Compositional Verification for Large-Scale Systems via Closure Certificates

Felipe Galarza-Jimenez, *Graduate Student Member, IEEE*, Vishnu Murali, *Graduate Student Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*—Closure certificates (CCs), function analogs of transition invariants, provide a framework to verify discrete-time dynamical systems against ω-regular specifications. Such certificates are similar to barrier certificates (BCs) yet are less conservative than BCs when leveraged to verify $\omega-$regular properties. However, CCs are defined over pairs of states of the system rather than over the state of the system, and seek to overapproximate the transitive closure of the transition relation. Thus, finding these certificates is often harder and computationally more demanding than BCs, especially for large-scale systems. To address this challenge, we propose a dissipativity-inspired approach to construct closure certificates for interconnected systems. In such a setting, we assume our large-scale system to be an interconnection of subsystems under a linear map. We then find local certificates for these subsystems. These local certificates are then composed to form a closure certificate for the interconnected system, acting as proof of the satisfaction of a desired ω-regular specification. Finally, we illustrate our approach with a numerical simulation.**

***Index Terms*—Verification, omega-regular specifications, compositionality, interconnected systems, dissipativity.**

I. Introduction

Closure certificates (CCs) proposed in [1] are a technique to verify dynamical systems against ω-regular specifications. These certificates seek to overapproximate the transitive closure of the transition relation of a system by characterizing all elements in this set as being above a level set of a function. Imposing a well-foundedness argument on such a function acts as a proof that a set of accepting states are visited finitely often and can thus be used to verify ω-regular specifications [2]. As CCs capture the behavior of system transitions, they are defined over *pairs* of system states. Thus, using conventional approaches such as sum-of-squares (SOS) [3] solvers to find such a function is computationally challenging as the dimension grows. To address this, we present a compositional approach to synthesize CCs for large-scale systems modeled as interconnections of subsystems.

Contributions: In this letter, we propose a compositional approach to construct CCs to verify large-scale systems against safety and more general ω-regular specifications described by Universal co-Büchi Automata (UCA). Here, we assume that the large-scale system can be modeled as an interconnection of smaller subsystems connected via a linear map. We construct a product of the system and the UCA and project the product onto these subsystems. We then provide local certificates for these projections. The conditions of these local certificates rely on strengthening the conditions of a CC to make them amenable to easy composition. We then compose these local certificates to form a CC for the interconnected system using a dissipativity-inspired approach. This allows us to provide a proof that the large-scale system satisfies a given ω-regular specification.

Related work: One approach to verify dynamical systems against ω-regular specifications leverages abstraction-based methods [4], where one quantizes the state set to create a finite-state abstraction. Then, ensuring that the abstraction satisfies the specification also provides a guarantee for the original system. Although such methods are easily automatable, they suffer from the *curse of dimensionality*. The construction of such an abstraction suffers exponentially as the system dimension grows. To address this issue, one can lean towards a compositional approach to construct abstractions [5], or instead, may use abstraction-free approaches. One such approach is the use of *barrier certificates* (BCs) [6] to prove safety of dynamical systems.

The success of BCs has inspired their use in proving ω-regular specifications given by automata. The authors of [7] presented a "triplets" approach that decomposes the specification into a finite collection of straightforward safety constraints. To do so, they partition consecutive automaton transitions or "triplets" of states and form safety arguments over these. Even though there are works that address the problem of computing such BCs for large-scale systems (see [8], [9] and references therein), this approach is potentially conservative; i.e., even though the system satisfies the specification, one cannot always find the required BC that guarantees its satisfaction [10], [11]. The result in [12] proposed a notion of *co-Büchi barrier certificates* (CBBC) that acts as proof that the accepting states of the automaton are

Manuscript received 8 March 2024; revised 16 May 2024; accepted 4 June 2024. Date of publication 7 June 2024; date of current version 17 September 2024. This work was supported in part by NSF under Grant CNS-2039062 and Grant CNS-2111688, and in part by CAREER Grant under Grant CNS-2145184. Recommended by Senior Editor V. Ugrinovskii. *(Corresponding author: Felipe Galarza-Jimenez.)*

The authors are with the Department of Computer Science, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: felipe.galarzajimenez@colorado.edu; vishnu.murali@colorado.edu; majid.zamani@colorado.edu).

Digital Object Identifier 10.1109/LCSYS.2024.3411508

visited only finitely often by keeping track of the number of visitations via a *counter*. This approach is inspired by bounded verification and synthesis approaches [13], [14]. Here, one selects an a priori upper bound for the counter and tries to prove that the counter value never exceeds the upper bound via a safety argument. If the CBBC is not found, the upper bound may be iteratively increased until a desired certificate is found, providing a more general framework than the one provided by the "triplets" approach. Moreover, the results in [15] provide a compositional approach for large-scale systems using CBBC, addressing the time complexity issues. Similar to how BCs act as function analogs of state invariants, the CCs act as function analogs of *transition invariants*. Transition invariants were introduced in [2] as a framework to verify program termination and programs against ω-regular specifications. This approach has since been implemented to demonstrate program termination [16], [17], and has also seen use in the verification of stability and safety for hybrid systems [18], [19]. The use of CCs deals with the conservatism of the "triplets" approach while simultaneously removing the necessity of fixing an a priori bound on the number of visitations. Though CCs may provide flexibility and benefits over BCs and CBBCs in specific scenarios, their computation becomes intractable for large-scale systems as they are defined over pairs of system states rather than over states of the system directly.

