51st IEEE Conference on Decision and Control
December 10-13, 2012. Maui, Hawaii, USA

On the Existence of Compositional Barrier Certificates

Christoffer Sloth, Rafael Wisniewski, and George J. Pappas

Abstract— **This paper provides a necessary and sufficient condition for the compositional verification of a continuous system with additively separable barrier functions. The compositional safety verification enables the verification of an interconnection of subsystems. The idea behind the compositional analysis is to allow the verification of systems with a high dimension, by the verification of multiple lower dimensional subproblems. In the compositional safety analysis, a particular structure is imposed on the barrier certificate, restricting the applicability of the method.**

We show an example of a system that cannot be verified using the compositional method, but can be verified using a centralized method. This example highlights how not to decompose systems, and should be used to guide the decomposition of a system into appropriate subsystems. Finally, we provide a second condition for the compositional safety analysis that enables the verification of the counterexample, by imposing a less restrictive structure of the barrier function. This shows that the counterexample can be solved with a compositional method, but at an increased computational complexity.

I. Introduction

Safety verification is a necessary part of developing safety-critical control systems, where a malfunction may have severe consequences. The safety verification ensures that a control system does not violate any state constraints. Numerous methods have been developed for verifying the safety of a system; see [1] for a survey.

The safety verification determines if the reachable set intersects a set of unsafe states. The computation of the reachable states for a dynamical system is in general very difficult [2], and it may only be possible to calculate approximate the reachable states for systems of low dimension. According to [3], safety verification is applicable for systems with approximately five or less continuous states. Therefore, several methods have been developed to approximate the reachable set of a dynamical system. In [4], the reachable states are approximated using a finite number of simulated trajectories, and exploiting an incremental stability condition.

Another class of methods, e.g., [5], [6] verifies the safety of a system, by using the vector field to find invariant sets that do not include the unsafe states. Similarly, the papers [7], [8] provide a method for calculating barrier certificates for safety analysis of continuous, stochastic, and hybrid systems. The idea of these works is to find a barrier function that is decreasing along system trajectories, and has a zero level set (a so-called barrier), which no solution trajectory crosses. If the set of initial states is a subset of the zero sublevel set of the barrier function, and the set of unsafe states is in its complement, then the system is safe.

The generation of the barrier certificates is similar to the generation of Lyapunov functions for proving stability. Therefore, it is important to use a computational method that scales well. Therefore, linear matrix inequalities (LMIs) and sum of squares (SOS) are used to generate the barrier certificates [9].

Common to the previously mentioned methods is that they verify the safety of a system, by studying a system directly. However, it may be beneficial to study a system as an interconnection of subsystems, and decompose the verification problem into smaller subproblems. This is suggested for compositional stability analysis in [10] and an analysis framework based on assume-guarantee reasoning is presented in [11]. In addition, a compositional method for generating barrier certificates is proposed in [12].

In this paper, we show when compositional barrier certificates can be generated using the method presented in [12]. It is shown that barrier certificates generated by the compositional method are additively separable functions. This implies that the decomposition of a system into subsystems should be generated such that an additively separable barrier certificate exists. Otherwise, the compositional method fails to verify the system. This is a very restrictive assumption; hence, the method is not as general as the centralized method presented in [7], [8]. However, in oppose to the centralized method, the compositional method scales very well.

We provide a simple example, where the compositional method fails. To alleviate the experienced issues, we propose another safety condition that is capable of handling the previous counterexample, but the method has a higher computational complexity.

To shorten the presentation, we only consider so-called weak barrier certificates, but the results apply for strict barrier certificates as well. Furthermore, we do not show how to algorithmically generate the certificates. Details about the generation of barrier certificates can be found in [12].

The paper is organized as follows. Section II explains the verification problem in terms of barrier certificates, and Section III explains the compositional condition for generating barrier certificates. Section IV classifies the barrier certificates that can be generated by the compositional method, and Section V proposes a more general method for doing the compositional safety analysis. Finally, Section VI comprises conclusions.

This work was supported by Smart & Cool.

Christoffer Sloth is with Department of Computer Science, Aalborg University, 9220 Aalborg East, Denmark csloth@cs.aau.dk

Rafael Wisniewski is with the Section of Automation & Control, Aalborg University, 9220 Aalborg East, Denmark raf@es.aau.dk

George J. Pappas is with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104 USA pappasg@seas.upenn.edu

978-1-4673-2064-1/12/$31.00 ©2012 IEEE

II. Barrier Certificates

In this section, we present the barrier certificate method, which can be used to verify the safety of a dynamical system.

We consider a continuous system given as a system of ordinary differential equations

$$\dot{x} = f(x), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state. Compared to [7], [8], [12] on which this paper is based, the disturbance input to the system is omitted to clarify the presentation. However, the results in this paper can be easily extended to include disturbances.

We denote the solution of the Cauchy problem (1) with $x(0) = x_0$ on an interval $[0, T]$ by ϕ_{x_0}, i.e.,

$$\frac{d\phi_{x_0}(t)}{dt} = f\left(\phi_{x_0}(t)\right) \tag{2}$$

for all $t \in [0, T]$.

