2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Compositional Synthesis of Safety Barrier Certificates for Infinite Networks

Ali Aminzadeh, *Student Member, IEEE,* and Abolfazl Lavaei, *Senior Member, IEEE*

***Abstract*— This paper offers a formal compositional framework for the construction of control barrier certificates (CBC) for an interconnected network comprised of a *countably infinite* number of discrete-time control subsystems. Inspired by small-gain type conditions designed inherently for the stability analysis of large-scale interconnected systems, our proposed approach aims to synthesize control strategies that ensure safety properties across infinite networks using local certificates of their individual subsystems. Specifically, this is achieved by employing a notion of *control sub-barrier certificates* (CSBC) for individual subsystems, using which one can ensure that the interconnected network avoids entering unsafe regions over an infinite time horizon under specific small-gain type conditions. We utilize a sum-of-squares (SOS) optimization approach to systematically search for CSBC and their associated control strategies that align with the desired safety criteria. We showcase the efficacy of our compositional approach through its application to a vehicle platooning scenario, which involves a countably *infinite number* of vehicles with a single leader and an *unlimited number* of followers.**

I. Introduction

Large-scale interconnected networks have garnered considerable attention in the past decade as a rich modeling framework that encompasses a wide array of applications, ranging from transportation to pivotal domains such as energy, biology, and critical infrastructures. To address systems potentially involving an unspecified number of subsystems, it is commonly considered reasonable to model a vast yet finite network as an infinite one, symbolizing the interconnection of numerous subsystems, each possessing finite dimensionality. This approach finds relevance in applications like vehicle platooning [1], [2], road traffic control [3], and multi-robot systems [4], where a substantial number of agents is engaged, justifying the representation of the system as an infinite coupling. In such applications, the presence of infinitely many subsystems in the network invalidates the assumption of treating it as finite. As a result, the exiting frameworks proposed for finite networks are not applicable to infinite ones.

The existing body of research concerning the formal verification and controller synthesis of complex dynamical systems heavily relies on the utilization of *finite abstractions*, as a discretization-based technique. In essence, finite abstractions act as a simplified representation for control systems that operate within continuous spaces, achieving this by associating discrete states and inputs with aggregated continuous counterparts [5], [6]. Various abstraction methods have been developed to synthesize controllers that enforce complex specifications, as exemplified by works [7], [8], [9], [10], [11], [12]. By leveraging computational tools rooted in discrete-event systems, it becomes feasible to synthesize controllers to fulfill high-level logic specifications, such as those expressed through linear temporal logic formulas (LTL) [13], which are often challenging to address using classical control design methods.

While finite-abstraction techniques hold a great promise, a significant limitation lies in their reliance on state and input discretization parameters. This dependency makes them susceptible to the curse of dimensionality, wherein computational complexity increases *exponentially* as the system's dimensionality grows. In practice, constructing such finite abstractions entails partitioning the state and input sets of concrete models based on predefined discretization parameters, rendering these approaches impractical for large-dimensional networks. To address this challenge, one promising solution is to construct a finite abstraction for the interconnected network by abstracting its individual subsystems with smaller dimensions using a compositional technique (see *e.g.,* [14], [15], [16], [17], [18], [19], [20], [21]).

In recent years, there has been a growing interest among researchers in approaches that do not rely on discretization when verifying and synthesizing complex systems. Notably, attention has been directed towards employing *control barrier certificates*, as initially introduced in [22], [23]. In particular, control barrier certificates are increasingly recognized as a promising *discretization-free* method for controller synthesis of complex systems (see *e.g.*, [24], [25], [26]). Compositional techniques have also been proposed to construct control barrier certificates for interconnected systems, building upon local certificates of smaller subsystems [27], [28], [29], [30], [31].

The aforementioned compositional techniques, designed primarily for finite networks in both abstraction and barrier methodologies, faced limitations when dealing with networks composed of an *infinite number* of subsystems. While some efforts have been made to address the *stability analysis* of infinite networks (*e.g.,* [32], [33], [34], [35]), or to focus on the *finite abstraction* of infinite networks (*e.g.,* [36]), there has been no prior work addressing the compositional synthesis of *safety barrier certificates* in the context of *infinite networks* of subsystems, without resorting to discretization.

The primary contribution of this work lies in developing, for the first time, a formal compositional scheme for the construction of control barrier certificates within an interconnected network consisting of a *countably infinite number* of discrete-time control subsystems. Drawing inspiration from

A. Aminzadeh is with the K. N. Toosi University of Technology, Iran. A. Lavaei is with the School of Computing, Newcastle University, United Kingdom. Email: aliaminzadeh@email.kntu.ac.ir, abolfazl.lavaei@newcastle.ac.uk.

small-gain type conditions originally designed for the stability analysis of interconnected systems, our approach aims to synthesize control strategies that guarantee safety properties across infinite networks by utilizing local certificates of individual subsystems. To achieve this goal, we introduce the concept of *control sub-barrier certificates* (CSBC) for individual subsystems. These CSBC are instrumental in ensuring that the interconnected network avoids entering unsafe regions subject to specific small-gain type conditions. We employ a systematic sum-of-squares optimization approach to search for CSBC and the corresponding control strategies that meet desired safety requirements. Proofs of all statements are omitted due to space constraints.