II. Notation and Preliminaries

We denote by $\mathbb{N}$ and $\mathbb{R}$ the natural (including zero) and the real numbers. Given $a \in \mathbb{R}$, we use $\mathbb{N}_{\geq a}$ (resp. $\mathbb{R}_{\geq a}$) to denote all values in $\mathbb{N}$ (resp. $\mathbb{R}$) greater than or equal to a. Notations $[a, b]$, $]a, b[$, $[a, b[$, and $]a, b]$ denote closed, open, and half-open sets in $\mathbb{R}$. Likewise, $[a; b]$, $]a; b[$, $[a; b[$ and $]a; b]$ denote closed, open, and half-open sets in $\mathbb{N}$. Given sets $X_1, \ldots, X_m$, for some $m \in \mathbb{N}_{\geq 1}$, we denote the product by $X_1 \times X_2 \times \ldots \times X_m$, or more compactly by $\prod_{i=1}^{m} X_i$. Moreover, we denote an element $(x_1, \ldots, x_m) \in \prod X_i$ of the product set by $\prod x_i$, where $x_i \in X_i$ for all $i \in [1; m]$. Similarly, we denote the projection of $x \in X$ on the subset X_i by $\text{proj}_i(x) = x_i$. Note that we drop the counter index from the product when it is clear from the context. Given sets A and B, we represent the set difference as $A \backslash B := \{x \in A \mid x \notin B\}$. We use $f : A \rightrightarrows B$ to denote a *set-valued map*, whereas $f : A \to B$ denotes a *single-valued map*. Additionally, we use $f(A)$ to denote the set $\{f(a) \in B \mid \text{ for all } a \in A\}$. Given a set A, we denote the set of infinite-length sequences $A^\omega := \{s \mid s = \langle a_0, a_1, \ldots \rangle$ s.t. $a_0, a_1, \ldots \in A\}$. We say that an infinite sequence $s \in A^\omega$ visits $a \in A$ at most k times if there are k distinct indices $i \in \mathbb{N}$ such that $a_i = a$ with a_i appearing in s. Let $\mathsf{Inf}(s)$ be the set of elements $a \in A$ that occur infinitely many times in s. Lastly, a symmetric real matrix P is called *negative semidefinite* and denoted by $P \preceq 0$ if all its eigenvalues are non-positive.

A. Universal co-Büchi Automata

In this letter, we consider specifications or properties expressed by universal co-Büchi automata defined as follows.

Definition 1: A universal co-Büchi automaton [20] (UCA) is a tuple $\mathcal{A} = (Q, Q_0, Q_a, \delta, \Sigma)$, where Q is a finite set of states, $Q_0 \subseteq Q$ is the set of initial states, Q_a is the set of final or accepting states, Σ is a finite alphabet, and $\delta : Q \times \Sigma \rightrightarrows Q$ is a transition map. A run of the UCA $\mathcal{A}$ over a word $\mathbf{s} = \langle \sigma_0, \sigma_1, \sigma_2, \ldots \rangle \in \Sigma^\omega$ is an infinite state sequence $\mathbf{q} = \langle q_0, q_1, q_2, \ldots \rangle \in Q^\omega$ with $q_0 \in Q_0$ and $q_{i+1} \in \delta(q_i, \sigma_i)$. We say that an infinite word $\mathbf{s} = \langle \sigma_0, \sigma_1, \ldots \rangle \in \Sigma^\omega$ is accepted by $\mathcal{A}$ if for every run $\mathbf{q}$ of $\mathcal{A}$ over $\mathbf{s}$, we have $\mathsf{Inf}(\mathbf{q}) \cap Q_a = \emptyset$. We define the language of the UCA $\mathcal{A}$ by the set of words it accepts and denote this by $\mathcal{L}(\mathcal{A})$.

B. Dynamical Systems

We consider large-scale systems that can be decomposed into interconnected subsystems modeled as follows.

Definition 2 (System): A discrete-time dynamical subsystem $\mathcal{S}$ is a tuple $\mathcal{S} = (X, X_0, W, f, Y, h)$, where X is the state set, $X_0 \subseteq X$ is the set of initial states, W the internal input set, Y the output set, $f : X \times W \to X$ is the transition function, and $h : X \to Y$ is the output map. The state evolution of $\mathcal{S}$ and the output are given by

$$\mathbf{x}(t+1) = f(\mathbf{x}(t), \mathbf{w}(t)), \text{ and } \mathbf{y}(t) = h(\mathbf{x}(t)), \tag{1}$$

respectively, where $\mathbf{x} \in X^\omega$ with $\mathbf{x}(0) \in X_0$, $\mathbf{w} \in W^\omega$, and $\mathbf{y} \in Y^\omega$ are called state run, internal input run, and output run, respectively.

The internal input $w \in W$ is leveraged for interconnection with other subsystems. We now define the model of the interconnected as follows.

Definition 3 (Interconnected System): Consider $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$, and a linear interconnection map M of appropriate dimension. The interconnected system is a tuple $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$, whose evolution is described by the difference equation

$$\mathbf{x}(t+1) = f(\mathbf{x}(t)), \tag{2}$$

where $X = \prod_{i=1}^{N} X_i$, $X_0 = \prod_{i=1}^{N} X_{0i}$, and $f(x) = (f_1(x_1, w_1), \ldots, f_N(x_N, w_N))$, where $x = (x_1, \ldots, x_N) \in X$, and the interconnection variables are restricted as $(w_1, \ldots, w_N) = M(y_1, \ldots, y_N)$.

To verify an interconnected system $\mathfrak{I}(\mathcal{S})$ against an ω-regular specification, we associate the state runs of the system with words over an automaton via a labeling function.

Definition 4: Consider an interconnected system $\mathfrak{I}(\mathcal{S})$ composed of $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$ as in Definition 3 and measurable functions $L_i : X_i \to \Sigma_i$. A *labeling function* is defined as $L : X \to \Sigma$ (with $\Sigma = \prod \Sigma_i$) where $L(x) = (L_1(x_1), \ldots, L_N(x_N))$. Moreover, a trace or word associated with a run $\mathbf{x}$ is an infinite sequence $L(\mathbf{x}) = \langle L(\mathbf{x}(0)), L(\mathbf{x}(1)), \ldots \rangle$. We define the set of all such words by $TR(\mathfrak{I}(\mathcal{S}), L)$.

We say that a system $\mathfrak{I}(\mathcal{S})$, under a labeling function L, satisfies a desired ω-regular specification characterized by UCA $\mathcal{A}$, if $TR(\mathfrak{I}(\mathcal{S})), L) \subseteq \mathcal{L}(\mathcal{A})$. In the following section, we discuss how CCs provide a framework for verifying systems against ω-regular specifications.

