Data-Driven Safety Verification of Discrete-Time Networks: A Compositional Approach

Navid Noroozi, Ali Salamati, *Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*—This letter proposes a compositional data-driven approach for safety verification of networks of discrete-time subsystems with *formal guarantees*. Following a modular approach and for each subsystem, we search for a so-called sub-barrier candidate represented as a linear combination of a priori user-defined basis functions. We formulate the conditions on sub-barrier candidates as robust convex programs (RCPs) which are semi-infinite linear programs. Collecting sampled data from each subsystem, we approximate each RCP via a scenario convex program (SCP) which is a finite linear program. We provide an *explicit* formula to compute the minimum number of sampled data guaranteeing a desired mismatch between the optimal value of each RCP and that of the corresponding SCP in a probabilistic sense. To ensure that the sum of the sub-barrier candidates is a barrier function for the whole network, we define a global dissipativity condition on top of the local SCPs. The local SCPs are thus related to each other via this global condition. This results in a large-scale optimization problem in a standard canonical form which is efficiently solved by the alternating direction method of multipliers (ADMM) algorithm. The effectiveness of our approach is illustrated by applying it to a room temperature control problem in a 100-room building.**

***Index Terms*—Data-driven methods, formal safety verification, interconnected systems, barrier functions.**

I. Introduction

INCREASING complexity in dynamical networks as well as rapid advances in big data management and low-cost, distributed sensing and computing have made the use of data-driven methods for system analysis and control increasingly popular, e.g., [1]–[4]. Data-driven methods exploit measurements of the system and may not require any prior knowledge of the system model. However, two of the main drawbacks with most data-driven methods are i) lack of formal out-of-sample performance guarantees and ii) computational complexity, among others. The latter can particularly become an issue while dealing with large-scale interconnected bbsystems.

This letter aims to simultaneously address both issues in the context of safety verification of discrete-time networks. To this end, we mainly rely on the notion of barrier functions. Barrier functions have been introduced as a tool for safety verification of dynamical systems [5], [6]. They are also used to verify robustness and/or design controllers enforcing safety, e.g., [7], [8]. Most of these results, however, rely on having a sufficiently accurate knowledge of models of the systems. In this letter, we do not make such an assumption; instead we assume that we have access to a sufficient number of sampled data for each subsystem in a network. Specially, we provide an *explicit* formula for the minimum number of data required for each subsystem to provide an out-of-sample guarantee on the safety of the whole network.

Following a modular approach, we associate a so-called sub-barrier candidate to each subsystem, which is expressed as a linear combination of a priori user-defined basis functions, e.g., monomials. For each subsystem, we formulate the conditions over each sub-barrier candidate as a robust convex program (RCP), where the coefficients associated with the corresponding sub-barrier candidate are considered as the decision variables. Within each RCP, the constraints have to be satisfied over all state set which makes the RCP a semi-infinite linear program. Given that sub-systems' models are *unavailable*, the RCPs cannot be solved directly. Instead, we *approximate* each RCP by a data-driven optimization program called *scenario convex program* (SCP) [9]. By collecting data from each subsystem, an SCP is obtained by replacing the original inequality constraints in the RCP with finitely many ones computed over the data set. By leveraging the results in [9], we provide a minimum number of data ensuring that the optimal value of an SCP lies within a desired vicinity of that of the associated RCP in a probabilistic sense.

Obtaining sub-barrier candidates from local SCPs, the overall barrier candidate for the whole network is constructed by taking the sum of those sub-barrier candidates. There is, however, no guarantee that the resulting function satisfies all the requirements of a barrier certificate for the overall network. We

Manuscript received September 14, 2021; revised November 14, 2021; accepted December 1, 2021. Date of publication December 14, 2021; date of current version January 11, 2022. The work of Navid Noroozi and Ali Salamati was supported by the Deutsche Forschungsgemeinschaft (DFG) under Grant WI 1458/16-1. The work of Majid Zamani was supported by the H2020 European Resuscitation Council (ERC) Starting Grant AutoCPS under Grant 804639. Recommended by Senior Editor C. Prieur. *(Corresponding author: Navid Noroozi.)*

Navid Noroozi is with Model-Based Systems Engineering (MBSE), SIGNON Deutschland GmbH, 10117 Berlin, Germany (e-mail: navid.noroozi@signon-group.com).

Ali Salamati is with the Institute of Informatics, Ludwig Maximilian University of Munich, 80539 Munich, Germany (e-mail: ali.salamati@lmu.de).

Majid Zamani is with the Institute of Informatics, Ludwig Maximilian University of Munich, 80539 Munich, Germany, and also with the Computer Science Department, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: majid.zamani@colorado.de).

Digital Object Identifier 10.1109/LCSYS.2021.3135455

address this issue by enforcing a global dissipativity condition on top of the local SCPs. The global dissipativity condition is expressed as a linear matrix inequality (LMI) and relates local SCPs to each other. This results in a distributed semi-definite program which is efficiently solved by the alternating direction method of multipliers (ADMM) algorithm [10]. We illustrate the effectiveness of our approach by applying it to a room temperature problem in a circular building consisting of 100 rooms, where the dynamics are unknown.

Literature review: A series of recent approaches has been proposed in order to combine the notion of barrier certificates with data-driven techniques and address safety verification and synthesis problems. In [11], an approach based on barrier functions is developed to verify if there is a set of parameters for which the trajectory of a parametric continuous-time nonlinear system is consistent with a data-set collected from the system. In [12], a controller is synthesized based on limited data along with a single trajectory of the system and then a safety analysis is performed using barrier certificates. In [13], an approach is provided to learn a control barrier function via safe trajectories considering appropriate Lipschitz continuity assumptions on the dynamical system. A procedure is proposed in [14] to synthesize controllers for unknown nonlinear systems by using learned Gaussian processes in place of dynamics, and constructing control barrier certificates for them.