II. Discrete-Time Control Systems

A. Notation and Preliminaries

We employ the symbols $\mathbb{R}, \mathbb{R}_{>0}$, $\mathbb{R}_{\geq 0}$, $\mathbb{N}_0$, and $\mathbb{N}$, to represent the sets of real numbers, positive real numbers, non-negative real numbers, non-negative integers and positive integers, respectively. For any $b \in \mathbb{R}$, $|b|$ represents the absolute value of b, and for any $x = [x_1; \ldots; x_n] \in \mathbb{R}^n$, the infinity norm of x is determined as $|x| = max_{1\leq i\leq n}|x_i|$. Moreover, for any $m \times n$ matrix $C = (c_{ij})_{1\leq i\leq m, 1\leq j\leq n}$, we define $|C| = \max_{1\leq i\leq m} \sum_{j=1}^{n} |c_{ij}|$ as infinity norm of C. A vector μ consisting of infinitely many components μ_i is denoted by $\mu := (\mu_i)_{i\in\mathbb{N}}$. The identity matrix of size m is represented by $\mathbf{I}_m$. A continuously and strictly increasing function $\varphi : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ belongs to the class $\mathcal{K}$ if it satisfies $\varphi(0) = 0$ and to the class $\mathcal{K}_\infty$ if $\varphi(s) \to \infty$ as $s \to \infty$.

We use the notation l^∞ to refer to the Banach space that includes all infinite uniformly bounded sequences $s := (s_i) \in l^\infty, i \in \mathbb{N}$, where s_i represents the i-th element of a sequence $s \in l^\infty$. Furthermore, let l^∞_+ be defined as the positive cone within l^∞, encompassing all vectors $s \in l^\infty$ for which $s_i \geq 0, i \in \mathbb{N}$ holds true. In the context of l^∞, when comparing two sequences s and s', we establish that $s \leq s'$ holds true if each element in sequence s is less than or equal to its corresponding element in sequence s'. The standard unit vectors in l^∞, denoted as e_i, depict sequences that consist primarily of zeros with a solitary "1" positioned at index i, while all other entries are "0". The identity function is represented as $\mathcal{I}$, while the composition of functions is indicated by $\circ$. Given $\zeta : l^\infty_+ \to l^\infty_+$ being an operator, for all $n \in \mathbb{N}$, we define $\zeta^n(\cdot) := \zeta^{n-1} \circ \zeta(\cdot)$, with ζ^0 denoting the identity operator on l^∞.

B. Infinite Networks

Firstly, we introduce discrete-time control subsystems as the initial building blocks. These subsystems will be subsequently interconnected to construct an infinite network.

Definition 2.1: A discrete-time control subsystem $\Psi_i, i \in \mathbb{N}$, can be represented as

$$\Psi_i = (X_i, W_i, U_i, f_i, Y_i, h_i),$$

where:

- $X_i \subseteq \mathbb{R}^{n_i}, W_i \subseteq \mathbb{R}^{p_i}, U_i \subseteq \mathbb{R}^{m_i}$ are state, *internal* and *external* input sets of the subsystem, respectively;
- $f_i : X_i \times W_i \times U_i \to X_i$ is the transition map that characterizes the evolution of the subsystem;
- $Y_i \subseteq \mathbb{R}^{q_i}$ and $h_i : X_i \to Y_i$ are the output set and map of the subsystem.

The discrete-time control subsystem Ψ_i is characterized by a difference equation expressed as

$$\Psi_i : \begin{cases} x_i(k+1) = f_i(x_i(k), w_i(k), u_i(k)), \\ y_i(k) = h_i(x_i(k)), \end{cases} \quad k \in \mathbb{N}_0. \tag{1}$$

The input-output configuration of each subsystem $\Psi_i, i \in \mathbb{N}$, is defined as

$$w_i = (w_{ij})_{j\in \boldsymbol{N}_i} \in W_i := \prod_{j\in \boldsymbol{N}_i} W_{ij}, \tag{2}$$

$$y_i = (y_{ij})_{j\in (i\cup \boldsymbol{M}_i)} \in Y_i := \prod_{j\in (i\cup \boldsymbol{M}_i)} Y_{ij}, \tag{3}$$

$$h_i(x_i) = (h_{ij}(x_i))_{j\in (i\cup \boldsymbol{M}_i)}, \tag{4}$$

where:

- $\boldsymbol{N}_i \in \mathbb{N}$ represents a finite set comprising those subsystems Ψ_j, $j \in \boldsymbol{N}_i$, *that affect* Ψ_i;
- $\boldsymbol{M}_i \in \mathbb{N}$ represents a finite set comprising those subsystems $\Psi_{j'}$, $j' \in \boldsymbol{M}_i$ *that are affected by* Ψ_i.

Note that $i \notin \boldsymbol{N}_i \cup \boldsymbol{M}_i$, for any $i \in \mathbb{N}$, $w_{ij} \in W_{ij}$, and $y_{ij} = h_{ij}(x_i) \in Y_{ij}$. The *external* outputs are characterized by y_{ii} while $y_{ij}, j \in \boldsymbol{M}_i$, serve as *internal* outputs that facilitate interconnections between subsystems. It is assumed that the dimension of w_{ij} is equal to that of y_{ji} for all $i \in \mathbb{N}$ and for all $j \in \boldsymbol{N}_i$.

In the subsequent definition, we present a formal definition of *infinite networks* composed of individual subsystems.

