2018 European Control Conference (ECC)
June 12-15, 2018. Limassol, Cyprus

On the Composition of Discrete and Continuous-time Assume-Guarantee Contracts for Invariance*

Adnane Saoud[1,2], Antoine Girard[1] and Laurent Fribourg[2]

Abstract— **Many techniques for verifying invariance properties are limited to systems of moderate size. In this paper, we propose an approach based on assume-guarantee contracts and compositional reasoning for verifying invariance properties of a broad class of discrete-time and continuous-time systems consisting of interconnected components. The notion of assume-guarantee contracts makes it possible to divide responsibilities among the system components: a contract specifies an invariance property that a component must fulfill under some assumptions on the behavior of its environment (i.e. of the other components). We define weak and strong semantics of assume-guarantee contracts for both discrete-time and continuous-time systems. We then establish a certain number of results for compositional reasoning, which allow us to show that a global invariance property of the whole system is satisfied when all components satisfy their own contract. Interestingly, we show that the weak satisfaction of the contract is sufficient to deal with cascade compositions, while strong satisfaction is needed to reason about feedback composition. Specific results for systems described by differential inclusions are then developed. Throughout the paper, the main results are illustrated using simple examples.**

I. Introduction

The concept of positive invariance plays an important role in control theory (see [Bla99], [BM08] and the references therein). They allow, for instance, to verify that a set of unsafe states cannot be reached by the trajectories of a system starting in a given set of initial states. However, centralized approaches to verify invariance properties usually suffer from the curse of dimensionality and are limited to systems of moderate size. The study of invariance properties of dynamical systems using decentralized approaches has been an ongoing research area in recent years. Numerical methods have been developed to compute compositionally invariants [RKF10], [CVZ+12], [NO16], [SPW12], [CA15] under the form of ellipsoids, polytopes or level sets of (polynomial) functions. Other compositional approaches, using formal methods and symbolic techniques, are presented in [MGW15], [LFM+16]. All these works develop efficient computational techniques by making specific assumptions on the classes of dynamical systems and of sets to which they can be applied.

*This work has been supported by Labex DigiCosme (project ANR-11-LABEX-0045-DIGICOSME) operated by ANR as part of the program "Investissement d'Avenir" Idex Paris Saclay (ANR-11-IDEX-0003-02).

[1]Laboratoire des Signaux et Systèmes (L2S), CNRS, CentraleSupélec, Université Paris-Sud, Université Paris-Saclay, 3, rue Joliot-Curie, 91192 Gif-sur-Yvette, cedex, France. {adnane.saoud,antoine.girard}@l2s.centralesupelec.fr

[2]Laboratoire Spécification et Vérification, CNRS, ENS Paris-Saclay, 61, avenue du Président Wilson, 94235 Cachan Cedex, France. fribourg@lsv.ens-cachan.fr

In the current work, we aim at proposing a general theoretical framework and thus we make weak assumptions on systems and invariants. We initiate a high-level framework for verifying invariance properties of complex systems, consisting of interconnected components, using a contract-based approach [BCN+15]. Each component is assigned an assume-guarantee contract, which specifies the invariance property that the component must fulfill under assumption about its environment (i.e. the other components). We introduce contracts and define weak and strong semantics for both discrete-time and continuous-time systems. We then establish results that allow us to reason compositionally using assume-guarantee contracts: i.e. if all components satisfy their own contract then a global invariance property of the whole system is satisfied.

Assume-guarantee reasoning have been previously used in control theory. The authors in [KVDS09] presented a compositionality result for linear dynamical systems based on the notion of simulation introduced in [VdS04]. In spirit, our work is closer to the framework presented in [KAS17] for verifying general properties (not only invariance) using parametric assume-guarantee contracts and compositional reasoning by means of small-gain theorems. However, the main compositionality result in that work requires to assume that at least one component satisfies a contract (for some parameter value), independently of the behavior of other components. This breaks the circularity of implications of the assume-guarantee contracts, which is arguably the main difficulty in rigorous contract-based design. In the present work, we do not make such an assumption.