The result in [15] introduces a scenario-driven approach to provide a lower bound on the number of samples required to solve a chance constraint optimization problem with an a priori confidence. The proposed results in [9] establish a direct probabilistic connection between the optimal value of an RCP and that of the corresponding scenario convex program (SCP). The proposed results in [16] provide a data-driven approach on the safety verification of unknown stochastic systems by leveraging the results in [9]. Despite the effectiveness of the method proposed in [16] in computing barrier functions, the required number of data, unfortunately, grows *exponentially* with the dimension of the system. Hence, the applicability of this approach, in general, is limited to systems with very low dimensions.

Contributions: In this letter, we address the computational complexity issue in [16] and extend the approach to deal with networks of discrete-time systems. Our proposed method *breaks down* the order of the computational complexity into that of subsystems level, i.e., the computational complexity is linear with respect to the number of subsystems. In addition, we provide a confidence on the safety of the overall network, which is obtained from some confidences associated to subsystems. To the best of our knowledge, this is the first result on the safety verification of unknown interconnected systems by integrating data-driven techniques, barrier functions, and dissipativity reasoning in a modular manner.

Notation: For any pair $(x, y) \in \mathbb{R}^n \times \mathbb{R}^m$, we write (x, y) to represent $[x^\top, y^\top]^\top$. By I_n we denote the identity matrix of dimension n. Given a vector $v \in \mathbb{R}^n$, we denote the infinity norm of v by $|v|_\infty$. Given a matrix $A \in \mathbb{R}^{n\times m}$, the Frobenius norm of matrix A is defined by $||A||_F = \sqrt{\text{trace}(A^\top A)}$. Given a set $\mathcal{A} \subseteq \mathbb{R}^n$, the indicator function associated to set $\mathcal{A}$ is defined by $\mathbb{1}_{\mathcal{A}} : \mathbb{R}^n \to \{0, 1\}$, where $\mathbb{1}_{\mathcal{A}}(x) = 1$ if $x \in \mathcal{A}$ and $\mathbb{1}_{\mathcal{A}}(x) = 0$ otherwise. Given a complete probability space $(\Omega, \mathcal{F}, \mathbb{P})$, let Ω^N be the N-Cartesian product of set Ω and denote the respective product measure by $\mathbb{P}^N$.

II. Problem Statement

Consider a discrete-time system

$$\Sigma : x^+ = g(x), \tag{1}$$

where state $x \in \mathcal{X} \subseteq \mathbb{R}^n$. We assume that $g\colon \mathcal{X} \to \mathcal{X}$ is well-defined over $\mathcal{X}$.

Given an unsafe set $\mathcal{X}_u \subseteq \mathcal{X}$, we aim to verify if any trajectory of the system starting from an initial set $\mathcal{X}_0 \subseteq \mathcal{X}\backslash\mathcal{X}_u$, always stays away from the unsafe set $\mathcal{X}_u$, while the system dynamics g is unknown. We use the notion of barrier certificates defined as next to verify safety of the system.

Definition 1: Consider system (1) and sets $\mathcal{X}_0, \mathcal{X}_u \subseteq \mathcal{X}$. A function $B : \mathcal{X} \to \mathbb{R}$ is called a barrier function for Σ if there exist $\gamma, \sigma \in \mathbb{R}$ with $\gamma < \sigma$ such that

$$B(x) \leq \gamma, \qquad \forall x \in \mathcal{X}_0, \tag{2a}$$

$$B(x) \geq \sigma, \qquad \forall x \in \mathcal{X}_u, \tag{2b}$$

$$B(g(x)) \leq B(x), \qquad \forall x \in \mathcal{X}. \tag{2c}$$

Our main goal here is to compositionally verify safety of the system. Therefore, we assume that system Σ is expressed as an interconnection of ℓ subsystems Σ_i:

$$\Sigma_i : x_i^+ = g_i(x_i, w_i) \tag{3}$$

where states $x_i \in \mathcal{X}_i \subseteq \mathbb{R}^{n_i}$, internal inputs $w_i \subseteq \mathcal{W}_i \in \mathbb{R}^{p_i}$, $\mathcal{X} = \prod_{i=1}^{\ell} \mathcal{X}_i$, and $\mathcal{W} = \prod_{i=1}^{\ell} \mathcal{W}_i$. The static interconnection matrix $M \in \mathbb{R}^{n\times p}$, where $n = \sum_{i=1}^{\ell} n_i$ and $p = \sum_{i=1}^{\ell} p_i$, characterizes the way subsystems Σ_i are connected to each other, i.e., $(w_1, \ldots, w_\ell) = M(x_1, \ldots, x_\ell)$.

Accordingly, we assume the initial and unsafe sets are partitioned as $\mathcal{X}_0 = \prod_{i=1}^{\ell} \mathcal{X}_{0i}$ and $\mathcal{X}_u = \prod_{i=1}^{\ell} \mathcal{X}_{ui}$, $\mathcal{X}_{0i}, \mathcal{X}_{ui} \subseteq \mathcal{X}_i$. Now we propose a notion of so-called sub-barrier functions for subsystems Σ_i. These functions will later be used to build barrier functions as in Definition 1 for the whole interconnected system Σ.