Definition 2.2: Given subsystems $\Psi_i = (X_i, W_i, U_i, f_i, Y_i, h_i)$, defined in Definition 2.1 with an input-output structure characterized by equations (2)-(4), the infinite network can be formally expressed as a tuple $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}} = (X, U, f, Y, h)$, where

- $X = \{x = (x_i)_{i\in\mathbb{N}} : x_i \in X_i, \|x\| := \sup_{i\in\mathbb{N}}\{|x_i|\} < \infty\}$,
- $U = \{u = (u_i)_{i\in\mathbb{N}} : u_i \in U_i, \|u\| := \sup_{i\in\mathbb{N}}\{|u_i|\} < \infty\}$,
- $f(x, u) = (f_i(x_i, w_i, u_i))_{i\in\mathbb{N}}$,
- $Y = \prod_{i\in\mathbb{N}} Y_{ii}, h(x) = (h_{ii}(x_i))_{i\in\mathbb{N}}$.

The evolution of the infinite network $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}}$ is defined as

$$\Psi : \begin{cases} x(k+1) = f(x(k), u(k)), \\ y(k) = h(x(k)), \end{cases} \quad k \in \mathbb{N}_0, \tag{5}$$

wherein the interconnection among subsystems is illustrated through the following constraint:

$$\forall i \in \mathbb{N}, \forall j \in \boldsymbol{N}_i: \quad w_{ij} = y_{ji},\ Y_{ji} \subseteq W_{ij}. \tag{6}$$

The sequence $x_{x_0u} : \mathbb{N} \to X$, which satisfy (5) for any initial state $x_0 \in X$, and input sequence $u(\cdot)$, is referred to as the *solution process* of Ψ, when subjected to an external input u, and an initial state x_0. To establish the well-posedness of the infinite network in (5), it is imperative that $f(x, u) \in X$, for all pair $(x, u) \in X \times U$.

In the upcoming section, to ensure that the infinite network avoids entering a specific unsafe region within an infinite time horizon, we present the notion of control sub-barrier certificates (CSBC) and control barrier certificates (CBC) for, respectively, discrete-time control systems (comprising both internal and external signals) and interconnected networks (lacking internal signals).

III. Control (Sub-)barrier Certificates

Definition 3.1: Consider a discrete-time control subsystem $\Psi_i = (X_i, W_i, U_i, f_i, Y_i, h_i)$, and sets $X_{0_i}, X_{a_i} \subseteq X_i$, where the *initial set* X_{0_i} comprises states from which the subsystem Ψ_i can initiate its operation, while the *unsafe set* X_{a_i} encompasses states that must be avoided due to safety concerns. Assuming the existence of functions $\delta_i, \xi_i \in \mathcal{K}_\infty$, where $\xi_i < \mathcal{I}$, $\rho_{w_i} \in \mathcal{K}_\infty \cup \{0\}$ as well as constants $\sigma_i, \phi_i \in \mathbb{R}_{>0}$, a function $\mathbb{B}_i : X_i \to \mathbb{R}_{\geq 0}$ is referred to as a *control sub-barrier certificate (CSBC)* for Ψ_i if the subsequent conditions are fulfilled:

$$\mathbb{B}_i(x_i) \geq \delta_i(|h(x_i)|^2), \qquad \forall x_i \in X_i, \tag{7a}$$

$$\mathbb{B}_i(x_i) \leq \sigma_i, \qquad \forall x_i \in X_{0_i}, \tag{7b}$$

$$\mathbb{B}_i(x_i) \geq \phi_i, \qquad \forall x_i \in X_{a_i}, \tag{7c}$$

and $\forall x_i \in X_i$, $\exists u_i \in U_i$, such that $\forall w_i \in W_i$, one has

$$\mathbb{B}_i(x_i(k+1)) \leq \max\Big\{\xi_i(\mathbb{B}_i(x_i(k))), \rho_{w_i}(|w_i(k)|^2)\Big\}. \tag{7d}$$

We now provide the following definition to describe control barrier certificates for interconnected networks.

Definition 3.2: Consider an infinite network $\Psi = (X, U, f, Y, h)$ as in Definition 2.2. Assuming the existence of a function $\xi \in \mathcal{K}_\infty$, with $\xi < \mathcal{I}$, and constants $\sigma, \phi \in \mathbb{R}_{>0}$, with $\phi > \sigma$, a function $\mathbb{B} : X \to \mathbb{R}_{\geq 0}$ is referred to as a *control barrier certificate (CBC)* for Ψ, if the subsequent conditions hold:

$$\mathbb{B}(x) \leq \sigma, \qquad \forall x \in X_0, \tag{8a}$$

$$\mathbb{B}(x) \geq \phi, \qquad \forall x \in X_a, \tag{8b}$$

and $\forall x \in X$, $\exists u \in U$, such that

$$\mathbb{B}(x(k+1)) \ \leq \xi(\mathbb{B}(x(k))), \tag{8c}$$

where sets $X_0, X_a \subseteq X$ denote the initial and unsafe sets of the interconnected network, respectively.

As outlined in Definition 3.2, control barrier certificates are designed within the state space of the system while imposing conditions on both the function itself, specifically conditions (8a)-(8b), and its one-step transition, as represented by condition (8c). An essential aspect of this concept is its initial level set σ, which could be designed using SOS programming as a decision variable, effectively segregating an unsafe region X_a from all system trajectories originating from a specified set of initial states X_0. The computational complexity of finding CBC for interconnected networks is notably high, primarily due to the system's dimensionality. This challenge primary motivated us to introduce the concept of CSBC for individual subsystems with an internal input variable w_i, as defined in Definition 3.1. Subsequently, in Section IV, we propose a compositional approach for constructing a CBC for an infinite network based on the CSBC of individual subsystems. It is worth noting that the additional condition (7a) in CSBC plays a crucial role in the subsequent section, facilitating compositionality.