We consider a system given by $\Gamma = (f, X, X_0, X_{\mathrm{u}})$, where $f : \mathbb{R}^n \to \mathbb{R}^n$ is continuous, $X \subseteq \mathbb{R}^n$, $X_0 \subseteq X$, and $X_{\mathrm{u}} \subseteq X$. In the safety verification, we only consider trajectories initialized in X_0 that are contained in the set X. We verify if there exists a trajectory that can reach an unsafe set X_{u}.

For a map $f : A \to B$ and subset $C \subset A$, we write $f(C) \equiv \{f(x) |\ x \in C\}$. Thus, the safety of a system Γ is defined as follows.

Definition 1 (Safety): Let $\Gamma = (f, X, X_0, X_{\mathrm{u}})$ be given. A trajectory $\phi_{X_0} : [0, T] \to \mathbb{R}^n$ is unsafe if there exists a time $t \in [0, T]$, such that $\phi_{X_0}([0, t]) \cap X_{\mathrm{u}} \neq \emptyset$ and $\phi_{X_0}([0, t]) \subseteq X$.

We say that a system Γ is safe if there are no unsafe trajectories.

To verify the safety of Γ, we use the following proposition.

Proposition 1 (Weak barrier certificate [7], [8]): Let $\Gamma = (f, X, X_0, X_{\mathrm{u}})$ be given. If there exists a differentiable function $B : X \to \mathbb{R}$ satisfying

$$B(x) \leq 0 \quad \forall x \in X_0, \tag{3a}$$

$$B(x) > 0 \quad \forall x \in X_{\mathrm{u}}, \text{ and} \tag{3b}$$

$$\frac{\partial B}{\partial x}(x) f(x) \leq 0 \quad \forall x \in X. \tag{3c}$$

Then the system Γ is safe.

Proposition 1 states that a trajectory of a system initialized in a state within the zero sublevel set of a nonincreasing function (along system trajectories), cannot reach the complement of the zero sublevel set.

A. Notation

For $k \in \mathbb{N}$. Given $x = (x_1, \ldots, x_k) \in \mathbb{R}^{n_1} \times \cdots \times \mathbb{R}^{n_k}$, with $x_i \in \mathbb{R}^{n_i}$, we define $\hat{x}_i \equiv (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$. Similarly, given a sequence of maps $(h_1, \ldots, h_k)$, we define $\hat{h}_i \equiv (h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_k)$. Finally, $n = \sum_i n_i$.

III. Compositional Barrier Certificates

In this section, we pose the safety verification as a compositional problem, by assuming that a dynamical system is given as an interconnection of subsystems. This is based on conditions given in [12].

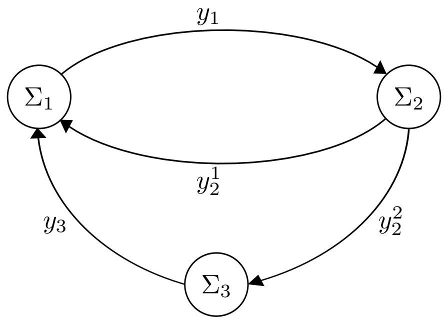

Fig. 1. Interconnection of three subsystems $\Sigma_1, \Sigma_2, \Sigma_3$.

First, we provide the definition of an interconnected system and provide a small example, to give the necessary intuition. Note that any system (1) can be given as an interconnection of subsystems.

Definition 2: Let $\Gamma = (f, X, X_0, X_{\mathrm{u}})$ be a dynamical system with

$$\dot{x} = f(x), \tag{4}$$

where $x \in \mathbb{R}^n$ is the state.

Let $k \in \mathbb{N}$ and $x = (x_1, \ldots, x_k)$. For $i = 1, \ldots, k$, let $x_i \in \mathbb{R}^{n_i}$, let $g_i : \mathbb{R}^{n - n_i} \to \mathbb{R}^{m_i}$ and $h_i : \mathbb{R}^{n_i} \to \mathbb{R}^{q_i}$ be continuous maps, and let $q \equiv \sum_i q_i$. Let $X = X_1 \times \cdots \times X_k$, $X_0 = X_{0,1} \times \cdots \times X_{0,k}$, and $X_{\mathrm{u}} = X_{\mathrm{u},1} \times \cdots \times X_{\mathrm{u},k}$. We say that the system $\Gamma = (\{f_i\}, \{X_i\}, \{X_{0,i}\}, \{X_{\mathrm{u},i}\})$ with

$$\begin{aligned} \dot{x}_i &= f_i(x_i, g_i(\hat{x}_i)), \\ y_i &= h_i(x_i) \end{aligned} \tag{5}$$

where the map g_i gives the inputs to subsystem i and that the map h_i gives the outputs of subsystem i for $i = 1, \ldots, k$ is an interconnected system of $f(x)$ if

$$f(x) = \begin{bmatrix} f_1(x_1, g_1(\hat{x}_1)) \\ \vdots \\ f_i(x_i, g_i(\hat{x}_i)) \\ \vdots \\ f_k(x_k, g_k(\hat{x}_k)) \end{bmatrix} \tag{6}$$

for all $x \in X$ and there exist maps $e_i : \mathbb{R}^{q - q_i} \to \mathbb{R}^{m_i}$

$$g_i = e_i \circ \hat{h}_i. \tag{7}$$

The input of subsystem i, given by g_i, is a composition of outputs $\hat{h}_i$ and the interconnection graph e_i. The compositional setup is clarified by providing a system consisting of three interconnected subsystems shown in Figure 1.