The paper is organized as follows. In Section II, we introduce the class of systems and interconnections considered through the paper. In Section III, we introduce assume-guarantee contracts, their weak and strong semantics and we establish compositionality results for reasoning about interconnected systems. In Section IV, we develop specific results for systems described by differential inclusions. Throughout the paper, simple examples are used as illustrations of the main results. Due to space constraints, The proofs for the propositions and theorems can be found in the appendix of the online version of this paper[1].

Notation: $\mathbb{Z}$, $\mathbb{N}$ and $\mathbb{N}^+$ denote the sets of integers, of non-negative integers, and of positive integers, respectively. $\mathbb{R}$, $\mathbb{R}_0^+$, $\mathbb{R}^+$ and $\mathbb{R}_0^-$ denote the sets of real, of non-negative real, of positive real and of non-positive real numbers, respectively. For $p \in \mathbb{N}$, $[0,p]_{\mathbb{N}} = [0,p] \cap \mathbb{N}$ is an interval

[1]Available at:https://hal.archives-ouvertes.fr/hal-01712710

of integers. The set of discrete-time domains is $\mathbb{I}(\mathbb{N}) = \{[0,a]_{\mathbb{N}},\ a \in \mathbb{N}\} \cup \{\mathbb{N}\}$ and the set of continuous-time domains is $\mathbb{I}(\mathbb{R}_0^+) = \{[0,a],\ a \in \mathbb{R}_0^+\} \cup \{[0,a),\ a \in \mathbb{R}^+\} \cup \{\mathbb{R}_0^+\}$. For $x \in \mathbb{R}^n$, $\|x\|$ denotes the Euclidean norm of x. $\mathbb{B}$ denotes the unit ball. For $\varepsilon \in \mathbb{R}^+$, $A \subseteq \mathbb{R}^n$ the ε-expansion of A is $\mathcal{B}_\varepsilon(A) = \{y \in \mathbb{R}^n \mid \exists x \in A, \|x-y\| \leq \varepsilon\}$. Given a set $A \subseteq \mathbb{R}^n$, its interior is denoted $Int(A)$.

II. Systems and interconnections

In this section, we introduce the classes of systems and interconnections considered throughout this paper, it is important to note that the classes of systems used in the paper are quite general, and includes deterministic and nondeterministic systems, in discrete-time or in continuous-time, described by difference or differential equations and inclusions and allows us to deal with phenomena such as sampling, time delays...

Definition 1: A *discrete-time system* is a tuple $\Sigma = (W, X, Y, \mathcal{T})$ where

- $W \subseteq \mathbb{R}^m$, $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^p$, are the sets of inputs, states, and outputs;
- $\mathcal{T}$ is a set of discrete-time trajectories $(w, x, y) : I \to W \times X \times Y$ where $I \in \mathbb{I}(\mathbb{N})$.

Definition 2: A *continuous-time system* is a tuple $\Sigma = (W, X, Y, \mathcal{T})$ where

- $W \subseteq \mathbb{R}^m$, $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^p$, are the sets of inputs, states, and outputs;
- $\mathcal{T}$ is a set of continuous-time trajectories $(w, x, y) : I \to W \times X \times Y$ where $I \in \mathbb{I}(\mathbb{R}_0^+)$, and $y : I \to Y$ are left-continuous functions.

Let us remark that trajectories of continuous-time systems are allowed to be discontinuous though left-continuity of the output is required for technical reasons.

We consider interconnections of systems of the same temporal nature (discrete or continuous-time) that can be described using cascade and feedback compositions, as shown in Figure 1. Our notions of cascade and feedback compositions are consistent with common usage and are formally defined below.

Definition 3: Let $\Sigma_1 = (W_1, X_1, Y_1, \mathcal{T}_1)$ and $\Sigma_2 = (W_2, X_2, Y_2, \mathcal{T}_2)$ be two systems such that $Y_1 \subseteq W_2$. The *cascade composition* of Σ_1 and Σ_2 is the system $\Sigma_1||_c\Sigma_2 = (W_1, X_1 \times X_2, Y_2, \mathcal{T}_c)$, such that $(w_1, (x_1, x_2), y_2) : I \to W_1 \times (X_1 \times X_2) \times Y_2$ belongs to $\mathcal{T}_c$ if and only if there exist $(w_1, x_1, y_1) : I_1 \to W_1 \times X_1 \times Y_1$ in $\mathcal{T}_1$, and $(w_2, x_2, y_2) : I_2 \to W_2 \times X_2 \times Y_2$ in $\mathcal{T}_2$ such that $I = I_1 \cap I_2$ and for all $t \in I$, $y_1(t) = w_2(t)$.