Remark 3.3: In Definition 3.2, the requirement that $\phi > \sigma$ is crucial to guarantee the safety certificate for an infinite network, as established in Theorem 3.4. Nevertheless, Definition 3.1 does not impose such a condition as CSBC are solely utilized for constructing CBC for infinite networks without ensuring subsystem safety.

Now, via the notions of CBC in Definition 3.2, we ensure that the infinite network described in (5) will not enter unsafe regions through the following theorem [22].

Theorem 3.4: Given an infinite network $\Psi = (X, U, f, Y, h)$ defined in Definition 2.2, assume that $\mathbb{B}$ is a CBC for Ψ as defined in Definition 3.2. Then, for all $x_0 \in X_0$ and $k \in \mathbb{N}$, one has $x_{x_0 u} \notin X_a$ under the input trajectory $u(\cdot)$ associated with the CBC $\mathbb{B}$ within an infinite time horizon.

IV. Compositional Construction of CBC

In this section, inspired by [32], [36], our objective is to compositionally construct a CBC for the infinite network Ψ by leveraging CSBC of individual subsystems $\Psi_i, i \in \mathbb{N}$. To achieve this, we first define the following function based on ξ_i and ρ_{w_i}, associated with $\mathbb{B}_i$, $\forall i, j \in \mathbb{N}$:

$$\xi_{ij} := \begin{cases} \xi_i, & \text{if } i = j, \\ (\mathcal{I} - \xi_i)^{-1} \circ \rho_{w_i} \circ \delta_j^{-1}, & \text{if } j \in \boldsymbol{N}_i, \\ 0, & \text{if } i \neq j, j \notin \boldsymbol{N}_i. \end{cases} \tag{9}$$

Accordingly, we introduce an operator $\zeta : l_+^\infty \to l_+^\infty$ based on ξ_{ij} in (9) as

$$\zeta(s) = (\sup_{j \in \mathbb{N}}\{\xi_{ij}(s_j)\})_{i \in \mathbb{N}}, \quad s \in l_+^\infty. \tag{10}$$

We also raise the assumption that there exist functions $\tilde{\xi}, \tilde{\rho}_w, \tilde{\delta} \in \mathcal{K}_\infty$ that satisfy $\xi_i \leq \tilde{\xi}, \rho_{w_i} \leq \tilde{\rho}_w, \delta_i \geq \tilde{\delta}$, for all $i \in \mathbb{N}$. This assumption ensures the well-defined nature of the operator ζ as defined in (10). Subsequently, we present the following proposition to establish the small-gain condition ([32, Proposition 7.17]).

Proposition 4.1: Under the well-posedness of ζ in (10), the following conditions are equivalent:

- The spectral radius of ζ, denoted by $r(\zeta)$, fulfills

$$r(\zeta) = \lim_{n \to +\infty} (\sup_{j_1, \ldots, j_{n+1} \in \mathbb{N}} \xi_{j_1 j_2} \circ \cdots \circ \xi_{j_n j_{n+1}})^{1/n} < 1. \tag{11}$$

- There exists a vector $\mu := (\mu_i)_{i \in \mathbb{N}} \in l_+^\infty$ and a constant $\lambda \in (0, 1)$ such that

$$\zeta(\mu) \leq \lambda \mu. \tag{12}$$

The inequality in (11) is referred to as the *small-gain condition*, and its satisfaction guarantees the existence of

(potentially nonlinear) $\mathcal{K}_\infty$ functions μ_i according to (12) that fulfill the following condition:

$$\zeta(\mu(\theta)) \leq \lambda\mu(\theta), \quad \forall\theta \in \mathbb{R}_{\geq 0}.$$

For any $i \in \mathbb{N}$ and $\theta \in \mathbb{R}_{\geq 0}$, according to (10) we have

$$(\sup_{j\in\mathbb{N}}\{\xi_{ij} \circ \mu_j(\theta)\})_{i\in\mathbb{N}} \leq \lambda\mu(\theta),$$

from which, since $\lambda \in (0, 1)$, one can conclude that

$$\sup_{j\in\mathbb{N}}\{\xi_{ij} \circ \mu_j(\theta)\} \leq \lambda\mu_i(\theta) < \mu_i(\theta).$$

By applying μ_i^{-1} to both sides, we obtain:

$$\mu_i^{-1}(\sup_{j\in\mathbb{N}}\{\xi_{ij} \circ \mu_j(\theta)\}) = \sup_{j\in\mathbb{N}}\{\mu_i^{-1} \circ \xi_{ij} \circ \mu_j(\theta)\} < \theta. \quad (13)$$

Since (13) holds for all $i \in \mathbb{N}$, it can be finally stated as

$$\sup_{i,j\in\mathbb{N}}\{\mu_i^{-1} \circ \xi_{ij} \circ \mu_j\} < \mathcal{I}. \quad (14)$$

In the upcoming theorem, we demonstrate that under small-gain condition (11), *equivalently* condition (14), it is possible to construct a CBC for the infinite network Ψ using CSBC of individual subsystems $\Psi_i, i \in \mathbb{N}$.