Let each subsystem be described by a system of continuous ordinary differential equations and an output map

$$\Sigma_1 : \begin{cases} \dot{x}_1 = f_1(x_1, g_1(\hat{x}_1)) \\ y_1 = h_1(x_1) \end{cases} \tag{8a}$$

$$\Sigma_2 : \begin{cases} \dot{x}_2 = f_2(x_2, g_2(\hat{x}_2)) \\ y_2 = h_2(x_2) \end{cases} \tag{8b}$$

$$\Sigma_3 : \begin{cases} \dot{x}_3 = f_3(x_3, g_3(\hat{x}_3)) \\ y_3 = h_3(x_3), \end{cases} \tag{8c}$$

where $x_i \in X_i \subseteq \mathbb{R}^{n_i}$ is the state and $y_i \in \mathbb{R}^{q_i}$ is the output given by the map $h_i : \mathbb{R}^{n_i} \to \mathbb{R}^{q_i}$. Note that the interconnection of the three subsystems is defined by $e_i : \mathbb{R}^{q-q_i} \to \mathbb{R}^{m_i}$. From Figure 1, it is seen that

$$e_1 :(y_2^1, y_2^2, y_3) \mapsto (y_2^1, y_3), \tag{9a}$$

$$e_2 :(y_1, y_3) \mapsto y_1, \tag{9b}$$

$$e_3 :(y_1, y_2^1, y_2^2) \mapsto y_2^2. \tag{9c}$$

Note that the interconnected system induces a natural graph structure, where there are no self-loops and there is only one edge from one vertex to another. The graph can be described by an adjacency matrix $E \in \mathbb{R}^k \times \mathbb{R}^k$, where $E(i, j) = 1$ if there is an edge between subsystem i and j, with the head at subsystem i and the tail at subsystem j. Note that the ith row of E can be derived from e_i. For the graph in Fig. 1 the adjacency matrix is

$$E = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}. \tag{10}$$

Finally, we can state the combinatorial condition for safety.

Corollary 1 ([12]): Let $k \in \mathbb{N}$ and let the dynamical system $\Gamma = (\{f_i\}, \{X_i\}, \{X_{0,i}\}, \{X_{\mathrm{u},i}\})$ be given. If there exist differentiable functions $B_i : X_i \to \mathbb{R}$, constants $\alpha_i, \beta_i \in \mathbb{R}$, and continuous functions $\gamma_i : \mathbb{R}^{q_i+m_i} \to \mathbb{R}$ for $i = 1, \dots, k$ such that

$$B_i(x_i) + \alpha_i \le 0 \quad \forall x_i \in X_{0,i}, \tag{11a}$$

$$B_i(x_i) - \beta_i > 0 \quad \forall x_i \in X_{\mathrm{u},i}, \tag{11b}$$

$$\frac{\partial B_i}{\partial x_i}(x_i) f_i(x_i, g_i(\hat{x}_i)) \le \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \quad \text{for all } (x_i, \hat{x}_i) \in X_i \times \hat{X}_i, \tag{11c}$$

and for all $(x_i, \hat{x}_i) \in X_i \times \hat{X}_i$,

$$\sum_i \alpha_i \ge 0, \sum_i \beta_i \ge 0, \sum_i \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \le 0. \tag{11d}$$

Then the system Γ is safe.

IV. Existence of Compositional Barrier Certificates

In this section, we show that Proposition 1 and Corollary 1 are equivalent, if the barrier certificate is assumed to be additively separable and the differential of the output maps has constant rank. First, we define an additively separable function and state a necessary assumption on the output map. Then we provide three lemmas from which the main theorem follows. Finally, we provide two examples, one of which the compositional method fails to verify.

Definition 3: Let $k \in \mathbb{N}$ and $i = 1, \dots, k$. We say that a function $\varphi : \mathbb{R}^n \to \mathbb{R}$ is additively separable in $x = (x_1, \dots, x_k)$ if there exist functions $\varphi_i : \pi_i(\mathbb{R}^n) \to \mathbb{R}$, where π_i is a projection that takes $(x_1, \dots, x_k)$ to x_i such that

$$\varphi(x) = \sum_i \varphi_i(x_i) \quad \forall x \in \mathbb{R}^n, \tag{12}$$

where $x_i \in \mathbb{R}^{n_i}$ and $n = \sum_i n_i$.

Lemma 3 relies on the generation of a coordinate transformation that can be generated if the following assumption on the output map holds.