C. Closure Certificates

To verify whether a system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ satisfies an ω-regular specification, we make use of the notion of closure certificates [1]. Our approach relies on computing local certificates for each subsystem and composing these certificates to form a closure certificate for the system $\mathfrak{I}(\mathcal{S})$. To achieve this, we modify the conditions of CCs to attain our main compositionality result in Section III. First, we demonstrate how CCs can be used to verify the safety of a system with respect to a set of *unsafe states*. We say that an interconnected system $\mathfrak{I}(\mathcal{S})$ as in Definition 3 is *safe* with respect to a set of unsafe states $X_u \subseteq X$, if for every state run $\mathbf{x}$, we have $\mathbf{x}(t) \notin X_u$ for all $t \in \mathbb{N}$.

Definition 5 (Closure Certificate for Safety): Consider an interconnected system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3. Then, a function $\mathbb{T} : X \times X \to \mathbb{R}_{\geq 0}$ is a *Closure Certificate* (CC) for $\mathfrak{I}(\mathcal{S})$ with respect to a *unsafe set* $X_u \subseteq X$ if there exists $\varrho, \vartheta \in \mathbb{R}_{>0}$ with $\varrho < \vartheta$, and constant parameter $\lambda \in \mathbb{R}_{\geq 0}$ such that for all states $x, x' \in X$, $x^+ = f(x)$, and states $x_0 \in X_0$, $x_u \in X_u$ the following holds:

$$\mathbb{T}\big(x, x^+\big) \leq \varrho, \tag{3a}$$

$$\mathbb{T}\big(x, x'\big) \leq \lambda \mathbb{T}\big(x^+, x'\big) + \varrho(1 - \lambda), \tag{3b}$$

$$\mathbb{T}(x_0, x_u) \geq \vartheta. \tag{3c}$$

Notice that there are differences between the definition of CC in [1, Def. 3.1] and the conditions in Definition 5. First, we require $\mathbb{T}$ to be non-negative; hence, we consider bounds ϱ and ϑ for the initial and unsafe states to obtain conditions (3a) and (3c). Moreover, condition (3b) implies $(\mathbb{T}(x^+, x') \leq \varrho) \implies (\mathbb{T}(x, x') \leq \varrho)$ for all $x, x' \in X, x^+ = f(x)$, similar to the implication[1] in [1, eq. (12)]. Observe that one may construct a certificate $\mathbb{T}'(x, x') = -(\mathbb{T}(x, x') - \varrho)$ as in [1, Def. 3.1] from the certificate $\mathbb{T}(x, x')$ in Definition 5. Thus, the existence of such a certificate guarantees the system to be safe [1, Th. 2]. We discuss the utility of the changes to [1, Def. 3.1] after the proof of Theorem 2.

We now illustrate how one may use CCs to verify a system against an ω-regular specification described by a UCA $\mathcal{A}$. Similar to existing automata-theoretic approaches, such a CC depends on the states of the system $\mathfrak{I}(\mathcal{S})$ and the states of the automaton $\mathcal{A} = (Q, Q_0, Q_a, \delta, \Sigma)$. Hence, we define the *product system* $\mathfrak{I}(\mathcal{S}) \times \mathcal{A} = (Z, Z_0, f_{\mathcal{A}})$, where $Z := X \times Q$ denotes the set of states of the product, $Z_0 := X_0 \times Q_0$ denotes the initial set of states, $Z_a := X \times Q_a$ denotes the set of accepting states, and the transition function $f_{\mathcal{A}} : Z \rightrightarrows Z$ denotes the evolution of the system as follows:

$$\mathbf{z}(t+1) \in f_{\mathcal{A}}(\mathbf{z}(t)) := \begin{cases} \mathbf{x}(t+1) = f(\mathbf{x}(t)), \\ \mathbf{q}(t+1) \in \delta(\mathbf{q}(t), L(\mathbf{x}(t))). \end{cases}$$

Now, we state the following definition.

Definition 6 (Closure Certificate for UCA Specifications): Consider a system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3. Let UCA $\mathcal{A} = (Q, Q_0, Q_a, \delta, \Sigma)$, as in Definition 1, represent a desired ω-regular specification, and $L : X \to \Sigma$ denote a labeling function as in Definition 4. Consider the corresponding product $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$. A function $\mathbb{T} : Z \to \mathbb{R}_{\geq 0}$ is a *Closure Certificate for* $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$ if there exist $\varrho, \varsigma \in \mathbb{R}_{>0}$, and constant parameters $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}_{\geq 0}$ such that for all states $z, z' \in Z$, $z^+ \in f_{\mathcal{A}}(z)$, all initial states $z_0 \in Z_0$ and for all accepting states $z_a, z'_a \in Z_a$, the following inequalities hold:

$$\mathbb{T}\big(z, z^+\big) \leq \varrho, \tag{4a}$$

$$\mathbb{T}\big(z, z'\big) \leq \lambda_1 \mathbb{T}\big(z^+, z'\big) + \varrho(1 - \lambda_1), \tag{4b}$$

$$\mathbb{T}(z_0, z_a) - \mathbb{T}\big(z_0, z'_a\big) \leq \lambda_2 \mathbb{T}(z_0, z_a) + \lambda_3 \mathbb{T}\big(z_a, z'_a\big) - (\varsigma + \lambda_2 \varrho + \lambda_3 \varrho). \tag{4c}$$

The conditions in (4) strengthen those given in [1, Def. 3.3] while also requiring $\mathbb{T}$ to be non-negative. We note that condition (4b) implies $(\mathbb{T}(z^+, z') \leq \varrho) \implies (\mathbb{T}(z, z') \leq \varrho)$, and condition (4c) implies $(\mathbb{T}(z_0, z_a) \leq \varrho) \wedge (\mathbb{T}(z_a, z'_a) \leq \varrho) \implies (\mathbb{T}(z_0, z_a) \leq \mathbb{T}(z_0, z'_a) - \varsigma)$, which resemble [1, eq. (18)-(19)], respectively.

Now we show how the existence of a CC for the product system, as in Definition 6, guarantees that $\mathfrak{I}(\mathcal{S})$ satisfies the ω-regular specification described by UCA $\mathcal{A}$.