Theorem 4.2: Consider an infinite network $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}}$, which arises from an infinite number of subsystems Ψ_i. Let each individual subsystem Ψ_i possess a CSBC $\mathbb{B}_i$, as defined in Definition 3.1. If condition (11) is met and the following inequality holds

$$\sup_i\left\{\mu_i^{-1}(\phi_i)\right\} > \sup_i\left\{\mu_i^{-1}(\sigma_i)\right\}, \quad (15)$$

then $\mathbb{B}(x)$ defined as

$$\mathbb{B}(x) := \sup_i\left\{\mu_i^{-1}(\mathbb{B}_i(x_i))\right\}, \quad (16)$$

is a CBC for the infinite network $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}}$ with $\sigma = \sup_i\left\{\mu_i^{-1}(\sigma_i)\right\}$, $\phi = \sup_i\left\{\mu_i^{-1}(\phi_i)\right\}$, and $\xi(s) = \sup_{ij}\left\{\mu_i^{-1} \circ \xi_{ij} \circ \mu_j(s)\right\}$.

Remark 4.3: It is worth noting that by assuming $\xi_{ij} \leq \mathcal{I}$ for any $i, j \in \mathbb{N}$, inequality (14) can be satisfied by setting $\mu_i = \mathcal{I}$ for all $i \in \mathbb{N}$. Consequently, CBC in (16) simplifies to $\mathbb{B}(x) := \sup_i\{\mathbb{B}_i(x_i)\}$, and as a result, the small-gain condition (14) is *automatically fulfilled*.

V. Computation of CSBC and Safety Controller

In this section, we reformulate conditions (7a)-(7d) as a sum of squares (SOS) optimization problem [37]. This enables us to construct CSBC of individual subsystems and their associated safety controller in a systematic fashion. To do so, we assume that each subsystem has continuous state and input sets X, U, W, with polynomial transition maps f_i. Under this assumption, we now reformulate conditions (7a)-(7d) as an SOS optimization program.

Lemma 5.1: Consider subsystems Ψ_i in Definition 2.1. Let sets X_{0_i}, X_{a_i}, X_i, U_i, and W_i be semi-algebraic, defined by vectors of polynomial inequalities $g_{0_i}(x_i) \geq 0$, $g_{a_i}(x_i) \geq 0$, $g_i(x_i) \geq 0$, $g_{u_i}(u_i) \geq 0$, and $g_{w_i}(w_i) \geq 0$. Let there exist an SOS polynomial $\mathbb{B}_i(x_i)$, constants $\sigma_i, \phi_i \in \mathbb{R}_{>0}$, functions $\bar{\rho}_{w_i} \in \mathcal{K}_\infty \cup \{0\}$, $\delta_i, \bar{\xi}_i \in \mathcal{K}_\infty$, with $\bar{\xi}_i < \mathcal{I}$, polynomials $\gamma_{u_{zi}}(x_i)$ corresponding to the z^{th} input in $u_i = (u_{1_i}, u_{2_i}, ..., u_{m_i}) \in U_i \subseteq \mathbb{R}^{m_i}$, and vectors of SOS polynomials $\gamma_{0_i}(x_i), \gamma_{a_i}(x_i)$, $\gamma_i(x_i)$, $\hat{\gamma}_i(x_i)$, $\gamma_{u_i}(u_i)$, $\gamma_{w_i}(w_i)$ with appropriate dimensions such that the subsequent expressions are in the form of SOS polynomials:

$$\mathbb{B}_i(x_i) - \gamma_i^\top(x_i)g_i(x_i) - \delta_i(h_i(x_i)^\top h_i(x_i)) \quad (17a)$$

$$-\mathbb{B}_i(x_i) - \gamma_{0_i}^\top(x_i)g_{0_i}(x_i) + \sigma_i \quad (17b)$$

$$\mathbb{B}_i(x_i) - \gamma_{a_i}^\top(x_i)g_{a_i}(x_i) - \phi_i \quad (17c)$$

$$-\mathbb{B}_i(f_i(x_i, u_i, w_i)) + \bar{\xi}_i(\mathbb{B}_i(x_i)) + \bar{\rho}_{w_i}\left(\frac{{w_i}^\top w_i}{p_i}\right) - \sum_{z=1}^{m_i}(u_{zi} - \gamma_{u_{zi}}(x_i)) - \hat{\gamma}_i^\top(x_i)g_i(x_i) - \gamma_{u_i}^\top(u_i)g_{u_i}(u_i) - \gamma_{w_i}^\top(w_i)g_{w_i}(w_i), \quad (17d)$$

with p_i being the dimension of the internal input set W_i. Consequently, $\mathbb{B}_i(x)$ is a CSBC fulfilling conditions (7a)-(7d) with

$$\xi_i = \mathcal{I} - (\mathcal{I} - \pi_i) \circ (\mathcal{I} - \bar{\xi}_i), \rho_{w_i} = (\mathcal{I} - \bar{\xi}_i)^{-1} \circ \pi_i^{-1} \circ \bar{\rho}_{w_i}, \quad (18)$$

with π_i being an arbitrarily selected $\mathcal{K}_\infty$ function, where $\mathcal{I} - \pi_i \in \mathcal{K}_\infty$. Furthermore, $u_i = [\gamma_{u_{1i}}(x_i); \ldots; \gamma_{u_{mi}}(x_i)]$, $i \in \mathbb{N}$, acts as the associated controller for the subsystem Ψ_i.