Assumption 1: Let Dh_i be the differential of h_i. For $i = 1, \dots, k$

$$Dh_i(x_i) \tag{13}$$

has constant rank.

The assumption guarantees that an output cannot occasionally "disappear".

A necessary and sufficient condition is given below for the composition of inequality constraints.

Lemma 1: Let $k \in \mathbb{N}$. For $i = 1, \dots, k$, let $n_i \in \mathbb{N}$, $f_i : \mathbb{R}^{n_i} \to \mathbb{R}$ be a continuous function, and $X_i \subseteq \mathbb{R}^{n_i}$ be compact. There exist constants $c_i \in \mathbb{R}$ such that

$$f_i(x_i) - c_i \le 0 \quad \forall x_i \in X_i \text{ and} \tag{14a}$$

$$\sum_i c_i \le 0 \tag{14b}$$

if and only if

$$\sum_i f_i(x_i) \le 0 \quad \forall x_i \in X_i. \tag{15}$$

From Lemma 1, it is seen that an inequality (15) in n variables is equivalent to k inequalities in n_i variables and an inequality constraint involving only constants. This is used later to decompose inequality constraints.

The following result is used in Lemma 3, to reduce the number for coupling variables in the compositional condition for safety in Corollary 1, by exploiting Assumption 1.

Lemma 2: Let $\gamma : \mathbb{R}^n \to \mathbb{R}$ be a continuous function and let $h : \mathbb{R}^n \to \mathbb{R}^q$ be a smooth map such that Dh has constant rank k. Then there is a smooth map $\bar{h} : \mathbb{R}^n \to \mathbb{R}^{n-k}$ such that $D\bar{h}$ has constant rank $n - k$, and a continuous function $\tilde{\gamma} : \mathbb{R}^{q+(n-k)} \to \mathbb{R}$ such that

$$\gamma(x) = \tilde{\gamma}(h(x), \bar{h}(x)) \quad \forall x \in \mathbb{R}^n. \tag{16}$$

Proof: We use Constant Rank Theorem, recalled here for completeness: Let V, W be m, n-dimensional vector spaces and $U \subset V$ an open set. If $h : U \to W$ is a smooth map such that Dh has constant rank k in U, then for each point $p \in U$ there are charts (U, φ) and (W, ψ) containing p, $h(p)$ such that

$$\psi \circ h \circ \varphi^{-1} : (x_1, \dots, x_m) \mapsto (x_1, \dots, x_k, 0, \dots, 0). \tag{17}$$

To see how $\tilde{\gamma}$ and $\bar{h}$ can be generated, we give the following commutative diagram based on Constant Rank Theorem.

$$\begin{tikzcd}
 & \mathbb{R} & \\
\mathbb{R}^n \arrow[ur, "\gamma"] \arrow[rr, "h"] \arrow[d, "\varphi"', "x\mapsto(a,b)"] & & \mathbb{R}^q \arrow[d, "\psi"', "h(x)\mapsto(a,0)"] \\
\mathbb{R}^k \times \mathbb{R}^{n-k} \arrow[rr, dashed] \arrow[d, "\pi_2"', "(a,b)\mapsto b"] & & \mathbb{R}^k \times \mathbb{R}^{n-k} \arrow[d, "\pi_1"', "(a,0)\mapsto a"] \\
\mathbb{R}^{n-k} & & \mathbb{R}^k
\end{tikzcd}$$

Now, the functions $\bar{h}$ and γ that satisfy (16) are $\bar{h} = \pi_2 \circ \varphi$, where $\pi_2 : (x_1, \dots, x_n) \mapsto (x_{k+1}, \dots, x_n)$ and let $\tilde{\gamma} = \gamma \circ \varphi^{-1} \circ (\pi_1 \circ \psi, id)$, where $\pi_1 : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_k)$ and id is the identity map of dimension $n - k$. ■

The final lemma on the decomposition of inequality constraints is shown next.

Lemma 3: Let $k \in \mathbb{N}$. For $i \in \{1, \dots, k\}$, let

- $m_i, n_i, q_i \in \mathbb{N}$ and define $q \equiv \sum_i q_i$,
- $V_i \subseteq \mathbb{R}^{n_i + (n - n_i)}$ be compact,
- $f_i : \mathbb{R}^{n_i + m_i} \to \mathbb{R}^{n_i}$ and $g_i : \mathbb{R}^{n - n_i} \to \mathbb{R}^{m_i}$ be continuous maps,
- $\varphi_i : \mathbb{R}^{n_i} \to \mathbb{R}$ be a continuous function,
- $h_i : \mathbb{R}^{n_i} \to \mathbb{R}^{q_i}$ be a smooth map such that Dh_i has constant rank r_i.

