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 the room temperature regulation example.**

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. A set of compatible AGCs, when found by our algorithms, certifies the safety of the interconnected system. Moreover, we show that the proposed algorithms will find a solution whenever

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.

one exists under relevant technical assumptions in the case of acyclic interconnections or homogeneous systems.

II. Notation and Preliminaries

Notation: 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. 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 say that node i is 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. Due to space limit, preliminaries on control barrier functions and sum-of-squares programs, all proofs, as well as many intuitive interpretations to the obtained results are omitted and can be found online [22].

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 $I_S^E = \{z : E \to \mathbb{R}^n \in M(\mathbb{R}^n) : \forall t \in E, z(t) \in S\}$, 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 $C = (\{0\}, \Pi_{i\in\mathcal{I}} I_{\underline{X}_i}, \Pi_{i\in\mathcal{I}} I_{\underline{Y}_i})$.*

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. 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 CBF condition 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) *$b_i^0, q_i \in \mathcal{R}[x_i], d^i_{j_k} \in \mathcal{R}[y_{j_k}], f_i, g_i, k_i \in \mathcal{R}[x_i, w_i]$ 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*
   $\underline{\mathcal{Q}}_i = \{x_i : q_i(x_i) \geq \zeta\mathbf{1}$ for some $\zeta \geq 0\}$,
   $\underline{W}_i = \{(y_{j_1}, \dots, y_{j_p}) : d^i_{j_k}(y_{j_k}) \geq \delta\mathbf{1}$ for some $\delta \geq 0\}$.
6) *When searching for non-negative polynomials, we restrict the search to the set of SOS polynomials up to a certain degree.*

For notational simplicity, we define the projection of an internal input set W_i of subsystem G_i with respect to subsystem G_k as $\text{Proj}_k(W_i) = \{y_k : d^i_k(y_k) \geq 0\}$ if $k \in N(i)$, and $\text{Proj}_k(W_i) = \emptyset$ otherwise.

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 is

$$\dot{x}_i(t) = f_i(x_i, w_i) + g_i(x_i, w_i)k_i(x_i, w_i) := F_i(x_i, w_i). \quad (2)$$

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.

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 $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[x, y_k], k = 1, 2, \dots, p$, polynomial $h \in \mathcal{R}(x)$, and positive ϵ, a, δ such that*

$$h(x) - \sigma_{init}b^0(x) \in \Sigma[x]; \quad (3a)$$

$$-h(x) + \sigma_{safe}q(x) \in \Sigma[x]; \quad (3b)$$

$$\nabla h(x)F(x, y_1, \dots, y_p) + ah(x) - \sum_{k=1}^{p}\sigma_k(d_k(y_k) - \delta) - \epsilon \in \Sigma[x, y_1, \dots, y_p]. \quad (3c)$$

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

Even though (3) 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 (3) 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 (3) 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:

$$\min \delta \quad \text{s.t. } (3a), (3b), (3c), \delta \geq 0, \quad (4)$$

where the decision variables include SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[y_k], k = 1, 2, \dots, p$, polynomials $h \in \mathcal{R}(x)$, and a scalar δ. It should be noted that although (4) contains a bilinear term $\sigma_{input}\delta$, this can be solved efficiently by bisection as δ is a scalar. If (4) 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:

$$\begin{aligned} &\max \zeta \\ &\text{s.t. } (3a), (3c), \zeta \geq 0 \\ &\quad - h(x) + \sigma_{safe}(q(x) - \zeta) \in \Sigma[x]; \end{aligned} \quad (5)$$

where the decision variables include SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[y_k], k = 1, 2, \dots, p$, polynomials $h \in \mathcal{R}(x)$, and a scalar ζ. We take ϵ, a to be positive constants. δ in (3c) is known as we assume $\underline{W}$ is given. It should be noted that although (5) contains a bilinear term $\sigma_{safe}\zeta$, this can be solved efficiently by bisection as ζ is a scalar. If (5) 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 (4) is feasible for some $\delta' \geq 0$, then (4) is also feasible for $\delta'', \delta'' \geq \delta'$. If (5) is feasible for some $\zeta' > 0$, then (5) 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 (4) is feasible for the safe region $\underline{\mathcal{Q}}'$, then (4) 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 (5) is feasible with the internal input set $\underline{\mathcal{W}}''$, then (5) 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 (4) 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 (4) is feasible, letting $\underline{W} = \underline{W}^\star$, then (5) is feasible and $\underline{\mathcal{Q}}^\star$ is the smallest safe region in which G is safe w.r.t. $\underline{W}^\star$.*

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.

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*

$$\Pi_{j\in N(i)}\underline{Y}_j \subseteq \underline{W}_i, \tag{6}$$

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

We refer to the condition (6) 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 (6) holds. We call this refinement process *negotiation*. In what follows, we consider different 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:

$$\begin{aligned} &\min_{\zeta\geq 0} \zeta \\ \text{s.t. } & q_i(x_i) - \zeta - \sigma_k(d_i^k \circ o_i(x_i) - \delta^k) \\ &\qquad \in \Sigma[x_i], \forall k \in \text{Child}(i), \end{aligned} \tag{7}$$

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.*

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

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 (4) with $\mathcal{Q}_i'$;
 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
    $k \in$ 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 (7)
 3: return $\mathcal{Q}_i'$.
```

following sense.

Definition 4. 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 $\mathcal{Q}_i'$. We have the following results:

Proposition 6. *Consider a homogeneous interconnected system as per Definition 4. 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.*

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 because of these conditions, we do not have a definite conclusion on the existence of compatible contracts.

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 (4);
 3:     calculate $\zeta_i^\star$ by letting $\delta_i = \delta_i^\star$ and solving (5)
 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
```

IV. Room temperature Example

In this example, we consider a room temperature regulation problem [23] in a ring-shaped building. Each room has its temperature x_i, which is affected by neighboring rooms, the heater, and the environment as follows

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

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 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, $o_i(x_i) = x_i$, $U_i, X_i, Y_i = \mathbb{R}, W_i = \mathbb{R}^2, X_i^0 = \{x_i : 1 - (x_i - 25)^2 \geq 0\}$, 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 4, this interconnected system is homogeneous and we will apply Algorithm 4 for this example.

At the first iteration, by solving (4) and (5), we obtain $\delta^\star = 20.575, \zeta^\star = 0$. Thus, we have constructed a local

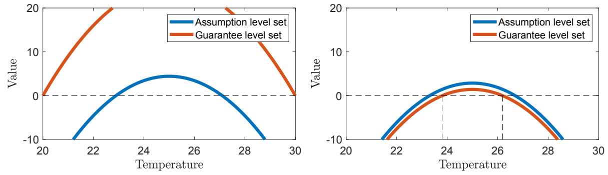

Fig. 1: Assume/guarantee sets for the room temperature example. Left: iteration 1, right: iteration 2.

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 (6) 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 (6) holds, and thus, certifies the safety of the room temperature system. An illustration of the assume and the guarantee sets is given in Fig. 1. 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.

Another numerical example on vehicle platooning is shown in [22], where we showcase how to apply the safety verification algorithms for interconnected systems with acyclic connectivity graphs.

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 eventually and will always find a solution when one exists in the case of acyclic connectivity graphs or homogeneous systems. We also demonstrate the effectiveness of the proposed algorithms for an room temperature regulation example.

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] X. Tan, A. Papachristodoulou, and D. V. Dimarogonas, "A contract negotiation scheme for safety verification of interconnected systems," 2023. [Online]. Available: https://arxiv.org/abs/2311.03164

[23] 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.