Definition 4: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a system such that $Y \subseteq W$. The *feedback composition* of Σ is the system $\Sigma_f = (\{0\}, X, \{0\}, \mathcal{T}_f)$, such that $(0, x, 0) : I \to \{0\} \times X \times \{0\}$ belongs to $\mathcal{T}_f$ if and only if there exists $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ such that for all $t \in I$, $y(t) = w(t)$.

Note that systems resulting from feedback composition have trivial null inputs and outputs. Hence, with an abuse of notation, we will denote $\Sigma_f = (X, \mathcal{T}_f)$ and $x \in \mathcal{T}_f$, with $x : I \to X$.

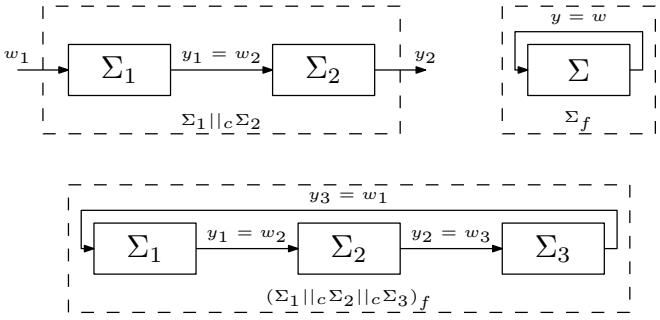

Fig. 1. Cascade, feedback compositions and an example of interconnection of systems

We should emphasize that trajectories of systems need not be defined on the whole time domains $\mathbb{N}$ or $\mathbb{R}_0^+$. This makes it possible to avoid forward-completeness issues related to feedback composition as shown in the following example.

Example 1: Let us consider $\Sigma = (W, X, Y, \mathcal{T})$ where $W = X = Y = \mathbb{R}$. A trajectory of Σ is a triple $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ where $I \in \mathbb{I}(\mathbb{R}_0^+)$, w is continuous, x and y are differentiable and such that $x(0) = 1$ and for all $t \in I$,

$$\begin{cases} \dot{x}(t) &= w(t) \\ y(t) &= x^2(t). \end{cases}$$

It is clear that Σ has trajectories defined on the whole time domain $\mathbb{R}_0^+$. However, if we only consider those trajectories, the set of trajectories $\mathcal{T}_f$ of the feedback composition Σ_f would be empty since the trajectories of $\mathcal{T}_f$ are of the form $x : I \to X$ where $I \subseteq [0, 1)$, and for all $t \in I$, $x(t) = \frac{1}{1-t}$.

III. Assume-guarantee reasoning for invariance

A. Assume-guarantee contracts

An assume-guarantee contract is a compositional tool that specifies how a system behaves under assumptions about its inputs [BCN+15]. The use of assume-guarantee contracts makes it possible to reason on a global system based on properties of its components. In this section, we introduce assume-guarantee contracts to reason on invariance properties of discrete or continuous-time systems. These contracts are equipped with a weak and a strong semantics, which will allow us to establish compositionality results. Let us first define contracts for discrete-time systems:

Definition 5: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a discrete-time system, an *assume-guarantee contract* for Σ is a tuple $\mathcal{C} = (A_W, G_X, G_Y)$ where

- $A_W \subseteq W$ is a set of assumptions;
- $G_X \subseteq X$ and $G_Y \subseteq Y$ are sets of guarantees.

We say that Σ *(weakly) satisfies* $\mathcal{C}$, denoted $\Sigma \models \mathcal{C}$, if for all trajectories $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$:

- for all $l \in I$, such that for all $k \in [0, l]_{\mathbb{N}}$, $w(k) \in A_W$, we have:
  - for all $k \in [0, l]_{\mathbb{N}}$, $x(k) \in G_X$;

– for all $k \in [0,l]_{\mathbb{N}}$, $y(k) \in G_Y$.