Definition 2: Consider subsystem Σ_i in (3) and sets $\mathcal{X}_{0i}, \mathcal{X}_{ui} \subseteq \mathcal{X}_i$. A function $B_i : \mathcal{X}_i \to \mathbb{R}$ is called a sub-barrier function for Σ_i if there exist matrix $X_i \in \mathbb{R}^{(p_i+n_i)\times(p_i+n_i)}$ with conformal block partitions $X_i^{j,k}$, $j, k \in \{1, 2\}$, and $\gamma_i < 1$ such that

$$B_i(x_i) \leq \gamma_i, \qquad \forall x_i \in \mathcal{X}_{0i}, \tag{4a}$$

$$B_i(x_i) \geq 1, \qquad \forall x_i \in \mathcal{X}_{ui}, \tag{4b}$$

$$B_i(g_i(x_i, w_i)) \leq B_i(x_i) + z_i^\top X_i z_i, \ \forall x_i \in \mathcal{X}_i, w_i \in \mathcal{W}_i, \tag{4c}$$

where

$$X_i = \begin{bmatrix} X_i^{11} & X_i^{12} \\ X_i^{21} & X_i^{22} \end{bmatrix}, z_i = \begin{bmatrix} w_i \\ x_i \end{bmatrix}.$$

The following theorem, borrowed from [17] and adapted to the context of this letter, allows us to construct a barrier certificate as in (1) for Σ from sub-barrier certificates as in (2) for Σ_i.

The proof is analogous to the result given in [17, Th. 3.4] and therefore is not presented here.

Theorem 1: Assume that system Σ is composed of subsystems Σ_i as in (3) with an interconnection matrix M. Also, suppose that for each Σ_i there exists a sub-barrier certificate $B_i : \mathcal{X}_i \to \mathbb{R}$ as in (2). If the following condition is satisfied:

$$\Delta := \begin{bmatrix} M \\ I_p \end{bmatrix}^\top \underbrace{\begin{bmatrix} \mathrm{diag}(X_1^{11}, \ldots, X_\ell^{11}) & \mathrm{diag}(X_1^{12}, \ldots, X_\ell^{12}) \\ \mathrm{diag}(X_1^{21}, \ldots, X_\ell^{21}) & \mathrm{diag}(X_1^{22}, \ldots, X_\ell^{22}) \end{bmatrix}}_{=:X} \begin{bmatrix} M \\ I_p \end{bmatrix} \preceq 0, \tag{5}$$

then the function

$$B(x) = \sum_{i=1}^{\ell} B_i(x_i), \tag{6}$$

is a barrier function for the overall system Σ.

Note that condition (5) is an LMI. To obtain an overall barrier function B using Theorem 1, one needs to know models of subsystems. In this letter, we assume that the systems dynamics (i.e., g_i's) are *unknown*. Instead, we collect N_i independent and identically distributed (i.i.d.) data sampled from $(\mathcal{X}_i, \mathcal{W}_i)$:

$$\mathcal{D}_i := \left(\hat{x}_{il}, \hat{w}_{il}, \hat{x}_{il}^+\right)_{l=1}^{N_i} \subseteq \mathcal{X}_i \times \mathcal{W}_i \times \mathcal{X}_i.$$

In particular, our objective is to construct sub-barrier functions B_i from data collected from subsystems Σ_i.

Remark 1: In our approach, subsystem Σ_i does not necessarily need to exchange information with its neighboring subsystems to collect samples from internal input w_i. In fact, samples can be collected by looking at each subsystem in isolation (i.e., considering w_i as an external input to Σ_i).

III. Compositional Data-Driven Safety Verification

To construct an overall barrier certificate, we show how sub-barrier candidates can be computed from data sets $\mathcal{D}_i$ in Section III-A. These individual barrier functions do not necessarily satisfy LMI (5) required for the overall barrier function. In Section III-B, we use the ADMM algorithm to enforce condition (5) on the parameters associated to sub-barrier functions so that (4) and (5) are simultaneously met.

A. Computation of Sub-Barrier Functions

We represent each sub-barrier function B_i as a linear combination of user-defined basis functions $p_j : \mathbb{R}^{n_i} \to \mathbb{R}$ as follows:

$$B_i(x_i) = \sum_{j=1}^{r_i} q_{ij} p_j(x_i), \tag{7}$$

where coefficients $q_i := (q_{i1}, \ldots, q_{ir_i}) \in \mathbb{R}^{r_i}$ are determined later. Given the basis functions p_j, to enforce conditions (4) on B_i in (7), we reformulate the search for B_i into the following RCP.

Problem 1: Consider subsystem Σ_i in (3). Given sets $\mathcal{X}_i, \mathcal{X}_{0i}, \mathcal{X}_{ui}$ and the structure of B_i as in (7), solve the following problem:

$$\begin{aligned} \min_{\eta_i, \nu_i, X_i} \quad & \eta_i \\ \text{s.t.} \quad & \max_{j\in\{1,2,3\}} c_j(x_i, w_i, \nu_i, X_i) \le \eta_i, \\ & \forall x_i \in \mathcal{X}_i, \forall w_i \in \mathcal{W}_i, \\ & \nu_i := (\gamma_i, q_i), \ \ \gamma_i < 1, \end{aligned} \tag{RCP-i}$$

where

$$\begin{aligned} c_1(x_i, w_i, \nu_i, X_i) &= (B_i(x_i) - \gamma_i)\mathbb{1}_{\mathcal{X}_{0i}}(x_i) \\ c_2(x_i, w_i, \nu_i, X_i) &= (-B_i(x_i) + 1)\mathbb{1}_{\mathcal{X}_{ui}}(x_i) \\ c_3(x_i, w_i, \nu_i, X_i) &= B_i(g_i(x_i, w_i)) - B_i(x_i) - z_i^\top X_i z_i. \end{aligned}$$