There exist continuous functions $\gamma_i : \mathbb{R}^{q_i + m_i} \to \mathbb{R}$ such that for all $(x_i, \hat{x}_i) \in V_i \subseteq \mathbb{R}^{n_i} \times \mathbb{R}^{n - n_i}$

$$\varphi_i(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq \gamma_i(h_i(x_i), g_i(\hat{x}_i)), \text{ and} \tag{18a}$$

$$\sum_i \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \leq 0 \tag{18b}$$

if and only if for all $(x_i, \hat{x}_i) \in V_i$

$$\sum_i \varphi_i(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq 0. \tag{19}$$

Proof: It is seen that (18) implies (19), by summing (18a) for $i = 1, \dots, k$, such that for all $(x_i, \hat{x}_i) \in V_i$

$$\sum_i \varphi_i(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq \sum_i \gamma_i(h_i(x_i), g_i(\hat{x}_i)), \tag{20}$$

which by (18b) is bounded from above by zero.

To show that (19) implies (18), let

$$\bar{\gamma}_i(x_i, g_i(\hat{x}_i)) \equiv \varphi_i(x_i) f_i(x_i, g_i(\hat{x}_i)) \quad \forall (x_i, \hat{x}_i) \in V_i. \tag{21}$$

By (19)

$$\sum_i \bar{\gamma}_i(x_i, g_i(\hat{x}_i)) \leq 0 \quad \forall (x_i, \hat{x}_i) \in V_i. \tag{22}$$

Lemma 2 states that by assuming that Dh_i has constant rank r_i; there exist functions $\tilde{\gamma}_i : \mathbb{R}^{q_i + (n_i - r_i) + m_i} \to \mathbb{R}$ and maps $\bar{h}_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i - r_i}$ such that for all $(x_i, \hat{x}_i) \in V_i$

$$\tilde{\gamma}_i(h_i(x_i), \bar{h}_i(x_i), g_i(\hat{x}_i)) = \bar{\gamma}_i(x_i, g_i(\hat{x}_i)). \tag{23}$$

We rewrite (22) as follows

$$\sum_i \tilde{\gamma}_i(h_i(x_i), \bar{h}_i(x_i), g_i(\hat{x}_i)) \leq 0 \quad \forall (x_i, \hat{x}_i) \in V_i. \tag{24}$$

It is seen from (24) that only $\tilde{\gamma}_i$ depends on $\bar{h}_i(x_i)$; hence, we define

$$\gamma_i(h_i(x_i), g_i(\hat{x}_i)) \equiv \sup_{z_i \in X_i} \tilde{\gamma}_i(h_i(x_i), \bar{h}_i(z_i), g_i(\hat{x}_i)). \tag{25}$$

Then by Proposition 2.3 and Lemma 2.2 in [13] γ_i is a continuous function and for all $(x_i, \hat{x}_i) \in V_i$

$$\varphi_i(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \text{ and} \tag{26a}$$

$$\sum_i \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \leq 0. \tag{26b}$$

■

Notice the importance of using γ_i in oppose to $\bar{\gamma}_i$. γ_i is only a function of the outputs of subsystem i, while $\bar{\gamma}_i$ is a function of its entire state vector. This implies that the dimension of the coupling is drastically reduced if the number of output variables is small compared to the number of states. Furthermore, it is important to note that γ_i is continuous, as it enables γ_i to be approximated arbitrarily close by polynomials on a compact set. This is favorable, as polynomial inequality and equality constraints can be solved algorithmically by use of sum of squares programming [14].

We can now state when Proposition 1 and Corollary 1 are equivalent.

Theorem 1: Let $k \in \mathbb{N}$, and let

$$\begin{bmatrix} \dot{x}_1 \\ \vdots \\ \dot{x}_i \\ \vdots \\ \dot{x}_k \end{bmatrix} = \begin{bmatrix} f_1(x_1, g_1(\hat{x}_1)) \\ \vdots \\ f_i(x_i, g_i(\hat{x}_i)) \\ \vdots \\ f_k(x_k, g_k(\hat{x}_k)) \end{bmatrix} \tag{27}$$

be an interconnected system of $f(x)$.

There exists an additively separable continuous function $\varphi : \mathbb{R}^n \to \mathbb{R}$ such that

$$\varphi(x) \leq 0 \quad \forall x \in X_0, \tag{28a}$$

$$\varphi(x) > 0 \quad \forall x \in X_{\mathrm{u}}, \text{ and} \tag{28b}$$

$$\frac{\partial \varphi}{\partial x}(x) f(x) \leq 0 \quad \forall x \in X \tag{28c}$$

if and only if for $i = 1, \dots, k$ there exist continuous functions $\varphi_i : \mathbb{R}^{n_i} \to \mathbb{R}$ and $\gamma_i : \mathbb{R}^{q_i + m_i} \to \mathbb{R}$ and constants $\alpha_i, \beta_i \in \mathbb{R}$ such that

$$\varphi_i(x_i) + \alpha_i \leq 0 \quad \forall x \in X_0, \tag{29a}$$

$$\varphi_i(x_i) - \beta_i > 0 \quad \forall x \in X_{\mathrm{u}}, \tag{29b}$$

$$\frac{\partial \varphi_i}{\partial x_i}(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \quad \forall x \in X \tag{29c}$$