Proof: Let us assume there is a run $\mathbf{z}$ of the system that visits Z_a infinitely many times, and there exists $\mathbb{T}$ as in Definition 6. Let $\mathbf{z}_a$ be a subsequence of the run $\mathbf{z}$ such that $\mathbf{z}_a(t') \in Z_a$ for all $t' \in \mathbb{N}$. From (4a)-(4b) and backwards induction over the first argument we have $\mathbb{T}(\mathbf{z}(0), \mathbf{z}_a(t'_2)) \leq \varrho$ and $\mathbb{T}(\mathbf{z}_a(t'_1), \mathbf{z}_a(t'_2)) \leq \varrho$ for all $t'_2 > t'_1$ with $t'_1, t'_2 \in \mathbb{N}$. Now, from (4c) and induction over the second argument, we have $\mathbb{T}(\mathbf{z}(0), \mathbf{z}_a(0)) \leq \mathbb{T}(\mathbf{z}(0), \mathbf{z}_a(t'_2)) - \varsigma t'_2 \leq \varrho - \varsigma t'_2$ for any $t'_2 \in \mathbb{N}_{>0}$. For this to be true, the value of $\mathbb{T}(\mathbf{z}(0), \mathbf{z}_a(0))$ must be negative as t'_2 goes to infinity. This contradicts the assumption of $\mathbb{T}$ being non-negative. Therefore, $TR(\mathfrak{I}(\mathcal{S}), L) \subseteq \mathcal{L}(\mathcal{A})$. ■

Remark 1: Note that if a UCA describes a *safety* specification, we can recover similar conditions to those stated in Definition 5 from Definition 6 by setting $\lambda_2 = 1$ and $\lambda_3 = 0$. However, these conditions must hold for $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$ with an accepting state set $Z_a = X \times Q_a$ (where clearly $\text{proj}_X(Z_a) = X$) in contrast to the unsafe set $X_u \subset X$. Hence, a CC for $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$ following Definition 6 might have a more complex structure than a CC found under Definition 5. See also [1, Sec. 6.1] for an example where a linear CC exists following [1, Definition 3.1] (similar to Definition 5 here) but a linear CC for the product of the system and UCA cannot be found.

These CCs may be easier to find compared to traditional BCs in some cases (see [1, Sec. 3]); however, they are always defined over *pairs of states*. Hence, they are more computationally expensive to compute compared to barrier certificates. The time complexity of finding a polynomial closure certificate $\mathbb{T}$ of degree $2d$, if it exists, using an SOS approach is polynomial in $\mathcal{O}(|Q|^2 \binom{2n+2d}{d}^2)$, where $|Q|^2$ is the maximum number of possible transitions for a given UCA, and n corresponds to the dimension of the state set of $\mathfrak{I}(\mathcal{S})$ ($X \subset \mathbb{R}^n$), [1, Sec. 4.2]. Hence, given the system, the UCA specification, and a fixed degree for $\mathbb{T}$, the time complexity is

[1]Both conditions are equivalent under additional assumptions, e.g., assumptions for the S-procedure [21].

polynomial in n^2. Therefore, in the next section, we propose a divide-and-conquer approach by computing local certificates for each subsystem $\mathcal{S}_i$, whose composition results in a CC for the interconnected system.

Problem definition: Given an interconnected system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3, a labeling function L as in Definition 4 and an ω-regular specification characterized by a UCA $\mathcal{A}$ as in Definition 1, determine whether $TR(\mathfrak{I}(\mathcal{S}), L) \subseteq \mathcal{L}(\mathcal{A})$ through the use of *only* local certificates for each subsystem $\mathcal{S}_i$.

III. Main Compositionality Result

We adopt a compositional approach to find a CC for the interconnected system $\mathfrak{I}(\mathcal{S})$ by designing local certificates for its N subsystems $\mathcal{S}_i$. To do so, we leverage dissipativity-inspired conditions to construct these local certificates [22], which provide the interconnected system with a guarantee of satisfaction of the desired specifications.

A. Safety

The following result provides sufficient conditions for the composition of local certificates over the subsystems to imply safety of the interconnected system given an *unsafe set* X_u. First, we present the definition of *local certificate for safety* and then show how these certificates may be composed to form a certificate for the interconnected system.

Definition 7 (Local Certificate for Safety): Consider the system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3 composed of $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$ interconnected via the linear map M and a given set of unsafe states $X_u = \prod X_{ui}$ with $i \in [1; N]$. Let $\overline{\lambda} \in \mathbb{R}_{\geq 0}$ and consider symmetric matrices Υ_i, Γ_i of appropriate dimension, and parameters $\varrho_i, \vartheta_i \in \mathbb{R}_{>0}$, with $\varrho_i < \vartheta_i$, and $\lambda_i \in [0, \overline{\lambda}]$. Then, $\mathbb{T}_i : X_i \times X_i \to \mathbb{R}_{\geq 0}$ is a *local certificate for safety* for subsystem $\mathcal{S}_i$ if for all states $x_i, x_i' \in X_i$, $x_i^+ = f_i(x_i, w_i)$, and all initial states $x_{0i} \in X_{0i}$, unsafe states $x_{ui} \in X_{ui}$, internal inputs $w_i \in W_i$, and output $y_i = h_i(x_i)$, the following inequalities hold:

$$\mathbb{T}_i\big(x_i, x_i^+\big) \leq \varrho_i + (w_i, y_i)^T \Gamma_i (w_i, y_i), \tag{5a}$$

$$\mathbb{T}_i\big(x_i, x_i'\big) \leq \lambda_i \mathbb{T}_i\big(x_i^+, x_i'\big) + \varrho_i\big(1 - \overline{\lambda}\big) + (w_i, y_i)^T \Upsilon_i (w_i, y_i), \tag{5b}$$

$$\mathbb{T}_i(x_{0i}, x_{ui}) \geq \vartheta_i, \tag{5c}$$

where $\Gamma_i = \begin{bmatrix} \Gamma_i^{11} & \Gamma_i^{12} \\ \Gamma_i^{21} & \Gamma_i^{22} \end{bmatrix}$ and $\Upsilon_i = \begin{bmatrix} \Upsilon_i^{11} & \Upsilon_i^{12} \\ \Upsilon_i^{21} & \Upsilon_i^{22} \end{bmatrix}$.

Observe that a local certificate is not a CC by itself. However, these local certificates can be composed to form a CC for $\mathfrak{I}(\mathcal{S})$ as illustrated in the following theorem.