Note that a feasible solution to Problem 1 provides a candidate B_i satisfying conditions (4). Observe that constraints (RCP-i) are linear in terms of decision variables. However, it has to be solved for all possible values of $x_i \in \mathcal{X}_i$ and $w_i \in \mathcal{W}_i$. Therefore, RCP-i is of the form of a semi-infinite linear program. Since the system model (i.e., map g_i) is unavailable, we *cannot* directly solve (RCP-i). These challenges motivate us to employ data-driven approaches and propose a scenario convex program (SCP) of RCP-i. The crucial step is to provide an error bound between the optimal solution of (RCP-i) and that of the corresponding SCP. Below is the scenario convex problem associated to (RCP-i).

Problem 2: Consider subsystem Σ_i in (3). Given sets $\mathcal{X}_i, \mathcal{X}_{0i}, \mathcal{X}_{ui}$, data set $\mathcal{D}_i$, and the structure of B_i as in (7), solve the following problem:

$$\begin{aligned} \min_{\eta_i, \nu_i, X_i} \quad & \eta_i \\ \text{s.t.} \quad & \max_{j\in\{1,2,3\}} c_j(\hat{x}_{il}, \hat{w}_{il}, \nu_i, X_i) \le \eta_i, \\ & \nu_i := (\gamma_i, q_i), \ \ \gamma_i < 1, \ \ \forall (\hat{x}_{il}, \hat{w}_{il}, \hat{x}_{il}^+) \in \mathcal{D}_i, \end{aligned} \tag{SCP-i}$$

with c_j's as in (RCP-i). Note that the last constraint will be of the form: $c_3(\hat{x}_{il}, \hat{w}_{il}, \nu_i, X_i) = B_i(\hat{x}_{il}^+) - B_i(\hat{x}_{il}) - z_i^\top X_i z_i$.

Following [16, Th. 5.2], we provide a probabilistic closeness between the optimal value of (RCP-i), denoted by $\eta^*_{\mathrm{RCP-i}}$, and that of (SCP-i), denoted by $\eta^*_{\mathrm{SCP-i}}(\mathcal{D}_i)$. In particular, this is given based on the minimum number of data N_i and the probabilistic confidence parameter denoted by β_i, cf. (8) below. To this end, we make the following regularity assumption on functions c_j in (RCP-i).

Assumption 1: Functions $c_j : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{r_i+1} \times \mathbb{R}^{(p_i+n_i)^2} \to \mathbb{R}$, $j = 1, 2, 3$, are locally Lipschitz with respect to the first two arguments, uniformly in the others, with the corresponding Lipschitz constants $L_j > 0$, $j = 1, 2, 3$.[1]

Remark 2: As shown in [16, Lemma 5.4], one can compute Lipschitz constants $L_j, j = 1, 2, 3$, (or their upper bounds) by assuming continuous differentiability of the system dynamics g_i and bounding the coefficients q_i in (7). The latter can be ensured by enforcing extra constraints over q_i in SCP-i. We further discuss this point in Section IV.

Now we propose the first result of this letter.

[1]To avoid notational burden, we consider the same Lipschitz constants $L_j, j = 1, 2, 3$, for all RCP-i, $i \in \{1, \ldots, \ell\}$.

Theorem 2: Consider subsystem Σ_i and associated sets $\mathcal{X}_i, \mathcal{X}_{0i}$ and $\mathcal{X}_{ui}$. Let Assumption 1 hold with Lipschitz constants L_j, $j = 1, 2, 3$. Also, let $\epsilon_i, \beta_i \in [0, 1]$ with $\epsilon_i \leq L := \max\{L_1, L_2, L_3\}$, $\bar{\epsilon}_i := (\frac{\epsilon_i}{L})^{n_i}$ and $s_i := r_i + 1 + (p_i + n_i)^2$. If $N_i \geq N(\bar{\epsilon}_i, \beta_i)$, where

$$N(\bar{\epsilon}_i, \beta_i) := \min\left\{\tilde{n} \in \mathbb{N} \mid \sum_{j=0}^{s_i} \binom{\tilde{n}}{j} \bar{\epsilon}_i^j (1-\bar{\epsilon}_i)^{\tilde{n}-j} \leq \beta_i\right\}, \quad (8)$$

and $\eta^*_{\text{SCP-i}} + \epsilon_i \leq 0$, then function B_i obtained from solving Problem 2 satisfies conditions (4) with a confidence of at least $1 - \beta_i$.

Proof: From [9, Th. 3.6], one has

$$\mathbb{P}^{N_i}\left[\eta^*_{\text{RCP-i}} - \eta^*_{\text{SCP-i}}(\mathcal{D}_i) \in [0, \epsilon_i]\right] \geq 1 - \beta_i,$$

for any $N_i \geq N((\frac{\epsilon_i}{L_{sp}L})^{n_i}, \beta_i)$, where L_{sp} is a Slater constant as defined in [9, eq. (5)]. Since (RCP-i) can be cast as a min-max optimization problem, the constant L_{sp} can be selected as 1 [9, Remark 3.5]. The number of decision variables in the original RCP-i is $r_i + 2 + (p_i + n_i)^2$. This leads to the expression (8) for the minimum required number of samples according to [9, eq. (3)]. Now, one can readily conclude that for any $N_i \geq N(\bar{\epsilon}_i, \beta_i)$, we have

$$\mathbb{P}^{N_i}\left[\eta^*_{\text{RCP-i}} \leq \eta^*_{\text{SCP-i}}(\mathcal{D}_i) + \epsilon_i\right] \geq 1 - \beta_i. \quad (9)$$

Since $\eta^*_{\text{SCP-i}} + \epsilon_i \leq 0$, inequality (9) implies that $\eta^*_{\text{RCP-i}}$ is non-positive with a confidence of at least $1-\beta_i$, which ensures satisfaction of conditions (4) with a confidence of at least $1 - \beta_i$. This completes the proof. ∎

The above result only gives certain confidences on the correctness of sub-barrier functions obtained from SCP-i, while we need to ensure that their summations give an overall barrier function for network Σ with some confidence. The following theorem provides such a confidence bound for the overall barrier function B, which provides the desired out-of-sample safety guarantee for the overall network Σ.

