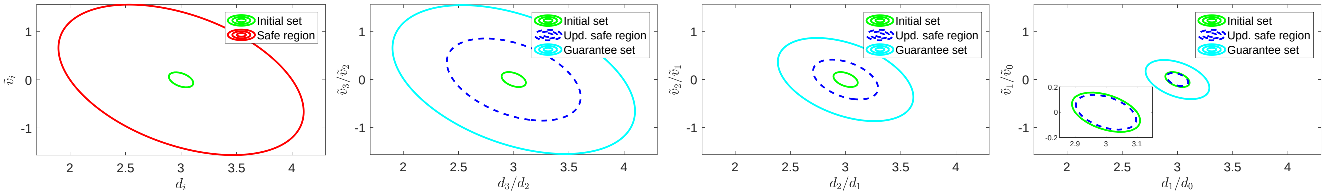
$$\begin{aligned} &\dot{x}_i(t) = \alpha(x_{i+1} + x_{i-1} - 2x_i) + \beta(t_e - x_i) + \gamma(t_h - x_i)u_i, \\ &y_i(t) = x_i, \end{aligned}$$

where x_{i+1}, x_{i-1} are the temperatures of room $i+1$ and $i-1$ (and we conveniently let $x_0(t) = x_N(t), x_{N+1}(t) = x_1(t)$), t_e, t_h are the temperatures of the environment and the heater, respectively. α, β, γ are the respective conduction factors for the neighboring room, the environment, and the heater. u_i denotes the valve control to the heater. Choose $(t_e, t_h, \alpha, \beta, \gamma) = (-1, 50, 0.05, 0.008, 0.004)$, and

$$u_i = 0.05(x_{i+1} + x_{i-1} - 2x_i) + 0.05(25 - x_i).$$

The initial set is $\mathcal{S}_{I,i} = [24, 26]$ and the safe region is $\mathcal{Q}_i = [20, 30]$ for every room.

We can model the temperature system as an interconnected system. In particular, each subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$ has x_i as the state, (x_{i-1}, x_{i+1}) as the internal input, u_i as the external input, $o_i(x_i) = x_i$,



(a) X_i^0 and $\mathcal{Q}_i$, $i = 1, 2, 3$.

(b) AGC sets for vehicle 3.

(c) AGC sets for vehicle 2.

(d) AGC sets for vehicle 1.

Fig. 2: Results for the platooning example.

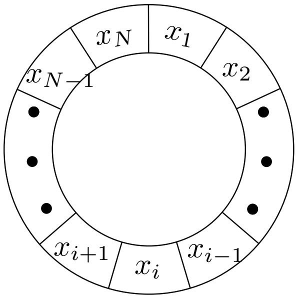


Fig. 3: Room temperature scenario.

$U_i, X_i, Y_i = \mathbb{R}, W_i = \mathbb{R}^2, X_i^0 = \{x_i : 1 - (x_i - 25)^2 \geq 0\}$, and $\mathcal{Q}_i = \{x_i : 5^2 - (x_i - 25)^2 \geq 0\}$. The connectivity relation $\mathcal{E}$ is defined that $(j, i) \in \mathcal{E}$ if and only if $j = i \pm 1, i = 1, 2, \ldots, N$. Per Definition 6, this is a homogeneous interconnected system and we will apply Algorithm 4 for this example.

At the first iteration, by solving (7) and (8), we obtain $\delta^\star = 20.575, \zeta^\star = 0$. Thus, we have constructed a local iAGC $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ with

$$\underline{W}_i = \{(x_{i-1}, x_{i+1}) : -x_j^2 + 50x_j - 620.575 \geq 0, j = i \pm 1\},$$
$$\underline{X}_i = \underline{Y}_i = \{x_i : -x_i^2 + 50x_i - 600 \geq 0\}.$$

After assigning the same local contract to all subsystems, one verifies that the contract compatibility condition (9) does not hold. According to Step 12 of Algorithm 4, we update the safe region for each room to be $\mathcal{Q}_i' = \{x_i : -x_i^2 + 50x_i - -620.575 \geq 0\}$ and start over. For the second iteration, we obtain local iAGC $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$ with

$$\underline{W}_i = \{(x_{i-1}, x_{i+1}) : -x_j^2 + 50x_j - 622.138 \geq 0, j = i \pm 1\},$$
$$\underline{X}_i = \underline{Y}_i = \{x_i : -x_i^2 + 50x_i - 623.575 \geq 0\}.$$

This time, one verifies that the compatibility condition (9) holds, and thus, certifies the safety of the room temperature system. An illustration of the assume and the guarantee sets is given in Fig. 4. We note that the computation expense is not related to the number of rooms N, and only small-size SOS optimization problems involving 3 independent variables are to be solved. This is in contrast to a naive SOS approach for synthesizing a barrier function, which will become intractable when thousands of rooms are involved.