Remark 5.2: In conditions (7a) and (7d), we encounter infinity norms associated with $h_i(x_i)$ and w_i, respectively. To render them amenable to polynomial solutions, we transformed these norms into Euclidean norms by incorporating their respective weighting factors. This conversion allows us to express (17a) and (17d) as polynomial expressions. Similarly, we reformulated the max-form condition (7d) as a summation form (17d) by recovering ξ_i and ρ_{w_i} according to (18). Through these appropriate conversions, Lemma 5.1 ensures that fulfilling conditions (17a)-(17d) implies the original conditions (7a)-(7d).

Remark 5.3: Note that, akin to Lyapunov functions, Lemma 5.1 provides a set of *sufficient* conditions for the existence of CSBC, as per Definition 3.1. In cases where an SOS polynomial CSBC is not found at a fixed degree, one may consider increasing the degree of the CSBC in order to potentially design it, albeit at the expense of increased computational complexity.

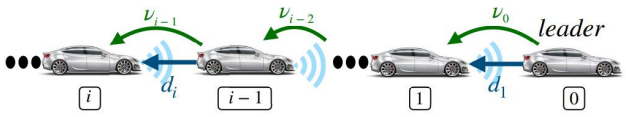

Fig. 1. A platoon consisting of an *infinitely countable number* of vehicles.

VI. Case Study

In this section, we illustrate the effectiveness of our approach over a vehicle platoon consisting of an infinitely countable number of vehicles, as depicted in Fig. 1.

The evolution of the states within the *interconnected network* can be elucidated as follows [1]:

$$\Psi: \begin{cases} x(k+1) = Ax(k) + u(k), \\ y(k) = x(k), \end{cases}$$

where A constitutes a block matrix featuring diagonal elements denoted by $\hat{A}$ and off-diagonal blocks designated as $A_{i(i-1)} = A_w$, with $i \in \mathbb{N}$, and $i \geq 2$, as

$$\hat{A} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \; A_w = \begin{bmatrix} 0 & \tau \\ 0 & 0 \end{bmatrix},$$

with $\tau = 0.005$ representing the interconnection strength, and all non-diagonal blocks are specified as zero matrices. Furthermore, $x(k) = (x_i(k))_{i\in\mathbb{N}}$ and $u(k) = (u_i(k))_{i\in\mathbb{N}}$. We now represent the description of each individual vehicle as:

$$\Psi_i: \begin{cases} x_i(k+1) = \hat{A}x_i(k) + u_i(k) + A_w w_i(k), \\ y_i(k) = x_i(k). \end{cases}$$

It can be readily ascertained that $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}}$, where $w_i(k) = [0; w_{i(i-1)}(k)]$, with $w_{i(i-1)}(k) = [0;1]^\top x_{i-1}(k)$, and $w_{1,0}(k) = 0$. The state representation of the i-th vehicle is characterized by $x_i = [d_i; v_i]$, where d_i represents the difference in position between vehicle i and its proceeding vehicle $i-1$, where the vehicle labeled as the 0-th vehicle serves as the leader. In addition, v_i denotes the velocity of the vehicle i in the reference frame of the leader. The control input u_i lives within $[-0.35, 0.35]$. The main control objective in vehicle platoon is to adjust each vehicle's speed to uphold a safe distance from its preceding vehicle [1]. To do so, we aim at constructing CSBC of subsystems Ψ_i and subsequently designing local controllers. As a result, the controller for the interconnected network Ψ takes the form of a vector, with each of its elements serving as a controller for the individual subsystems Ψ_i.

Our initial step involves verifying the well-defined nature of our infinite network $\Psi = \mathcal{N}(\Psi_i)_{i\in\mathbb{N}}$ by ensuring that $\|f(x,u)\| < \infty$, according to Definition 2.2. By defining $C = \max\{|\hat{A}|, 1, |A_w|\}$, we have:

$$\begin{aligned} \|f(x,u)\| &= \sup_{i\in\mathbb{N}}\{|f_i(x_i,w_i,u_i)|\} = \sup_{i\in\mathbb{N}}\{|\hat{A}x_i + u_i + A_w w_i|\} \\ &\leq |\hat{A}| \sup_{i\in\mathbb{N}}\{|x_i|\} + \sup_{i\in\mathbb{N}}\{|u_i|\} + |A_w| \sup_{i\in\mathbb{N}}\{|w_i|\} \\ &\leq C(\sup_{i\in\mathbb{N}}\{|x_i|\} + \sup_{i\in\mathbb{N}}\{|u_i|\} + \sup_{i\in\mathbb{N}}\{|x_i|\}) \\ &= C(\|x\| + \|u\| + \|x\|) < \infty. \end{aligned}$$

As a result, one can infer that $\Psi = \mathcal{N}(\Psi)_{i\in\mathbb{N}}$ is indeed well-defined.