Theorem 1: Consider a system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3 composed of $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$ interconnected via the linear map M and a given set of *unsafe states* $X_u = \prod X_{ui}$ with $i \in [1; N]$. Assume that there is a *local certificate for safety* for each subsystem $\mathcal{S}_i$ as in Definition 7 and conditions (6) and (7) hold. Then, the function $\sum \mathbb{T}_i$ is a CC that guarantees the safety of $\mathfrak{I}(\mathcal{S})$ with respect to the unsafe set X_u.

$$\overline{\Gamma} := \begin{bmatrix} M \\ I \end{bmatrix}^T \begin{bmatrix} \Gamma_1^{11} & & & \Gamma_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \Gamma_N^{11} & & & \Gamma_N^{12} \\ \Gamma_1^{21} & & & \Gamma_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \Gamma_N^{21} & & & \Gamma_N^{22} \end{bmatrix} \begin{bmatrix} M \\ I \end{bmatrix} \preceq 0. \tag{6}$$

$$\overline{\Upsilon} := \begin{bmatrix} M \\ I \end{bmatrix}^T \begin{bmatrix} \Upsilon_1^{11} & & & \Upsilon_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \Upsilon_N^{11} & & & \Upsilon_N^{12} \\ \Upsilon_1^{21} & & & \Upsilon_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \Upsilon_N^{21} & & & \Upsilon_N^{22} \end{bmatrix} \begin{bmatrix} M \\ I \end{bmatrix} \preceq 0. \tag{7}$$

The proof of Theorem 1 follows similarly to that of Theorem 2 and is omitted for brevity.

Notice that $\overline{\lambda}$ is a hyperparameter for the interconnected system and an upper bound for λ_i. Moreover, the gap $\lambda_i - \overline{\lambda}$ must be considered in the local certificate's design, as we illustrate next. Consider a subsystem with index $j \in [1; N]$ and assume that for all $x_j, x_j' \in X_j$, and $w_j \in W_j$, $\mathbb{T}_j(f_j(x_j, w_j), x_j') \leq \varrho_j$. Then, the local condition (5b) takes the following form:

$$0 \leq \mathbb{T}_j\big(x_j, z_j\big) \leq \varrho_j\big(1 + \lambda_j - \overline{\lambda}\big) + \big(w_j, y_j\big)^T \Upsilon_j\big(w_j, y_j\big).$$

Thus, if in addition $\lambda_j - \overline{\lambda} \leq -1$, $(w_j, y_j)^T \Upsilon_j (w_j, y_j)$ must be positive to compensate the negative term contributed by $\varrho_j(1+\lambda_j-\overline{\lambda})$. Hence, having Υ_i not being negative semidefinite provides freedom in the design of $\mathbb{T}_j$. However, the summation of all Υ_i must be negative semidefinite to ensure the conditions of a CC. An extended discussion on the feasibility of $\overline{\Gamma}$ and $\overline{\Upsilon}$ is presented in [22].

Theorem 1 provides a local certificate for each $\mathcal{S}_i$ to guarantee safety for $\mathfrak{I}(\mathcal{S})$. Next, we show how one can leverage local certificates for subsystems to ensure ω-regular specifications for the overall interconnected system.

B. UCA Specifications

In order to provide local certificates for subsystems in the case of UCA specifications, one needs to project the product system $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$ onto the local subsystems. First, we retrieve the local labeling functions $L_i : X_i \to \Sigma_i$, and define local UCAs $\mathcal{A}_i = (Q_i, Q_{0i}, Q_{ai}, \delta_i, \Sigma_i)$, where $Q_i = Q$ denotes the state set, $Q_{0i} = Q_0$ denotes the initial set of states, $Q_{ai} = Q_a$ denotes the set of accepting states, and $\delta_i : Q_i \times \Sigma_i \rightrightarrows Q_i$ denotes the transition relation, where $\delta_i(q_i, \sigma_i) = \delta(q_i, \text{proj}^{-1}\sigma_i)$. Then, the *local* product system $\mathcal{S}_i \times \mathcal{A}_i$ for all $i \in [1; N]$ is defined as $\mathcal{S}_i \times \mathcal{A}_i = (Z_i, Z_{0i}, f_{\mathcal{A}i})$, where we use $Z_i = X_i \times Q_i$ to denote the set of states, $Z_{0i} = X_{0i} \times Q_{0i}$ denotes the set of initial states, $Z_{ai} := X_i \times Q_{ai}$ denotes the set of accepting states of the local product, $y_i = \tilde{h}_i(z_i) = h_i(x_i)$ denotes the local output, and the transition function $f_{\mathcal{A}i} : Z_i \times W_i \rightrightarrows Z_i$ is defined for all $z_i \in Z_i$ and $w_i \in W_i$ as follows:

$$\mathbf{z}_i(t+1) \in f_{\mathcal{A}i}(\mathbf{z}_i(t), \mathbf{w}_i(t))$$

$$:= \begin{cases} \mathbf{x}_i(t+1) = f_i(\mathbf{x}_i(t), \mathbf{w}_i(t)), \\ \mathbf{q}_i(t+1) \in \delta_i(\mathbf{q}_i(t), L_i(\mathbf{x}_i(t))). \end{cases}$$

Having defined the local product system, we now present certificates for these local products, which can then be composed to form a certificate for the interconnected system.

Definition 8 (Local Certificate for UCA Specifications): Consider an interconnected system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ as in Definition 3 composed of $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$ interconnected via the linear map M. Consider a UCA $\mathcal{A} = (Q, Q_0, Q_a, \delta, \Sigma)$ as in Definition 1, a labeling function $L : X \to \Sigma$ as in Definition 4, and the corresponding *local* product system $\mathcal{S}_i \times \mathcal{A}_i$. Let $\overline{\lambda}_1, \overline{\lambda}_2, \overline{\lambda}_3 \in \mathbb{R}_{\geq 0}$ and consider symmetric matrices Υ_i, Γ_i of appropriate dimension, and parameters $\varrho_i, \varsigma_i \in \mathbb{R}_{>0}$, and $\lambda_{1i} \in [0, \overline{\lambda}_1]$, $\lambda_{2i} \in [0, \overline{\lambda}_2]$, $\lambda_{3i} \in [0, \overline{\lambda}_3]$. Then, $\mathbb{T}_i : Z_i \times Z_i \to \mathbb{R}_{\geq 0}$ is a *local certificate for UCA specifications* for subsystem $\mathcal{S}_i \times \mathcal{A}_i$ if for all states $z_i, z_i' \in Z_i$, internal inputs $w_i \in W_i$, state $z_i^+ \in f_{\mathcal{A}i}(z_i, w_i)$, all initial states $z_{0i} \in Z_{0i}$, all accepting states $z_{ai}, z_{ai}' \in Z_{ai}$, and output $y_i = \tilde{h}_i(z_i) = h_i(x_i)$, the following inequalities hold:

$$\mathbb{T}_i(z_i, z_i^+) \leq \varrho_i + (w_i, y_i)^T \Gamma_i (w_i, y_i), \tag{8a}$$

$$\mathbb{T}_i(z_i, z_i') \leq \lambda_{1i} \mathbb{T}_i(z_i^+, z_i') + \varrho_i(1 - \overline{\lambda}_1) + (w_i, y_i)^T \Upsilon_i (w_i, y_i), \tag{8b}$$

$$\mathbb{T}_i(z_{0i}, z_{ai}) - \mathbb{T}_i(z_{0i}, z_{ai}') \leq -(\varsigma_i + \overline{\lambda}_2 \varrho_i + \overline{\lambda}_3 \varrho_i) + \lambda_{2i} \mathbb{T}_i(z_{0i}, z_{ai}) + \lambda_{3i} \mathbb{T}_i(z_{ai}, z_{ai}'), \tag{8c}$$

where $\Gamma_i = \begin{bmatrix} \Gamma_i^{11} & \Gamma_i^{12} \\ \Gamma_i^{21} & \Gamma_i^{22} \end{bmatrix}$ and $\Upsilon_i = \begin{bmatrix} \Upsilon_i^{11} & \Upsilon_i^{12} \\ \Upsilon_i^{21} & \Upsilon_i^{22} \end{bmatrix}$.

Now, we show how these local certificates can be leveraged to verify the interconnected system $\mathfrak{I}(\mathcal{S})$ against a desired ω-regular specification.

Theorem 2: Consider a system $\mathfrak{I}(\mathcal{S}) = (X, X_0, f)$ composed of $N \in \mathbb{N}_{\geq 1}$ subsystems $\mathcal{S}_i = (X_i, X_{0i}, W_i, f_i, Y_i, h_i)$ interconnected via a linear map M as in Definition 3. Consider also a UCA $\mathcal{A} = (Q, Q_0, Q_a, \delta, \Sigma)$ as in Definition 1, a labeling function $L : X \to \Sigma$ as in Definition 4, and the corresponding *local* product systems $\mathcal{S}_i \times \mathcal{A}_i$. Assume that there is a *local certificate for a UCA specification* for each $\mathcal{S}_i \times \mathcal{A}_i$ as in Definition 8 and conditions (6) and (7) hold. Then, the function $\sum \mathbb{T}_i$ is a CC that guarantees $TR(\mathfrak{I}(\mathcal{S}), L) \subseteq \mathcal{L}(\mathcal{A})$.

Proof: The proof follows the same steps as in the proof of Theorem 1. We show that given $\overline{\lambda}_1, \overline{\lambda}_2, \overline{\lambda}_3$, the function $\mathbb{T} = \sum \mathbb{T}_i$ is a CC for $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$ as in Definition 6. First, denote $z = \prod z_i$ and z', z_0, z_a, z_a' in a similar fashion. For given $\prod_{i=1}^N (z_i, w_i)$, let $z^+ \in \{\prod_{i=1}^N z_i^+ \mid z_i^+ \in f_{\mathcal{A}i}(z_i, w_i)$, for all $i \in [1; N]\}$. Note that since $\mathbb{T}_i(z_i, z_i') \geq 0$ for all $z_i, z_i' \in Z_i$, then, $\mathbb{T}(z, z') = \sum \mathbb{T}_i(z_i, z_i') \geq 0$ for all $z, z' \in Z$. Now, for all $z, z^+ \in Z$, we obtain condition (4a) from (8b) as follows:

$$\begin{aligned} \mathbb{T}(z, z^+) &= \sum \mathbb{T}_i(z_i, z_i^+) \leq \sum \varrho_i + \sum (w_i, y_i)^T \Gamma_i (w_i, y_i) \\ &\leq \varrho + (y_1, \dots, y_N, y_1, \dots, y_N)^T \overline{\Gamma} (y_1, \dots, y_N, y_1, \dots, y_N) \\ &\leq \varrho, \end{aligned}$$

where $\varrho := \sum \varrho_i$. Now, for all z, z', z^+, since $\mathbb{T}_i(z_i^+, z_i') \geq 0$, and λ_{1i} is bounded, one obtains (4b) from (8b) as follows:

$$\begin{aligned} \mathbb{T}(z, z') &= \sum \mathbb{T}_i(z_i, z_i') \leq \sum \lambda_{1i} \mathbb{T}_i(z_i^+, z_i') \\ &\quad + \sum \varrho_i(1 - \overline{\lambda}_1) + \sum (w_i, y_i)^T \Upsilon_i (w_i, y_i) \\ &\leq \max \lambda_{1i} \sum \mathbb{T}_i(z_i^+, z_i') + \varrho(1 - \overline{\lambda}_1) \\ &\quad + (y_1, \dots, y_N, y_1, \dots, y_N)^T \overline{\Gamma} (y_1, \dots, y_N, y_1, \dots, y_N) \\ &\leq \overline{\lambda}_1 \mathbb{T}(z^+, z') + \varrho(1 - \overline{\lambda}_1). \end{aligned}$$