and

$$\sum_i \alpha_i \geq 0, \tag{29d}$$

$$\sum_i \beta_i \geq 0, \text{ and} \tag{29e}$$

$$\sum_i \gamma_i(h_i(x_i), g_i(\hat{x}_i)) \leq 0. \tag{29f}$$

Proof: The conditions (29) implies (28) directly. Therefore, we only show the opposite direction. Suppose φ is additively separable, then per definition there exist continuous functions $\varphi_i : \mathbb{R}^{n_i} \to \mathbb{R}$ such that

$$\varphi(x) = \sum_i \varphi_i(x_i) \quad \forall x \in X. \tag{30}$$

This implies that (28) can be written as

$$\sum_i \varphi_i(x_i) \leq 0 \quad \forall x \in X_0, \tag{31a}$$

$$\sum_i \varphi_i(x_i) > 0 \quad \forall x \in X_{\mathrm{u}}, \text{ and} \tag{31b}$$

$$\sum_i \frac{\partial \varphi_i}{\partial x_i}(x_i) f_i(x_i, g_i(\hat{x}_i)) \leq 0 \quad \forall x \in X. \tag{31c}$$

From Lemma 1, it follows directly that (31a) is equivalent to (29a) and (29d). In addition, (31b) is equivalent to (29b) and (29e). Finally, Lemma 3 shows that (28c) is equivalent to (29c) and (29f). ■

Remark that to generate the additively separable barrier functions, one should only use the sum of bases in x_i for $i \in \{1, \ldots, k\}$.

To clarify the theorem, two examples are provided. Example 1 demonstrates the necessity of α_i and β_i, and Example 2 demonstrates the restrictiveness of assuming that φ is additively separable.

Example 1: Consider the following simple dynamical system

$$\Sigma_1 : \dot{x} = -x \tag{32a}$$

$$\Sigma_2 : \dot{y} = -y \tag{32b}$$

where $x, y \in \mathbb{R}$. The system is split into two independent dynamical systems Σ_1 and Σ_2. The set of initial states is $X_0 = [4,5] \times [4,5]$ and the set of unsafe states is $X_{\mathrm{u}} = [1,2] \times [4,5]$. The vector field, X_0, and X_{u} are illustrated in Fig. 2.

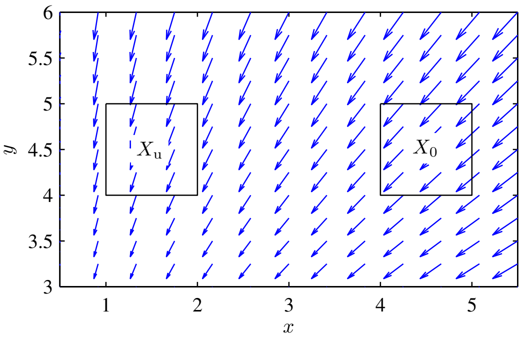

Fig. 2. Vector field (blue arrows) and safe and unsafe sets (black boxes).

From X_0 and X_{u}, it is seen that there exists no function φ_2 such that $\varphi_2(y) \leq 0$ for all $y \in [4,5]$ and $\varphi_2(y) > 0$ for all $y \in [4,5]$. Therefore, the constants α_i and β_i are necessarily different from zero, even though the dynamics is completely decoupled for the two subsystems.

An additively separable barrier certificate $\varphi = \sum_i \varphi_i$ is given by $\varphi_1 = 0.26x^4 - 2x^3 + 3x^2 + 2.65$ and $\varphi_2 = 0.1y^2 - 1.6$. For $\alpha_1 = 2.2$, $\alpha_2 = -1.8$, $\beta_1 = 1.2$, $\beta_2 = -0.8$, the conditions in (29) are satisfied.

In the next example, we show that compositional barrier certificates cannot always be generated, even for linear systems with real eigenvalues.

Example 2: Consider the following 2-dimensional dynamical system

$$\Sigma_1 : \dot{x} = -x + y \tag{33a}$$

$$\Sigma_2 : \dot{y} = -y \tag{33b}$$

where $x, y \in \mathbb{R}$. The system is split into two subsystems Σ_1 and Σ_2, and the state of Σ_2 is input to Σ_1. We consider a compact set of the state space $(x,y) \in V$, where $V \equiv [-a,a] \times [-b,b]$ and $a, b \in \mathbb{R}_{\geq 0}$.