We say that Σ *strongly satisfies* $\mathcal{C}$, denoted $\Sigma \models_s \mathcal{C}$, if for all trajectories $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}$:

- $y(0) \in G_Y$;
- for all $l \in I$, such that for all $k \in [0,l]_{\mathbb{N}}$, $w(k) \in A_W$, we have:
  – for all $k \in [0,l]_{\mathbb{N}}$, $x(k) \in G_X$;
  – for all $k \in [0,l+1]_{\mathbb{N}} \cap I$, $y(k) \in G_Y$.

Let us remark that $\Sigma \models_s \mathcal{C}$ obviously implies $\Sigma \models \mathcal{C}$. Intuitively, an assume-guarantee contract for a discrete-time system states that if the input of the system belongs to A_W up to a time $l \in \mathbb{N}$, then the state of the system belongs to G_X at least until l and the output of the system belongs to G_Y at least until l, or until $l+1$ in the case of strong satisfaction. We now introduce contracts for continuous-time systems:

Definition 6: Let $\Sigma = (W,X,Y,\mathcal{T})$ be a continuous-time system, an *assume-guarantee contract* for Σ is a tuple $\mathcal{C} = (A_W, G_X, G_Y)$ where

- $A_W \subseteq W$ is a set of assumptions;
- $G_X \subseteq X$ and $G_Y \subseteq Y$ are sets of guarantees, where G_Y is closed.

We say that Σ *(weakly) satisfies* $\mathcal{C}$, denoted $\Sigma \models \mathcal{C}$, if for all trajectories $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}$:

- for all $t \in I$, such that for all $s \in [0,t]$, $w(s) \in A_W$, we have:
  – for all $s \in [0,t]$, $x(s) \in G_X$;
  – for all $s \in [0,t]$, $y(s) \in G_Y$.

We say that Σ *strongly satisfies* $\mathcal{C}$, denoted $\Sigma \models_s \mathcal{C}$, if for all trajectories $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}$:

- $y(0) \in G_Y$;
- for all $t \in I$, such that for all $s \in [0,t]$, $w(s) \in A_W$, we have:
  – for all $s \in [0,t]$, $x(s) \in G_X$;
  – there exists $\delta > 0$, such that for all $s \in [0,t+\delta] \cap I$, $y(s) \in G_Y$.

Again, $\Sigma \models_s \mathcal{C}$ obviously implies $\Sigma \models \mathcal{C}$. An assume-guarantee contract for a continuous-time system states that if the input of the system belongs to A_W up to a time $t \in \mathbb{R}_0^+$, then the state of the system belongs to G_X at least until t, and the output of the system belongs to G_Y at least until t, or until $t+\delta$ with $\delta > 0$ in the case of strong satisfaction. Let us remark that the value of δ may depend on the trajectory $(w,x,y) \in \mathcal{T}$ and on the value of the time instant $t \in I$, which makes a noticeable difference with the discrete-time case. Another difference is that for technical reasons, in the continuous-time case, the set G_Y is required to be closed.

B. Compositional reasoning

We now provide results allowing to reason about interconnected systems based on contracts satisfied by the components. The results apply equally to discrete or continuous-time systems.

Firstly, we provide the following result on assume-guarantee contracts under cascade composition:

Theorem 1 (Contracts under cascade composition): Let $\Sigma_i = (W_i, X_i, Y_i, \mathcal{T}_i)$, $i = 1,2$ be systems with $Y_1 \subseteq W_2$. Let $\mathcal{C}_i = (A_{W_i}, G_{X_i}, G_{Y_i})$ be assume-guarantee contracts for Σ_i, $i = 1,2$ with $G_{Y_1} \subseteq A_{W_2}$, and let $\mathcal{C}_c = (A_{W_1}, G_{X_1} \times G_{X_2}, G_{Y_2})$. The following implications hold:

- If $\Sigma_1 \models \mathcal{C}_1$ and $\Sigma_2 \models \mathcal{C}_2$, then $\Sigma_1 ||_c \Sigma_2 \models \mathcal{C}_c$;
- If $\Sigma_1 \models_s \mathcal{C}_1$ and $\Sigma_2 \models \mathcal{C}_2$, then $\Sigma_1 ||_c \Sigma_2 \models_s \mathcal{C}_c$;
- If $\Sigma_1 \models \mathcal{C}_1$ and $\Sigma_2 \models_s \mathcal{C}_2$, then $\Sigma_1 ||_c \Sigma_2 \models_s \mathcal{C}_c$.