Finally, since $\mathbb{T}_i \geq 0$ and $\lambda_{2i}, \lambda_{3_i}$ are bounded, we obtain (3b) from (5b) as follows:

$$\begin{aligned} \mathbb{T}(z_0, z_a') - \mathbb{T}(z_0, z_a) &= \sum \mathbb{T}_i(z_{0i}, z_{ai}') - \sum \mathbb{T}_i(z_{0i}, z_{ai}) \\ &\leq -\sum (\varsigma_i + \overline{\lambda}_2 \varrho_i + \overline{\lambda}_3 \varrho_i) + \sum \lambda_{2i} \mathbb{T}_i(z_{0i}, z_{ai}) \\ &\quad + \sum \lambda_{3i} \mathbb{T}_i(z_{ai}, z_{ai}') \\ &\leq -(\varsigma + \overline{\lambda}_2 \varrho + \overline{\lambda}_3 \varrho) + \max \lambda_{2i} \sum \mathbb{T}_i(z_{0i}, z_{ai}) \\ &\quad + \max \lambda_{3i} \sum \mathbb{T}_i(z_{ai}, z_{ai}') \\ &\leq -(\varsigma + \overline{\lambda}_2 \varrho + \overline{\lambda}_3 \varrho) + \overline{\lambda}_2 \mathbb{T}(z_0, z_a) + \overline{\lambda}_3 \mathbb{T}(z_a, z_a'), \end{aligned}$$

where $\varsigma := \sum \varsigma_i$. Then, according to Definition 6, $\mathbb{T} = \sum \mathbb{T}_i$ is a CC for the interconnected system $\mathfrak{I}(\mathcal{S}) \times \mathcal{A}$. Hence, by [1, Th. 6] we conclude that $TR(\mathfrak{I}(\mathcal{S}), L) \subseteq \mathcal{L}(\mathcal{A})$. ∎

Notice that the fact of $\mathbb{T}_i$ being non-negative is necessary to obtain the upperbound $\sum \lambda_{\ell i} \mathbb{T}_i(\cdot, \cdot) \leq \max \lambda_{\ell i} \mathbb{T}_i(\cdot, \cdot)$, with $\ell \in \{1, 2, 3\}$. Moreover, the strengthened conditions (8b) and (8b) provide the inequalities that allow the use of $\mathbb{T} = \sum \mathbb{T}_i$ as the CC for the interconnected system, which cannot be readily used under conditions [1, eq. (18)-(19)].

Additionally, we are now able to decompose the problem of finding $\mathbb{T}$ into finding individual $\mathbb{T}_i$ for all $i \in [1; N]$ and concurrently checking compositionality conditions on $\overline{\Gamma}$ and $\overline{\Upsilon}$, for example, via the Alternating Direction Method of Multipliers (ADMM). Then, if we use an SOS approach to compute every $\mathbb{T}_i$, the time complexity of finding $\mathbb{T}$ is $\sum_{i=1}^N \mathcal{O}(|Q_i|^2 \binom{2n_i + 2d_i}{d_i}^2)$, in addition to the time complexity of solving two semidefinite programs (SDPs) that is $\mathcal{O}(|\overline{\Gamma}\mathbf{1}|^3)$ and $\mathcal{O}(|\overline{\Upsilon}\mathbf{1}|^3)$, respectively, where $\mathbf{1}$ is a column vector of ones of appropriate dimension and $|\cdot|$ denotes the dimension of the vector in the argument. Hence, if we fix the same polynomial degree for the *monolithic* CC and the *composed* CC, we see an improvement in the computation of the latter since $\sum_i \mathcal{O}(n_i^2) << \mathcal{O}(\sum_i n_i)^2$.

IV. Numerical Example

We study the temperature control for a building modeled as an interconnection of N rooms. The temperature of each room is affected by the temperature of the exterior of the building and adjacent rooms. The specification of interest requires the building temperature to visit the region b finitely often. This specification can be modeled as the UCA in Fig. 1. The temperature of the system $\mathfrak{I}(\mathcal{S})$ is given by $\mathbf{x}(t+1) = A\mathbf{x}(t) + \mu T_h \mathbf{u}(t) + \theta T_e$, where $x = (x_1, x_2, \dots, x_N)$, $u = (u_1, u_2, \dots, u_N)$, $T_h = (T_{h1}, T_{h2}, \dots, T_{hN})$, and $T_e = (T_{e1}, T_{e2}, \dots, T_{eN})$. The matrix $A \in \mathbb{R}^{N \times N}$ is filled with zeros except for the elements $A_{i,i} = 1 - 2\alpha - \theta - \mu u_i(t)$, and $A_{i,i+1} = A_{i+1,i} = A_{1,N} = A_{N,1} = \alpha$ for all $i \in [1; N-1]$; which means hat the rooms form a circular interconnection. The parameters α, θ, μ are the conduction factors between a given room and

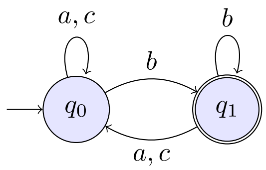

Fig. 1. This UCA models a specification that requires the system to be in a state with label b only finitely often.

the adjacent one, the exterior, and the heater, respectively. The alphabet $\Sigma = \{a, b, c\}$ and local alphabet $\Sigma_i = \{a_i, b_i, c_i\}$ where $a = \prod a_i$, $b = \prod b_i$, and $c = \prod c_i$.

In particular, we set $\alpha = 0.001$, $\theta = 0.06$, $\mu = 0.145$, $T_{h,i} = 30$, $T_{e,i} = 0$, and $u_i(t) = 1.3$ for all $i \in [1; N]$. Moreover, the initial state set is $X_{0i} = [18, 22]$ and the labeling function $L_i : X_i \to \Sigma_i$ is defined as follows: $a_i = L_i(x_i)$, for all $x_i \in [0, 10]$, $b_i = L_i(x_i)$, for all $x_i \in]10, 20]$, and $c_i = L_i(x_i)$, for all $x_i \in]20, 30]$.