V. Conclusions

In this work, we propose a safety verification scheme for interconnected continuous-time nonlinear systems based on assume-guarantee contracts (AGCs) and sum-of-squares (SOS) programs. The proposed scheme uses SOS optimization to calculate local invariance AGCs by synthesizing local (control) barrier functions, and then negotiates among neighboring subsystems at the contract level. If the proposed algorithms find compatible local contracts, safety property of the interconnected system is certified. We also show that the algorithms will terminate in finite steps and will always find a solution when one exists in the case of acyclic connectivity graphs or for homogeneous systems. We also demonstrate the effectiveness of the proposed algorithms for vehicle platooning and room temperature regulation examples.

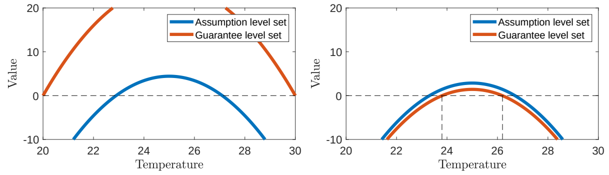


Fig. 4: Assume/guarantee sets for the room temperature example. Left: iteration 1, right: iteration 2.

References

[1] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, “Hamilton-Jacobi reachability: A brief overview and recent advances,” in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 2242–2253.

[2] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, “Control barrier function based quadratic programs for safety critical systems,” *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[3] E. F. Camacho and C. B. Alba, *Model predictive control*. Springer Science & Business Media, 2013.

[4] C. P. Bechlioulis and G. A. Rovithakis, “Robust adaptive control of feedback linearizable MIMO nonlinear systems with prescribed performance,” *IEEE Transactions on Automatic Control*, vol. 53, no. 9, pp. 2090–2099, 2008.

[5] S. Prajna and A. Jadbabaie, “Safety verification of hybrid systems using barrier certificates,” in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2004, pp. 477–492.

[6] A. Clark, “Verification and synthesis of control barrier functions,” in *2021 60th IEEE Conference on Decision and Control (CDC)*, 2021, pp. 6105–6112.

[7] H. Wang, K. Margellos, and A. Papachristodoulou, “Safety verification and controller synthesis for systems with input constraints,” *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 1698–1703, 2023.

[8] A. Robey, H. Hu, L. Lindemann, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, “Learning control barrier functions from expert demonstrations,” in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3717–3724.

[9] A. Abate, D. Ahmed, A. Edwards, M. Giacobbe, and A. Peruffo, “FOSSIL: a software tool for the formal synthesis of Lyapunov functions and barrier certificates using neural networks,” in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–11.

[10] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, "Robust control barrier–value functions for safety-critical control," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 6814–6821.

[11] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, 2020, pp. 1–11.

[12] Z. Lyu, X. Xu, and Y. Hong, "Small-gain theorem for safety verification of interconnected systems," *Automatica*, vol. 139, p. 110178, 2022.

[13] S. Coogan and M. Arcak, "A dissipativity approach to safety verification for interconnected systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1722–1727, 2014.

[14] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[15] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. A. Henzinger, K. G. Larsen *et al.*, "Contracts for system design," *Foundations and Trends® in Electronic Design Automation*, vol. 12, no. 2-3, pp. 124–400, 2018.

[16] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, p. 109910, 2021.

[17] E. S. Kim, M. Arcak, and S. A. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, 2017, pp. 207–216.

[18] K. Ghasemi, S. Sadraddini, and C. Belta, "Compositional synthesis via a convex parameterization of assume-guarantee contracts," in *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, 2020, pp. 1–10.

[19] A. Eqtami and A. Girard, "A quantitative approach on assume-guarantee contracts for safety of interconnected systems," in *2019 18th European Control Conference (ECC)*. IEEE, 2019, pp. 536–541.

[20] B. M. Shali, A. van der Schaft, and B. Besselink, "Composition of behavioural assume-guarantee contracts," *IEEE Transactions on Automatic Control*, vol. 68, no. 10, pp. 5991–6006, 2022.

[21] S. Liu, A. Saoud, P. Jagtap, D. V. Dimarogonas, and M. Zamani, "Compositional synthesis of signal temporal logic tasks via assume-guarantee contracts," in *2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 2184–2189.

[22] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[23] S. Prajna, A. Papachristodoulou, and P. A. Parrilo, "Introducing sostools: A general purpose sum of squares programming solver," in *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, vol. 1. IEEE, 2002, pp. 741–746.

[24] M. Arcak, C. Meissen, and A. Packard, *Networks of dissipative systems: compositional certification of stability, performance, and safety*. Springer, 2016.

[25] S. Liu and M. Zamani, "Compositional synthesis of almost maximally permissible safety controllers," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 1678–1683.

[26] A. Girard, G. Gössler, and S. Mouelhi, "Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models," *IEEE Transactions on Automatic Control*, vol. 61, no. 6, pp. 1537–1549, 2015.