Theorem 3: Consider network Σ and associated sets $\mathcal{X}, \mathcal{X}_0$ and $\mathcal{X}_u$. Suppose that for each subsystem Σ_i all assumptions in Theorem 2 are satisfied. In addition, assume that all X_i, $i = 1, \ldots, \ell$, computed from (SCP-i), satisfy (5). Then, function B in (6) is a barrier function for Σ with a confidence of at least $1-\sum_{i=1}^{\ell} \beta_i$, where β_i are the confidence parameters associated with B_i as in Theorem 2.

Proof: Recalling the proof of Theorem 2, for each subsystem Σ_i, $i \in \{1, \ldots, \ell\}$, one has $\mathbb{P}^{N_i}[\eta^*_{\text{RCP-i}} \leq \eta^*_{\text{SCP-i}}(\mathcal{D}_i) + \epsilon_i] \geq 1-\beta_i$. We define an event $\mathcal{A}_i$ whose occurrence is equivalent to having a data set $\mathcal{D}_i$ such that a solution to SCP-i also solves RCP-i with a probability of at least $1 - \beta_i$. Thus, we define $\mathcal{A}_i := \{\mathcal{D}_i \mid \eta^*_{\text{SCP-i}}(\mathcal{D}_i) + \epsilon_i \leq 0\}$, $i = 1, \ldots, \ell$. As for the overall network, we need all these ℓ events to simultaneously hold. Thus we obtain a probability lower bound on the intersection of these events. From probability theory, one can easily get the following inequality:

$$\mathbb{P}\left[\bigcap_{i=1}^{\ell} \mathcal{A}_i\right] \geq 1 - \mathbb{P}[\mathcal{A}_1] - \cdots - \mathbb{P}[\mathcal{A}_\ell]$$
$$\geq 1 - \beta_1 - \cdots - \beta_\ell = 1 - \sum_{i=1}^{\ell} \beta_i,$$

which completes the proof. ∎

B. Computation of the Overall Barrier Function

According to Theorem 2, solutions to (SCP-i) provide a set of sub-barrier functions B_i with a priori given confidence bounds. However, matrices X_i associated to these functions may not necessarily satisfy (5). To address this issue, we exploit the ADMM algorithm to formulate our problem into a set of local conditions aiming at solving (SCP-i) individually and a global condition enforcing condition (5). To do so, we define the following local constraints:

$$\mathcal{L}_i := \{(\eta_i, \nu_i, \mathcal{X}_i): \max_{j\in\{1,2,3\}} c_j(\hat{x}_{il}, \hat{w}_{il}, \nu_i, X_i) \leq \eta_i, \ \forall(\hat{x}_{il}, \hat{w}_{il}, \hat{x}^+_{il}) \in \mathcal{D}_i\}. \quad (10)$$

In addition, the global constraint is given by:

$$\mathcal{G} := \{(X_1, \ldots, X_\ell): (5) \text{ holds}\}. \quad (11)$$

The following indicator functions are also needed to represent the problem in a standard ADMM form:

$$\mathbb{1}_{\mathcal{L}_i}(\eta_i, \nu_i, X_i) := \begin{cases} 0 & (\eta_i, \nu_i, X_i) \in \mathcal{L}_i, \\ +\infty & \text{otherwise}, \end{cases} \quad (12)$$

and

$$\mathbb{1}_{\mathcal{G}}(X_1, \ldots, X_\ell) := \begin{cases} 0 & (X_1, \ldots, X_\ell) \in \mathcal{G}, \\ +\infty & \text{otherwise}. \end{cases} \quad (13)$$

Now by introducing auxiliary variables $Z_i \in \mathbb{R}^{(p_i+n_i)\times(p_i+n_i)}$, $i = 1, \ldots, \ell$, we write the following optimization problem in a standard canonical form.

Problem 3: Consider network Σ in (1). Given sets $\mathcal{X}_i, \mathcal{X}_{0i}, \mathcal{X}_{ui}$, data sets $\mathcal{D}_i$, and the structure of B_i as in (7), solve the following problem:

$$\min_{\substack{\eta_i, \nu_i, X_i, Z_i, \\ i\in\{1,\ldots,\ell\}}} \sum_{i=1}^{\ell} \left(\eta_i + \mathbb{1}_{\mathcal{L}_i}(\eta_i, \nu_i, X_i)\right) + \mathbb{1}_{\mathcal{G}}(Z_1, \ldots, Z_\ell)$$
$$\text{s.t. } X_i - Z_i = 0. \quad (14)$$

We note that Problem 3 is a convex program with a standard canonical structure which allows for the use of typical distributed convex optimization algorithms. To solve Problem 3, we use the ADMM algorithm [10] which updates the essential variables at each iteration k as follows:

1) For each $i \in \{1, \ldots, \ell\}$, solve the local problem:
$$(\eta_i^{k+1}, \nu_i^{k+1}, X_i^{k+1}) \in \underset{\eta_i^*, \nu_i^*, X_i^* \in \mathcal{L}_i}{\text{argmin}} \ \eta_i^* + ||X_i^* - Z_i^k + \Lambda_i^k||_F^2;$$
2) if $(X_1^{k+1}, \ldots, X_\ell^{k+1}) \in \mathcal{G}$, we successfully terminate the algorithm. Otherwise, solve the global problem:
$$(Z_1^{k+1}, \ldots, Z_\ell^{k+1}) \in \underset{Z_1^*, \ldots, Z_\ell^* \in \mathcal{G}}{\text{argmin}} \sum_{i=1}^{\ell} ||X_i^{k+1} - Z_i^* + \Lambda_i^k||_F^2;$$
3) Update the so-called dual variables Λ_i as:
$$\Lambda_i^{k+1} = X_i^{k+1} - Z_i^{k+1} + \Lambda_i^k,$$
and return to (i).

Algorithm 1 Compositional Data-Driven Safety Verification of Network Σ

Input: $\beta_i \in [0,1]$, $Z_i^0 \in \mathbb{R}^{(p_i+n_i)\times(p_i+n_i)}$, $\Lambda_i^0 \in \mathbb{R}^{(p_i+n_i)\times(p_i+n_i)}$, $i=1,\ldots,\ell$, $L := \max\{L_1,L_2,L_3\}$, $M \in \mathbb{R}^{n\times p}$, $k=0$.

Output: η_i, ν_i, X_i, $i=1,\ldots,\ell$.

1 Choose $\epsilon_i \leq L$.
2 Compute the minimum number of samples $N_i \geq N(\bar{\epsilon}_i, \beta_i)$ as in (8).
3 **foreach** $i \in \{1,\ldots,\ell\}$ **do**
4 $(\eta_i^{k+1}, \nu_i^{k+1}, X_i^{k+1}) \in \underset{\eta_i^*,\nu_i^*,X_i^*\in\mathcal{L}_i}{\operatorname{argmin}} \eta_i^* + ||X_i^* - Z_i^k + \Lambda_i^k||_F^2$.
5 **end**
6 **if** $(X_1^{k+1},\ldots,X_\ell^{k+1}) \notin \mathcal{G}$ **then**
7 $(Z_1^{k+1},\ldots,Z_\ell^{k+1}) \in \underset{Z_1^*,\ldots,Z_\ell^*\in\mathcal{G}}{\operatorname{argmin}} \sum_{i=1}^{\ell} ||X_i^{k+1} - Z_i^* + \Lambda_i^k||_F^2$.
8 Compute $\Lambda_i^{k+1} = X_i^{k+1} - Z_i^{k+1} + \Lambda_i^k$.
9 $k = k+1$.
10 Return to **3**
11 **else**
12 Break and go to **14**.
13 **end**
14 $\eta_i = \eta_i^k$, $\nu_i = \nu_i^k$, $X_i = X_i^k$ for all $i \in \{1,\ldots,\ell\}$.

Algorithm 1 summarizes the steps that are needed for the implementation of our compositional data-driven approach by each individual subsystem.

Remark 3: We note that one needs to feed Algorithm 1 with the Lipschitz constants $L_j, j=1,2,3$. If the dynamics g_i's are continuously differentiable, using [16, Lemma 5.4], one can compute $L_j, j=1,2,3$. In this lemma, a quadratic barrier candidate is considered. However, this choice of barrier candidates is not restrictive as any polynomial function can be cast as a quadratic function of monomials.

IV. Example

Here we verify the effectiveness of Algorithm 1 by applying it to a room temperature problem in a circular building. The overall system is described by

$$x(k+1) = Ax(k) + \alpha_e T_E + \alpha_h T_h u(k),$$

where $A \in \mathbb{R}^{\ell\times\ell}$ is a circulant matrix with $\{A\}_{ii} = 1-2\alpha-\alpha_e-\alpha_h u_i(k)$, $\{A\}_{i(i+1)} = \{A\}_{(i+1)i} = \{A\}_{1\ell} = \{A\}_{\ell 1} = \alpha$ for all $i \in \{1,\ldots,\ell-1\}$, and all other components are zero. Here, $x \in \mathbb{R}^\ell$ is the state vector, $u \in \mathbb{R}^\ell$ is the control input vector, $T_E \in \mathbb{R}^\ell$ is a constant vector containing the external temperature, $T_h > 0$ is the heater temperature, and $\alpha, \alpha_e, \alpha_h > 0$ are the heat exchange coefficients.

The state set is $\mathcal{X} = [19,28]^\ell$, the initial set is $\mathcal{X}_0 = [20.5,22.5]^\ell$, and the unsafe set is $\mathcal{X}_u = [24,28]^\ell$. Assume $T_{E_i} = 15°C$ for all $i \in \{1,\ldots,\ell\}$, $T_h = 55°C$, $\alpha = 5\times10^{-2}$, $\alpha_e = 8\times10^{-3}$, and $\alpha_h = 3.6\times10^{-3}$. We consider controllers $u_i(x_i) = -0.002398x_i + 0.5357$ as designed in [18]. It was shown in [18, Sec. 6.1] that state trajectories of the closed-loop system starting from $\mathcal{X}_0 = [20.5,22.5]^\ell$ will not enter the unsafe set $\mathcal{X}_u = [24,28]^\ell$. We aim to verify this safety property under the assumption that the model of the closed-loop system is unavailable.