We note that the value of $u_i(t) = 1.3$ for all $t \in \mathbb{N}$ renders $x_i = 22.57$ globally asymptotically stable for all $i \in [1; N]$. Therefore, there exists no BC with initial states in the set $L^{-1}(a) \cup L^{-1}(c)$ and unsafe states in the set $L^{-1}(b)$. Hence, we cannot obtain a BC following the "triplets" approach as in [7] nor in a compositional fashion as in [8]. Now, since every room has the same dynamics, we assign the same local certificate for each subsystem. We construct a piece-wise function $\mathbb{T}_i$ with respect to the transitions of $\mathcal{A}_i$, namely, for each $(q_i, q_i') \in Q_i \times Q_i$; such that for each transition $(z_i, z_i') \in Z_i \times Z_i$ with $z_i = (x_i, q_i)$, $z_i' = (x_i', q_i')$; the function $\mathbb{T}_i(\cdot, q_i, \cdot, q_i')$ is a polynomial of degree 2 with respect to x_i, x_i' as shown.

$$\begin{aligned}
\mathbb{T}_i(x_i, 0, x_i', 0) &= 5917.2 - 202.8x_i' + 4771.6x_i + 172.3x_i^2 \\
&\quad +0.1x_i'^2 - 154.3x_i x_i' \\
\mathbb{T}_i(x_i, 0, x_i', 1) &= 6864.8 - 361.3x_i' + 4005.1x_i - 10.7x_i^2 \\
&\quad +7.2x_i'^2 - 109.6x_i x_i' \\
\mathbb{T}_i(x_i, 1, x_i', 0) &= 7154.2 - 257.3x_i' + 5861x_i + 297.1x_i^2 \\
&\quad +0.1x_i'^2 - 194.141287384x_i' x_i \\
\mathbb{T}_i(x_i, 1, x_i', 1) &= 10447.2 - 558.8x_i' + 7107.4x_i + 221.5x_i^2 \\
&\quad +7x_i'^2 - 266.3x_i x_i'. \qquad (9)
\end{aligned}$$

We also obtain $\rho_i = 100$, $\varsigma_i = 2.8328$, $\lambda_{1i} = \overline{\lambda}_1 = 20$, $\lambda_{2i} = \overline{\lambda}_2 = 1$, $\lambda_{3i} = \overline{\lambda}_3 = 1$, and matrices $\Gamma_i = \begin{bmatrix} 0.0125 & 6.8894e-05 \\ 6.8894e-05 & -0.1266 \end{bmatrix}$, $\Upsilon_i = \begin{bmatrix} 0.0124 & 4.3253e-06 \\ 4.3253e-06 & -62.8787 \end{bmatrix}$.

We synthesized local certificates for our specification $N = 1000$. However, one can readily verify that these local certificates satisfy conditions in Theorem 2 for any N by confirming that $\overline{\Gamma}, \overline{\Upsilon} \preceq 0$.

V. Conclusion

We leveraged the notion of closure certificates to provide a formal guarantee that a given large-scale interconnected system satisfies a universal co-Büchi automaton specification. To ease the computation of such a certificate for large-scale systems, we propose a compositional approach. Under the assumption that the large-scale system is represented as an interconnection of smaller subsystems connected via a linear map, we compute local certificates for these subsystems and provide a closure certificate for the interconnected system by composing these local certificates. A promising direction for future research is to investigate whether such certificates can be adapted to stochastic and continuous-time systems.

References

[1] V. Murali, A. Trivedi, and M. Zamani, "Closure certificates," in *Proc. ACM Int. Conf. Hybrid Syst., Comput. Control*, 2024, pp. 1–14.

[2] A. Podelski and A. Rybalchenko, "Transition invariants," in *Proc. Annu. IEEE Symp. Logic Comput. Sci.*, 2004, pp. 32–41.

[3] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Math. Program.*, vol. 96, pp. 293–320, May 2003.

[4] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. New York, NY, USA: Springer, 2009.

[5] A. Swikir, A. Girard, and M. Zamani, "From dissipativity theory to compositional synthesis of symbolic models," in *Proc. Indian Control Conf.*, 2018, pp. 30–35.

[6] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Proc. ACM Int. Workshop Hybrid Syst., Comput. Control*, 2004, pp. 477–492.

[7] T. Wongpiromsarn, U. Topcu, and A. Lamperski, "Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems," *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp. 3344–3355, Nov. 2016.

[8] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in *Proc. ACM Int. Conf. Hybrid Syst., Comput. Control*, 2020, pp. 1–11.

[9] 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.

[10] L. Niu and A. Clark, "Control barrier functions for abstraction-free control synthesis under temporal logic constraints," in *Proc. IEEE Conf. Decision Control*, 2020, pp. 816–823.

[11] L. Niu, A. Clark, and R. Poovendran, "Necessary and sufficient conditions for satisfying linear temporal logic constraints using control barrier certificates," in *Proc. IEEE Conf. Decision Control*, 2023, pp. 8589–8595.

[12] V. Murali, A. Trivedi, and M. Zamani, "Co-Buchi barrier certificates for discrete-time dynamical systems," 2023, *arXiv:2311.07695*.

[13] S. Schewe and B. Finkbeiner, "Bounded synthesis," in *Proc. Int. Symp. Autom. Technol. Verif. Anal.*, 2007, pp. 474–488.

[14] E. Filiot, N. Jin, and J.-F. Raskin, "Antichains and compositional algorithms for LTL synthesis," *Formal Methods Syst. Design*, vol. 39, pp. 261–296, Dec. 2011.

[15] F. Galarza-Jimenez, V. Murali, and M. Zamani, "Compositional control synthesis via Co-Buchi barrier certificates," in *Proc. IFAC Conf. Anal. Design Hybrid Syst.*, 2024.

[16] B. Cook, A. Podelski, and A. Rybalchenko, "Terminator: Beyond safety," in *Proc. Comput. Aided Verif., Int. Conf.*, 2006, pp. 415–418.

[17] B. Cook, A. Podelski, and A. Rybalchenko, "Proving program termination," *Commun. ACM*, vol. 54, no. 5, pp. 88–98, 2011.

[18] A. Podelski and S. Wagner, "Model checking of hybrid systems: From reachability towards stability," in *Proc. ACM Int. Workshop Hybrid Syst., Comput. Control*, 2006, pp. 507–521.

[19] S. Sankaranarayanan and A. Tiwari, "Relational abstractions for continuous and hybrid systems," in *Proc. Comput. Aided Verif., Int. Conf.*, 2011, pp. 686–702.

[20] C. Löding, "Efficient minimization of deterministic weak ω-automata," *Inf. Process. Lett.*, vol. 79, no. 3, pp. 105–109, 2001.

[21] I. Pólik and T. Terlaky, "A survey of the S-lemma," *SIAM Rev.*, vol. 49, no. 3, pp. 371–418, 2007.

[22] M. Arcak, C. Meissen, and A. Packard, *Networks of Dissipative Systems: Compositional Certification of Stability, Performance, and Safety*. Cham, Switzerland: Springer, 2016.