Secondly, we provide a result on feedback composition:

Theorem 2 (Contracts under feedback composition): Let $\Sigma = (W,X,Y,\mathcal{T})$ be a system with $Y \subseteq W$ and let $\Sigma_f = (X, \mathcal{T}_f)$. Let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ with $G_Y \subseteq A_W$. If $\Sigma \models_s \mathcal{C}$ then, for all trajectories $x : I \to X$ in $\mathcal{T}_f$, we have for all $t \in I$, $x(t) \in G_X$.

Let us remark that, for continuous-time systems, the left-continuity of the output trajectories and the closedness of the guarantee set G_Y are crucial for the proof of Theorem 2.

Let us point out that weak semantics is generally insufficient to reason on feedback composition, as shown by the following counter-example:

Example 2: Let us consider $\Sigma = (W,X,Y,\mathcal{T})$ where $W = X = Y = \mathbb{R}_0^+$. A trajectory of Σ is a triple $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}$ where $I = \mathbb{R}_0^+$, w is continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w(t)} \\ y(t) &= x(t). \end{cases}$$

Let us consider the assume-guarantee contract $\mathcal{C} = (\{0\},\{0\},\{0\})$ for Σ. We can easily check that $\Sigma \models \mathcal{C}$. However, the conclusion of the previous theorem does not hold. Indeed, the map $x : \mathbb{R}_0^+ \to X$ defined by $x(t) = t^2/4$ can be shown to belong to $\mathcal{T}_f$ and there exists $t \in \mathbb{R}_0^+$ such that $x(t) \notin G_X = \{0\}$.

It is clear from the previous example that strong satisfaction is needed to reason about feedback interconnections. We show two modifications of the previous example, based on sampling or time-delays, which lead to strong satisfaction of the contract:

Example 3: Let the system $\Sigma_1 = (W,X,Y,\mathcal{T}_1)$ where $W = X = Y = \mathbb{R}_0^+$. A trajectory of Σ_1 is a triple $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}_1$ where $I = \mathbb{R}_0^+$, w is continuous, x is differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w(t)} & \\ y(t) &= 0 & 0 \le t \le t_0 \\ y(t) &= x(t_k) & t_k < t \le t_{k+1},\ k \in \mathbb{N}. \end{cases}$$

where $(t_k)_{k\in\mathbb{N}}$ a strictly increasing sequence of sampling instants with $t_0 \ge 0$ and $t_k \to +\infty$ when $k \to +\infty$. Let us remark that y is left-continuous. Let us consider the assume-guarantee contract $\mathcal{C} = (\{0\},\{0\},\{0\})$ for Σ. We can easily check that $\Sigma \models_s \mathcal{C}$, where the value of δ as in Definition 6 is

given by $\delta = t_{k+1} - t$ if $t_k \leq t < t_{k+1}$. We can also check that the conclusion of the previous theorem holds since the only trajectory $x : \mathbb{R}_0^+ \to X$ in $\mathcal{T}_f$ is given by $x(t) = 0$, for all $t \in \mathbb{R}_0^+$.

Example 4: Let the system $\Sigma_2 = (W, X, Y, \mathcal{T}_2)$ where $W = X = Y = \mathbb{R}_0^+$. A trajectory of Σ_2 is a triple $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}_2$ where $I = \mathbb{R}_0^+$, w is continuous, x is differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w(t)} \\ y(t) &= 0 & 0 \leq t \leq T \\ y(t) &= x(t-T) & T < t. \end{cases}$$

where $T > 0$ is a time delay. Let us remark that y is left-continuous. Let us consider the assume-guarantee contract $\mathcal{C} = (\{0\}, \{0\}, \{0\})$ for Σ. We can easily check that $\Sigma \models_s \mathcal{C}$, where the value of δ as in Definition 6 is given by $\delta = T$. We can also check that the conclusion of the previous theorem holds since the only trajectory $x : \mathbb{R}_0^+ \to X$ in $\mathcal{T}_f$ is given by $x(t) = 0$, for all $t \in \mathbb{R}_0^+$.