By decomposing the closed-loop system into ℓ subsystems, we have

$$\Sigma_i : x_i(k+1) = ax_i(k) + \alpha_e T_{E_i} + 0.5357\alpha_h T_h + \alpha w_i(k), \tag{15}$$

where $a = 1-2\alpha-\alpha_e+\alpha_h(0.002398x_i - 0.5357) - 0.002398\alpha_h^2 T_h$, and $w_i = x_{i-1} + x_{i+1}$, $i = 2,\ldots,\ell-1$, $w_1 = x_2 + x_\ell$, and $w_\ell = x_1 + x_{\ell-1}$. The interconnection matrix M is circulant whose components are given by $\{M\}_{i(i+1)} = \{M\}_{(i+1)i} = \{M\}_{1\ell} = \{M\}_{\ell 1} = 1$ for all $i \in \{1,\ldots,\ell-1\}$, and all other components are zero.

Let the network be composed of $\ell = 100$ subsystems. Taking the basis functions $p_j(x_i) = x_i^{j-1}$, $j \in \{1,2,3\}$, in (7), the sub-barrier candidates are expressed as $B_i(x_i) = \sum_{j=1}^3 q_{ij} x_i^{j-1}$, $i=1,\ldots,\ell$. Recalling Algorithm 1, we need to feed the algorithm with β_i's and L as input. We pick the confidence parameter $\beta_i = 10^{-3}$ for all $i \in \{1,\ldots,\ell\}$. Using Remark 2, to compute Lipschitz constants $L_j, j=1,2,3$, in Assumption 1, we assume that the Lipschitz constant associated with the dynamics of each subsystem in (15) is given and is equal to 2. We also assume $|\frac{\partial g_i}{\partial x}| \leq 1$. Then, by assuming $|q_i|_\infty \leq 15$ and using [16, Lemma 5.4], the Lipschitz constant L is calculated as 468. We also pick $\epsilon_i = 1$ which clearly satisfies $\epsilon_i \leq L$. From (8), the minimum number of data samples is calculated as $N(1/468, 10^{-3}) = 17474$ for each subsystem. As discussed earlier, we exploit the ADMM algorithm for computation of the sub-barrier functions and associated parameters. In particular, each local convex problem (i.e., Step 4 of Algorithm 1) is solved by CVX [19] and the global problem (i.e., Step 8 of Algorithm 1) is solved by YALMIP [20], where both software packages run in MATLAB. In each local convex problem $\mathcal{L}_i$ in (10), we enforce extra conditions $|q_i|_\infty \leq 15$ on the coefficients q_i associated to the sub-barrier functions B_i. This ensures that the a priori specified assumption $L \leq 468$ is not violated. The ADMM algorithm converges after six steps. On an iMac with 3.5 GHz Quad-Core Intel Core i7 and 32 GB RAM, our algorithm converges in 380 seconds on average. From (8), one can observe that N_i grows exponentially with the system's dimension. Moreover, the number of constraints in (SCP-i) is proportional to N_i. These clearly affect the overall computational complexity. To show the effectiveness of our approach over the one in [16], Table I reports the minimum number of data required to solve the corresponding SCP in [16] for various network sizes, with the same overall confidence parameter $\beta = 0.01$. In this table, $\lfloor\cdot\rfloor$ denotes the floor function. As seen, the method in [16] is not practically applicable to networks with more than 2 subsystems. On the contrary, our method breaks the computational complexity to the level of subsystems and, hence, it is independent of the network's size. We only need to globally solve LMI (5), which is possible for large networks in practice.

Given that the system is spatially invariant with identical dynamics, the sub-barrier functions are computed identically as $B_i(x_i) = 0.6466x_i^2 + 14.81x_i + 14.5$. The other decision

TABLE I
THE MINIMUM NUMBER OF COLLECTED DATA IN [16]

ℓ	2	4	10	50	100
$\lfloor \log_{10}(N) \rfloor$	7	13	30	139	275

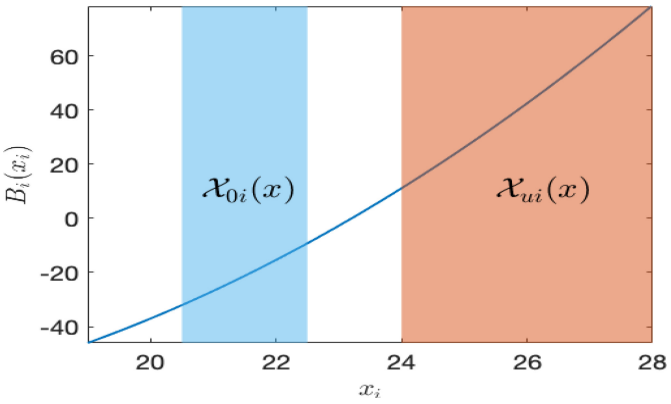

Fig. 1. The solid, blue line draws sub-barrier function B_i for any $i = 1, \ldots, 100$. The light blue and light red regions, respectively, represent the initial and unsafe sets.