We show that it is not possible to generate any meaningful additively separable barrier certificate $\varphi(x,y) = \varphi_i(x) + \varphi_i(y)$. For convenience, let $p_1 \equiv \partial\varphi_1/\partial x$ and $p_2 \equiv \partial\varphi_2/\partial y$. Then $\varphi(x,y)$ is nonincreasing along the vector field if

$$p_1(x)(-x+y) - yp_2(y) \leq 0 \quad \forall (x,y) \in V. \tag{34}$$

It is seen that

$$\begin{cases} p_1(x) \geq 0 \text{ for } x > 0 \\ p_1(x) \leq 0 \text{ for } x < 0 \end{cases} \tag{35a}$$

$$\begin{cases} p_1(x) - p_2(y) \leq 0 \text{ for } y > 0 \\ p_1(x) - p_2(y) \geq 0 \text{ for } y < 0. \end{cases} \tag{35b}$$

This implies that $p_2(y) \geq p_1(x) \geq 0$ for $y > 0$ and $0 \leq p_1(x) \geq p_2(y)$ for $y < 0$; hence, $p_2(y) \geq \sup_{x \in [-a,a]} p_1(x)$ for $y > 0$ and $p_2(y) \leq \inf_{x \in [-a,a]} p_1(x)$ for $y < 0$. It is seen that $p_2(y)$ makes a jump at $y = 0$ unless p_1 is the zero polynomial. This implies that we can verify nothing about Σ_1, i.e., our analysis will say that solutions may reach the entire state space for every initial condition.

Note other compositional methods for the analysis of dynamical systems do not apply for the previous example either. For an example, see the compositional stability condition given in [10].

V. Refined Compositional Analysis

To alleviate the issue experienced in Example 2, we propose another condition for safety, which at the cost of more coupling variables handles the previous example. The idea is to let each φ_i depend on both x_i and $g_i(\hat{x}_i)$.

To simplify the notation of the problem, we define the set of neighbors for subsystem i, as the set of subsystems, which has an output that is an input to subsystem i. The set of neighbors is defined from the adjacency matrix E, see (10), describing the interconnection of the subsystems. We say that the neighbors of subsystem i have the following indices

$$\mathcal{N}_i = \{j \in \{1, \ldots, k\} | E(i,j) = 1\}. \tag{36}$$

We define $\bar{\mathcal{N}_i} \equiv \mathcal{N}_i \cup \{i\}$. The complement of $\bar{\mathcal{N}_i}$ is given as

$$\bar{\mathcal{N}}_i^{\mathrm{c}} = \{1, \ldots, k\} \backslash \bar{\mathcal{N}_i}. \tag{37}$$

Let $z = (z_1, \ldots, z_k)$ and $A \subseteq \{1, \ldots, k\}$, then we define $\hat{z}_A \equiv \{z_i | i \in \{1, \ldots, k\} \backslash A\}$ and $z_A \equiv \sum_{i \in A} z_i$.

Now, we can state the refined safety condition as follows.

Proposition 2: Let $k \in \mathbb{N}$, and let

$$\begin{bmatrix} \dot{x}_1 \\ \vdots \\ \dot{x}_i \\ \vdots \\ \dot{x}_k \end{bmatrix} = \begin{bmatrix} f_1(x_1, g_1(\hat{x}_1)) \\ \vdots \\ f_i(x_i, g_i(\hat{x}_i)) \\ \vdots \\ f_k(x_k, g_k(\hat{x}_k)) \end{bmatrix} \tag{38}$$

be an interconnected system of $f(x)$.

There exists a continuous function $\varphi : \mathbb{R}^n \to \mathbb{R}$ given by

$$\varphi(x) = \sum_i \varphi_i(x_i, g_i(\hat{x}_i)) \quad \forall x \in \mathbb{R}^n \tag{39}$$

such that

$$\varphi(x) \leq 0 \quad \forall x \in X_0, \tag{40a}$$

$$\varphi(x) > 0 \quad \forall x \in X_{\mathrm{u}}, \text{ and} \tag{40b}$$

$$\frac{\partial \varphi}{\partial x}(x) f(x) \leq 0 \quad \forall x \in X \tag{40c}$$

if and only if for $i \in \{1, \ldots, k\}$ there exist continuous functions $\gamma_i : \mathbb{R}^{q_{\bar{\mathcal{N}}_i} + m_{\mathcal{N}_i}} \to \mathbb{R}$, $\alpha_i : \mathbb{R}^{q_i + m_i} \to \mathbb{R}$, and $\beta_i : \mathbb{R}^{q_i + m_i} \to \mathbb{R}$ such that

$$\varphi_i(x_i, g_i(\hat{x}_i)) + \alpha_i(h_i(x_i), g_i(\hat{x}_i)) \leq 0 \quad \forall x \in X_0, \tag{41a}$$

$$\varphi_i(x_i, g_i(\hat{x}_i)) - \beta_i(h_i(x_i), g_i(\hat{x}_i)) > 0 \quad \forall x \in X_{\mathrm{u}}, \tag{41b}$$

$$\begin{aligned} &\sum_{j \in \bar{\mathcal{N}}_i} \frac{\partial \varphi_i}{\partial x_j}(x_i, g_i(\hat{x}_i)) f_j(x_j, g_j(\hat{x}_j)) \\ &\quad \leq \gamma_i(\hat{x}_{\mathcal{N}_i^{\mathrm{c}}}, \hat{g}_{\mathcal{N}_i^{\mathrm{c}}}(\hat{x}_{\mathcal{N}_i^{\mathrm{c}}})) \quad \forall x \in X \end{aligned} \tag{41c}$$

and

$$\begin{aligned} &\sum_i \alpha_i(h_i(x_i), g_i(\hat{x}_i)) \geq 0, \\ &\sum_i \beta_i(h_i(x_i), g_i(\hat{x}_i)) \geq 0, \\ &\sum_i \gamma_i(\hat{x}_{\mathcal{N}_i^{\mathrm{c}}}, \hat{g}_{\mathcal{N}_i^{\mathrm{c}}}(\hat{x}_{\mathcal{N}_i^{\mathrm{c}}})) \leq 0. \end{aligned} \tag{41d}$$