It can be seen from the Examples 3 and 4 that our framework is suitable to reason on systems that includes some sampled or delayed behaviors. Moreover, these examples suggest that by sampling or delaying the output of a component, strong satisfaction of a contract can be obtained. These examples also show how one can go from weak to strong satisfaction by slightly modifying the system, in the next section we show that this is also possible by slightly modifying the contract.

Remark 1: Theorems 1 and 2 apply to a very general class of systems. When considering more specific classes, one can sometimes reason on feedback composition without strong contract satisfaction. Such a case will be shown in Section IV, where we consider systems modeled by Lipschitz differential inclusions.

C. From weak to strong contract satisfaction

In this section, we show that under some additional assumptions (continuity of output trajectories and strict inclusion of guarantees G_Y in assumptions A_W), it is possible to reason about feedback compositions using the weak semantics of assume guarantee contracts. The results of this section only apply to continuous-time systems:

Proposition 1: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a continuous-time system and let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ. Let us assume that for all trajectories $(w, x, y) \in \mathcal{T}$, y is continuous and $y(0) \in G_Y$. If $\Sigma \models \mathcal{C}$, then for all $\varepsilon > 0$, $\Sigma \models_s \mathcal{C}_\varepsilon$ where $\mathcal{C}_\varepsilon = (A_W, G_X, \mathcal{B}_\varepsilon(G_Y) \cap Y)$.

The following result on feedback composition, stated without proof, is a direct consequence of Proposition 1 and Theorem 2:

Corollary 1: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a system with $Y \subseteq W$ and let $\Sigma_f = (X, \mathcal{T}_f)$. Let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ such that $\mathcal{B}_\varepsilon(G_Y) \cap Y \subseteq A_W$ for some $\varepsilon > 0$. Let us assume that that for all trajectories $(w, x, y) \in \mathcal{T}$, y is continuous and $y(0) \in G_Y$. If $\Sigma \models \mathcal{C}$, then for all trajectories $x : I \to X$ in $\mathcal{T}_f$, we have for all $t \in I$, $x(t) \in G_X$.

The following example shows an application of the previous corollary:

Example 5: Let the system $\Sigma = (W, X, Y, \mathcal{T})$ where $W = X = Y = \mathbb{R}_0^+$. A trajectory of Σ is a triple $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ where $I = \mathbb{R}_0^+$, w is continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w(t)} - x(t) \\ y(t) &= x(t). \end{cases}$$

Let $a > 1$, let us consider the assume-guarantee contract $\mathcal{C} = (A_W, G_X, G_Y)$ for Σ where $A_W = [0, a^2]$, $G_X = G_Y = [0, a]$. We have $\mathcal{B}_\varepsilon(G_Y) \cap Y = [0, a + \varepsilon] \subseteq [0, a^2] = A_W$ for some $\varepsilon > 0$. It is easy to check that $\Sigma \models \mathcal{C}$ and that for all trajectories $(w, x, y) \in \mathcal{T}$, y is continuous and $y(0) = 0 \in G_Y$. Then, from Corollary 1, it follows that for all trajectories $x : I \to X$ in $\mathcal{T}_f$, $x(t) \in [0, a]$ for all $t \in \mathbb{R}_0^+$. In addition, since this holds for all $a > 1$, one can conclude that $x(t) \in [0, 1]$ for all $t \in \mathbb{R}_0^+$. Let us remark that there exists non-zero trajectories in $\mathcal{T}_f$ such as $x : \mathbb{R}_0^+ \to X$ defined by $x(t) = (1 - e^{-t/2})^2$, for all $t \in \mathbb{R}_0^+$.

It is important to note that Corollary 1 cannot be applied when $\mathcal{B}_\varepsilon(G_Y) \cap Y \subsetneq A_W$, for any $\varepsilon > 0$, and in particular, when $G_Y = A_W$ and $G_Y \neq Y$.

IV. Compositional invariants for differential inclusions

In this section, we focus on continuous-time systems $\Sigma = (W, X, Y, \mathcal{T})$ defined by differential inclusions. We use the classical characterization of invariant sets for differential inclusions developed using the concept of contingent cone (see [Aub09] and the references therein) to derive sufficient conditions for weak satisfaction of assume-guarantee contracts. We also show that invariant sets can be combined under cascade and feedback composition, making it possible to reason compositionally without strong satisfaction of assume-guarantee contracts.