The areas of interest for each vehicle encompass $X_i \in [0,1] \times [-0.3, 0.7]$, $X_{0_i} \in [0.25, 0.75] \times [-0.05, 0.45]$, and $X_{a_i} \in [0,1] \times [-0.3, -0.15] \cup [0,1] \times [0.55, 0.7]$. In the absence of a safety controller, Fig. 2 (left) illustrates that a representative vehicle repeatedly enters the unsafe region X_{a_i} when starting from the initial set X_{0_i}, indicating a lack of safety. In order to construct a CSBC and its corresponding safety controller for each individual vehicle as detailed in Section V, we utilize the software tool SOSTOOLS [38] in conjunction with the SDP solver SeDuMi [39]. In accordance

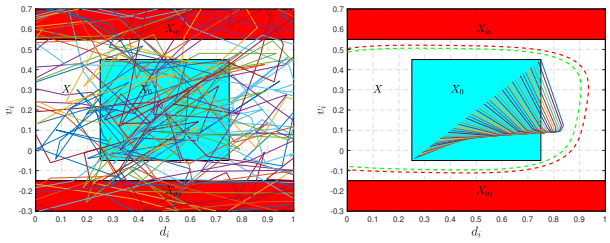

Fig. 2. **Left:** Closed-loop states trajectories of a representative vehicle under a *random controller*. The regions of interest encompass the state space $X_i \in [0,1] \times [-0.3, 0.7]$, the initial region $X_{0_i} \in [0.25, 0.75] \times [-0.05, 0.45]$, and unsafe regions $X_{a_i} \in [0,1] \times [-0.3, -0.15] \cup [0,1] \times [0.55, 0.7]$. **Right:** Closed-loop states trajectories of a representative vehicle are depicted for 30 different initial values under the safety controller in (19). Green and red dashed lines are initial and unsafe level sets, respectively.

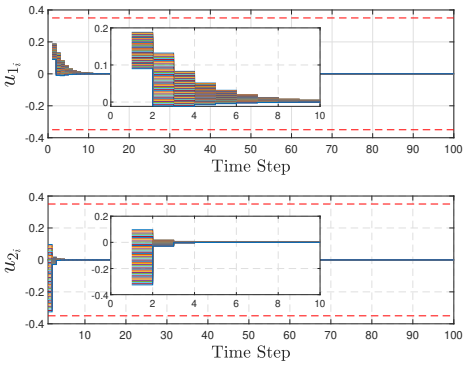

Fig. 3. Synthesized controllers $u_i = [u_{1_i}; u_{2_i}]$, as designed in (19), for a representative vehicle with 30 different initial conditions within 100 time steps.

with Lemma 5.1, we design CSBC with an order of 4 as follows:

$$\begin{aligned} \mathbb{B}_i(x_i) = {} & 7.16d_i^4 - 3.88d_i^3 v_i - 8.92d_i^3 + 4.28d_i^2 v_i^2 + 2.31d_i^2 v_i \\ & + 4.30d_i^2 + 5.40d_i v_i^3 - 6.72d_i v_i^2 + 0.62d_i v_i - 1.02d_i \\ & + 85.30v_i^4 - 71.91v_i^3 + 23.44v_i^2 - 3.31v_i + 0.25, \end{aligned}$$

and its associated safety controller as:

$$u_i = \begin{bmatrix} -0.4d_i + 0.2v_i + 0.3 \\ 0.4d_i - 0.9v_i + 0.05 \end{bmatrix}, \tag{19}$$

for all $i \in \mathbb{N}$. Additionally, the corresponding constants and functions within Definition 3.1 are designed as $\delta_i(s) = 10^{-5}s, s \in \mathbb{R}_{\geq 0}, \sigma_i = 0.7, \phi_i = 0.85, \xi_i = 0.975, \rho_{w_i}(s) = 8 \times 10^{-7}s, s \in \mathbb{R}_{\geq 0}$.

Next, we assess the small-gain condition (14) for the compositional results. It can be easily confirmed that $\xi_{ij} < 1$ for any $i, j \in \mathbb{N}$. Therefore, according to Remark 4.3, by selecting $\mu_i(s) = s$ for all $i \in \mathbb{N}$, condition (14) is always satisfied, regardless of the number of vehicles involved. Consequently, $\mathbb{B}(x) := \sup_i\{(\mathbb{B}_i(x_i))\}$ is a CBC for the infinite network Ψ, fulfilling conditions of Definition 3.2 with $\sigma = 0.7$, $\phi = 0.85$, and $\xi = 0.975$. By leveraging Theorem 3.4, we guarantee that the solution process of the vehicle platoon originating from X_0 will maintain within the safe domain within an infinite time horizon. Visual representations

of closed-loop state and input trajectories for a representative vehicle, starting from 30 different initial conditions, can be observed in Figs. 2 (right) and 3, respectively.

VII. Conclusion

In this paper, we introduced a formal compositional framework for constructing safety barrier certificates for an interconnected network comprised of a *countably infinite* number of subsystems. Our proposed approach aimed to synthesize control strategies that ensured safety properties across infinite networks using local certificates of their individual subsystems. Utilizing the concept of *control sub-barrier certificates (CSBC)* for individual subsystems, we enabled the infinite network to avoid entering unsafe regions under specific small-gain type conditions. Our approach transformed the required criteria into an SOS optimization problem, which facilitated the systematic search for CSBC and their corresponding safety controllers.

References

[1] S. Sadraddini, S. Sivaranjani, V. Gupta, and C. Belta, "Provably safe cruise control of vehicular platoons," *IEEE Control Systems Letters*, vol. 1, no. 2, pp. 262–267, 2017.

[2] A. Lavaei, L. Di Lillo, A. Censi, and E. Frazzoli, "Formal estimation of collision risks for autonomous vehicles: A compositional data-driven approach," *IEEE Transactions on Control of Network Systems*, vol. 10, no. 1, pp. 407–418, 2022.