Proof: The equivalence between (40a) and (41a), and (40b) and (41b) follows directly from the proof of Lemma 3 starting from (24) to the end of the proof. To obtain (41c), observe that $\frac{\partial \varphi_i}{\partial x_j}(x_i, g_i(\hat{x}_i))$ is only nonzero for $j \in \bar{\mathcal{N}}_i$. For each nonzero partial derivative, $\partial \varphi_i / \partial x_j$ is multiplied by $f_j(x_j, g_j(\hat{x}_j))$ that is a function of x_j and $g_j(\hat{x}_j)$. This implies that the left hand side of (41c) depends on $\hat{x}_{\bar{\mathcal{N}}_i^{\mathrm{c}}}$ (states of subsystem i and its neighbors) and $\hat{g}_{\mathcal{N}_i^{\mathrm{c}}}(\hat{x}_{\mathcal{N}_i^{\mathrm{c}}})$ (the neighbors inputs - not its own, as their states are already in γ_i). ■

The seemingly subtle change of φ_i has a great impact on the number of coupling variables involved in the generation of the barrier certificate. Therefore, one should only include $g_i(\hat{x}_i)$ in φ_i if it is really necessary. Remark that a subset of functions φ_i may be dependent of $g_i(\hat{x}_i)$, while others may only depend on x_i. Note that the issue of Example 2 is easily resolved, as one can generate quadratic forms in both x and y.

VI. Conclusion

We have classified the barrier certificates, which can be generated by a proposed compositional method for verifying the safety of continuous dynamical systems. It is shown that even for some linear systems, the compositional method fails to verify the safety.

Even though the compositional method is not as general as a centralized safety verification, it is very useful in the verification of high-dimensional systems, since it scales well in the number of states in the system. Therefore, the counterexamples where the compositional method fail should be used to generate ”good” decompositions of systems.

A second compositional condition for safety was proposed, which alleviates some of the issues of the initial method, but has a higher computational cost. Therefore, the choice of method is a compromise between generality and computational complexity. Therefore, our future work is to identify the necessary structure of the barrier certificate based on the vector field.

References

[1] H. Guéguen, M.-A. Lefebvre, J. Zaytoon, and O. Nasri, “Safety verification and reachability analysis for hybrid systems,” *Annual Reviews in Control*, vol. 33, no. 1, pp. 25–36, 2009.

[2] I. Mitchell, A. Bayen, and C. Tomlin, “A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games,” *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, 2005.

[3] J. Ding, J. H. Gillula, H. Huang, M. P. Vitus, W. Zhang, and C. J. Tomlin, “Hybrid systems in robotics,” *IEEE Robotics & Automation Magazine*, vol. 18, no. 3, pp. 33–43, September 2011.

[4] A. Girard and G. Pappas, “Verification using simulation,” in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2006, vol. 3927, pp. 272–286.

[5] A. Abate, A. Tiwari, and S. Sastry, “Box invariance in biologically-inspired dynamical systems,” *Automatica*, vol. 45, no. 7, pp. 1601–1610, 2009.

[6] C. Sloth and R. Wisniewski, “Verification of continuous dynamical systems by timed automata,” *Formal Methods in System Design*, vol. 39, no. 1, pp. 47–82, 2011.

[7] 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, August 2007.

[8] S. Prajna and A. Jadbabaie, “Safety verification of hybrid systems using barrier certificates,” in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2004, vol. 2993, pp. 271–274.

[9] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo, “SOSTOOLS and its control applications,” in *Positive Polynomials in Control*, ser. Lecture Notes in Control and Information Sciences. Springer Berlin / Heidelberg, 2005, vol. 312, pp. 273–292.

[10] U. Topcu, A. Packard, and R. Murray, “Compositional stability analysis based on dual decomposition,” in *Proceedings of the 48th IEEE Conference on Decision and Control*, December 2009, pp. 1175–1180.

[11] F. Kerber and A. van der Schaft, “Compositional analysis for linear control systems,” in *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*. New York, NY, USA: ACM, 2010, pp. 21–30.

[12] C. Sloth, G. J. Pappas, and R. Wisniewski, “Compositional safety analysis using barrier certificates,” in *Proceedings of Hybrid Systems: Computation and Control*, 2012, pp. 15–23.

[13] G. V. Smirnov, *Introduction to the Theory of Differential Inclusions*, ser. Graduate Studies in Mathematics. American Mathematical Society, 2002, vol. 41.

[14] P. A. Parrilo, “Semidefinite programming relaxations for semialgebraic problems,” *Mathematical Programming*, vol. 96, no. 2, pp. 293–320, 2003.