A trajectory of Σ is a triple $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ where $I \in \mathbb{I}(\mathbb{R}_0^+)$, w is locally measurable, x and y are absolutely continuous and continuous, respectively, and satisfy for almost all $t \in I$:

$$\begin{cases} \dot{x}(t) &\in F(x(t), w(t)), \quad x(0) \in X^0 \\ y(t) &= h(x(t)) \end{cases} \tag{1}$$

where $F : \mathbb{R}^n \times \mathbb{R}^m \rightrightarrows \mathbb{R}^n$ is a set-valued map, $h : \mathbb{R}^n \to \mathbb{R}^p$ is continuous and X^0 is the set of initial conditions. Let us introduce the following assumption on the system Σ:

Assumption 1: The set-valued map[2] $F : \mathbb{R}^n \times \mathbb{R}^m \rightrightarrows \mathbb{R}^n$ is locally Lipschitz, has compact values and $X \times W \subseteq$

[2]Given a set-valued map $F : \mathbb{R}^q \rightrightarrows \mathbb{R}^n$, the domain of F is $dom(F) = \{z \in \mathbb{R}^q |\ F(z) \neq \emptyset\}$. F is said to be locally Lipschitz if for all $z \in Int(dom(F))$, there exists a neighborhood U of z and a constant $L \geq 0$ (the Lipschitz constant) such that for every $z_1, z_2 \in U \cap dom(F)$, $F(z_1) \subseteq F(z_2) + L||z_1 - z_2||\mathbb{B}$. It has compact values if for all $z \in dom(F)$, $F(z)$ is compact.

$Int(dom(F))$. The map[3] $h : \mathbb{R}^n \to \mathbb{R}^p$ satisfies $X \subseteq Int(dom(h))$ and $h(X) \subseteq Y$.

Given systems $\Sigma_i = (W_i, X_i, Y_i, \mathcal{T}_i)$ of the form (1) with maps and initial sets F_i, h_i, X_i^0, $i = 1, 2$, and $Y_1 \subseteq W_2$, their cascade composition $\Sigma_1 ||_c \Sigma_2$ can be written under the same form with maps F_c, h_c and initial set X_c^0 given by

$$\begin{array}{rcl} F_c(x_1, x_2, w_1) & = & F_1(x_1, w_1) \times F_2(x_2, h_1(x_1)), \\ h_c(x_1, x_2) & = & h_2(x_2), \\ X_c^0 & = & X_1^0 \times X_2^0. \end{array}$$

The feedback composition Σ_f of $\Sigma = (W, X, Y, \mathcal{T})$ of the form (1) with $Y \subseteq W$ can also be written as a differential inclusion under the form:

$$\dot{x}(t) \in F_f(x(t)),\ x(0) \in X^0,$$

where $F_f(x) = F(x, h(x))$. Note that these representations are consistent with those given in Definitions 3 and 4.

The following technical result is straightforward and is stated without proof:

Claim 1: The following properties hold:

- If h_1 is locally Lipschitz and Assumption 1 holds for Σ_1 and Σ_2, then it holds for $\Sigma_1 ||_c \Sigma_2$;
- If h is locally Lipschitz and Assumption 1 holds for Σ, then F_f is locally Lipschitz, has compact values and $X \subseteq Int(dom(F_f))$.

A. Invariants relative to assume-guarantee contracts

We give sufficient conditions for weak satisfaction of assume-guarantee contracts based on the classical characterization of invariant sets for differential inclusions (see e.g. Theorem 5.3.4 in [Aub09]).

Definition 7: Let $K \subseteq \mathbb{R}^n$ and $x \in K$, the *contingent cone* to set K at point x, denoted $T_K(x)$, is given by:

$$T_K(x) = \left\{ z \in \mathbb{R}^n \mid \liminf_{h \to 0^+} \frac{d_K(x + hz)}{h} = 0 \right\}$$

where $d_K(y)$ denotes the distance of y to K, defined by $d_K(y) = \inf_{y' \in K} ||y - y'||$.