[3] S. Coogan, M. Arcak, and C. Belta, "Formal methods for control of traffic flow: Automated control synthesis from finite-state transition models," *IEEE Control Systems Magazine*, vol. 37, no. 2, pp. 109–128, 2017.

[4] L. Wang, A. D. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Transactions on Robotics*, vol. 33, no. 3, pp. 661–674, 2017.

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

[6] C. Belta, B. Yordanov, and E. A. Gol, *Formal methods for discrete-time dynamical systems*. Springer, 2017, vol. 89.

[7] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[8] A. A. Julius and G. J. Pappas, "Approximations of stochastic hybrid systems," *IEEE Transactions on Automatic Control*, vol. 54, no. 6, pp. 1193–1203, 2009.

[9] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2009.

[10] M. Zamani, G. Pola, M. Mazo, and P. Tabuada, "Symbolic models for nonlinear control systems without stability assumptions," *IEEE Transactions on Automatic Control*, vol. 57, no. 7, pp. 1804–1809, 2011.

[11] 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.

[12] S. Coogan and M. Arcak, "Efficient finite abstraction of mixed monotone systems," in *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, 2015, pp. 58–67.

[13] C. Baier, J. P. Katoen, and K. G. Larsen, *Principles of model checking*. MIT press, 2008.

[14] Y. Tazaki and J. Imura, "Bisimilar finite abstractions of interconnected systems," in *International Workshop on Hybrid Systems: Computation and Control*, 2008, pp. 514–527.

[15] G. Pola, P. Pepe, and M. D. Di Benedetto, "Symbolic models for networks of control systems," *IEEE Transactions on Automatic Control*, vol. 61, no. 11, pp. 3663–3668, 2016.

[16] M. Zamani and M. Arcak, "Compositional abstraction for networks of control systems: A dissipativity approach," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1003–1015, 2017.

[17] M. Zamani, M. Mazo, M. Khaled, and A. Abate, "Symbolic abstractions of networked control systems," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 1622–1634, 2017.

[18] A. Swikir and M. Zamani, "Compositional synthesis of finite abstractions for networks of systems: A small-gain approach," *Automatica*, vol. 107, pp. 551–561, 2019.

[19] A. Nejati and M. Zamani, "Compositional construction of finite MDPs for continuous-time stochastic systems: A dissipativity approach," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 1962–1967, 2020.

[20] A. Lavaei, "Automated verification and control of large-scale stochastic cyber-physical systems: Compositional techniques," Ph.D. dissertation, Department of Electrical Engineering, Technische Universität München, Germany, 2019.

[21] A. Lavaei and M. Zamani, "From dissipativity theory to compositional synthesis of large-scale stochastic switched systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 9, pp. 4422–4437, 2022.

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

[23] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[24] U. Borrmann, L. Wang, A. D. Ames, and M. Egerstedt, "Control barrier certificates for safe swarm behavior," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 68–73, 2015.

[25] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proceedings Volumes*, vol. 40, no. 12, pp. 462–467, 2007.

[26] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *18th European control conference (ECC)*, 2019, pp. 3420–3431.

[27] Z. Lyu, X. Xu, and Y. Hong, "Small-gain theorem for safety verification of interconnected systems," *Automatica*, vol. 139, pp. 1–6, 2022.

[28] A. Lavaei and E. Frazzoli, "Compositional controller synthesis for interconnected stochastic systems with markovian switching," in *American Control Conference (ACC)*, 2022, pp. 4838–4843.

[29] M. Anand, A. Lavaei, and M. Zamani, "From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 10, pp. 5638–5645, 2022.

[30] A. Nejati and M. Zamani, "From dissipativity theory to compositional construction of control barrier certificates," *Schloss-Dagstuhl-Leibniz Zentrum für Informatik*, 2022.

[31] A. Lavaei and E. Frazzoli, "Scalable synthesis of safety barrier certificates for networks of stochastic switched systems," *IEEE Transactions on Automatic Control*, 2024.

[32] A. Mironchenko, C. Kawan, and J. Glück, "Nonlinear small-gain theorems for input-to-state stability of infinite interconnections," *Mathematics of Control, Signals, and Systems*, vol. 33, no. 4, pp. 573–615, 2021.

[33] S. Dashkovskiy, A. Mironchenko, J. Schmid, and F. Wirth, "Stability of infinitely many interconnected systems," *IFAC-PapersOnLine*, vol. 52, no. 16, pp. 550–555, 2019.

[34] C. Kawan, A. Mironchenko, A. Swikir, N. Noroozi, and M. Zamani, "A Lyapunov-based small-gain theorem for infinite networks," *IEEE Transactions on Automatic Control*, vol. 66, no. 12, pp. 5830–5844, 2020.

[35] S. Dashkovskiy and S. Pavlichkov, "Stability conditions for infinite networks of nonlinear systems and their application for stabilization," *Automatica*, vol. 112, pp. 1–12, 2020.

[36] S. Liu, N. Noroozi, and M. Zamani, "Symbolic models for infinite networks of control systems: A compositional approach," *Nonlinear Analysis: Hybrid Systems*, vol. 43, pp. 1–16, 2021.

[37] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical programming*, vol. 96, pp. 293–320, 2003.

[38] 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.*, vol. 1, 2002, pp. 741–746.

[39] J. F. Sturm, "Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones," *Optimization methods and software*, vol. 11, no. 1-4, pp. 625–653, 1999.