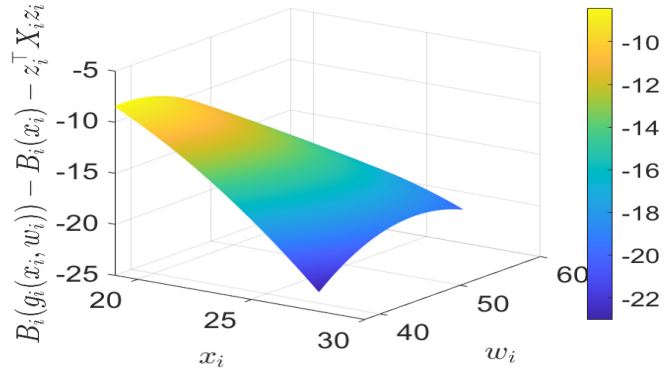

Fig. 2. Illustration of the decay condition (4c) for sub-barrier function B_i, $i = 15$, where $z_i = (w_i, x_i)$.

variables are also identically computed as $\eta^*_{\text{SCP}-\text{i}}(\mathcal{D}_i) = -10$ and $\gamma_i = 0.95$. As $\eta^*_{\text{SCP}-\text{i}} + \epsilon_i \leq 0$ for each $i \in \{1, \ldots, \ell\}$, from Theorem 2 the computed functions B_i can be considered as sub-barrier functions with a confidence of at least 0.999. The sub-barrier function B_{15} is depicted in Fig. 1 as a representative. Conditions (4a) and (4b) are clearly satisfied. Since sub-barrier functions are identical, the same conclusion is obtained for all other sub-barrier functions. This implies that the constructed overall barrier function which is the sum of sub-barrier functions have the same properties, i.e., conditions (2a) and (2b) are clearly fulfilled with $\mathcal{X}_0 = [20.5, 22.5]^{100}$ and $\mathcal{X}_u = [24, 28]^{100}$. Condition (4c) is also illustrated in Fig. 2 for the representative sub-barrier function B_{15}, where matrix X_{15} is computed as:

$$X_{15} = \begin{bmatrix} 0.0627 & 0.0445 \\ -0.0105 & -0.1264 \end{bmatrix}.$$

This figure illustrates that for all possible values of states within $\mathcal{X}_{15} = [19, 28]$ and of internal inputs within $\mathcal{W}_{15} = [38, 56]$, the decay condition (4c) is satisfied. The other matrices X_i are not presented here due to the space constraints. Nevertheless, we remark that the computed matrices X_i result in a negative definite matrix Δ as in (5) with the largest eigenvalue being equal to -0.4681, which implies that the global compositionality condition (5) holds. Since the overall barrier function is the sum over sub-barrier ones, this together with the satisfaction of condition (4c) imply that the decay condition (2c) holds. Thus, from Theorem 3, function B in (6) is a barrier function for the overall network with a confidence of at least 0.9.

REFERENCES

[1] H. Ravanbakhsh and S. Sankaranarayanan, "Learning control Lyapunov functions from counterexamples and demonstrations," *Auton. Robots*, vol. 43, no. 2, pp. 275–307, 2019.

[2] S. Sadraddini and C. Belta, "Formal guarantees in data-driven model identification and control synthesis," in *Proc. 21st Int. Conf. Hybrid Syst. Comput. Control (HSCC)*, 2018, pp. 147–156.

[3] E. Bartocci, L. Bortolussi, and G. Sanguinetti, "Data-driven statistical learning of temporal logic properties," in *Proc. Int. Conf. Formal Model. Anal. Timed Syst. (FORMATS)*, 2014, pp. 23–37.

[4] A. Rubbens, Z. Wang, and R. M. Jungers, "Data-driven stability analysis of switched linear systems with sum of squares guarantees," in *Proc. 7th IFAC Conf. Anal. Design Hybrid Syst. (ADHS)*, 2021, pp. 1–8.

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

[6] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *Proc. 18th Eur. Control Conf.*, 2019, pp. 3420–3431.

[7] M. Z. Romdlony and B. Jayawardhana, "Robustness analysis of systems' safety through a new notion of input-to-state safety," *Int. J. Robust Nonlinear Control*, vol. 29, no. 7, pp. 2125–2136, 2019.

[8] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 3861–3876, Aug. 2017.

[9] P. M. Esfahani, T. Sutter, and J. Lygeros, "Performance bounds for the scenario approach and an extension to a class of non-convex programs," *IEEE Trans. Autom. Control*, vol. 60, no. 1, pp. 46–58, Jan. 2015.

[10] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," in *Foundations and Trends in Machine Learning*, vol. 3. Hanover, MA, USA: Now Publishers, Jan. 2011, pp. 1–122.

[11] S. Han, U. Topcu, and G. J. Pappas, "A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems," in *Proc. 54th IEEE Conf. Decis. Control (CDC)*, 2015, pp. 2049–2054.

[12] M. Ahmadi, A. Israel, and U. Topcu, "Safe controller synthesis for data-driven differential inclusions," *IEEE Trans. Autom. Control*, vol. 65, no. 11, pp. 4934–4940, Nov. 2020.

[13] A. Robey *et al.*, "Learning control barrier functions from expert demonstrations," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, 2020, pp. 3717–3724.

[14] P. Jagtap, G. J. Pappas, and M. Zamani, "Control barrier functions for unknown nonlinear systems using Gaussian processes," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, 2020, pp. 3699–3704.

[15] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE Trans. Autom. Control*, vol. 51, no. 5, pp. 742–753, May 2006.

[16] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems," in *Proc. 7th IFAC Conf. Anal. Design Hybrid Syst. (ADHS)*, 2021, pp. 7–12.

[17] M. Anand, A. Lavaei, and M. Zamani, "Compositional synthesis of control barrier certificates for networks of stochastic systems against ω-regular specifications," 2021, *arXiv:2103.02226*.

[18] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in *Proc. 23rd Int. Conf. Hybrid Syst. Comput. Control (HSCC)*, 2020.

[19] M. Grant, S. Boyd, and Y. Ye, *Disciplined Convex Programming*. Boston, MA, USA: Springer, 2006, pp. 155–210.

[20] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2004, pp. 284–289.