Definition 8: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a continuous-time system described by (1). Let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ with a compact set of assumptions A_W. A closed set $K \subseteq X$ is said to be an *invariant of* Σ *relative to the contract* $\mathcal{C}$ if the following conditions hold:

(i) $X^0 \subseteq K \subseteq G_X \cap h^{-1}(G_Y)$;
(ii) for all $x \in K$, $F(x, A_W) \subseteq T_K(x)$.

where the set-valued map $F(., A_W) = \bigcup_{w \in A_W} F(., w)$.

We prove that the existence of an invariant of Σ relative to a contract $\mathcal{C}$ implies the weak satisfaction of this contract.

Proposition 2: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a continuous-time system described by (1) such that Assumption 1 holds. Let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ with a compact set of assumptions A_W. If there exists a closed set $K \subseteq X$ invariant of Σ relative to the contract $\mathcal{C}$ then $\Sigma \models \mathcal{C}$.

B. Composition of invariants

We now provide results allowing to reason about interconnected systems based on invariants of their components.

Firstly, we provide the following result on cascade composition:

Theorem 3 (Invariants under cascade composition): Let $\Sigma_i = (W_i, X_i, Y_i, \mathcal{T}_i)$, be continuous-time systems described by (1) with maps and initial sets F_i, h_i, X_i^0, $i = 1, 2$, and $Y_1 \subseteq W_2$. Let us assume that h_1 is locally Lipschitz and Assumption 1 holds for Σ_1 and Σ_2. Let $\mathcal{C}_i = (A_{W_i}, G_{X_i}, G_{Y_i})$ be assume-guarantee contracts for Σ_i, with compact set of assumptions A_{W_i}, $i = 1, 2$ and $G_{Y_1} \subseteq A_{W_2}$. If there exist closed sets $K_i \subseteq X_i$ invariants of Σ_i relative to the contracts $\mathcal{C}_i$, $i = 1, 2$, then $K_1 \times K_2$ is an invariant of $\Sigma_1 ||_c \Sigma_2$ relative to the contract $\mathcal{C}_c = (A_{W_1}, G_{X_1} \times G_{X_2}, G_{Y_2})$.

Secondly, we provide a result on feedback composition:

Theorem 4 (Invariants under feedback composition): Let $\Sigma = (W, X, Y, \mathcal{T})$ be a continuous-time system described by (1) with maps and initial sets F, h, X^0, with $Y \subseteq W$ and let $\Sigma_f = (X, \mathcal{T}_f)$. Let us assume that h is locally Lipschitz and Assumption 1 holds for Σ. Let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ, with compact set of assumptions A_W and $G_Y \subseteq A_W$. If there exists a closed set $K \subseteq X$ invariant of Σ relative to the contract $\mathcal{C}$, then, for all trajectories $x : I \to X$ in $\mathcal{T}_f$, we have for all $t \in I$, $x(t) \in G_X$.

We show an example to illustrate the application of the previous theorems.

Example 6: Consider systems $\Sigma_i = (W_i, X_i, Y_i, \mathcal{T}_i)$, $i = 1, 2$ where $W_i = X_i = Y_i = \mathbb{R}$. A trajectory of Σ_i is a triple $(w_i, x_i, y_i) : I \to W_i \times X_i \times Y_i$ in $\mathcal{T}_i$ where $I = \mathbb{R}_0^+$, w_i is locally measurable, x_i and y_i are absolutely continuous and continuous, respectively, and satisfy for almost all $t \in I$:

$$\left\{ \begin{array}{rcl} \dot{x}_i(t) & = & f_i(x_i(t), w_i(t)) = -a_i x_i(t) + a_i w_i(t), \\ y_i(t) & = & h_i(x(t)) = x_i(t). \end{array} \right.$$

where $x_i(0) \in [0, b_i]$ with $a_i, b_i \in \mathbb{R}_0^+$, let $b = \max(b_1, b_2)$. Let us remark that h_i is locally Lipschitz and that Assumption 1 holds for Σ_i. We can easily check that for all $x \in [0, b]$, $f_i(x, [0, b]) \subseteq T_{[0,b]}(x)$, since

$$T_{[0,b]}(x) = \left\{ \begin{array}{lll} \mathbb{R}^+ & \text{if} & x = 0, \\ \mathbb{R}^- & \text{if} & x = b, \\ \mathbb{R} & \text{if} & x \in (0, b) \end{array} \right.$$

Then $[0, b]$ is an invariant of the system Σ_i, relative to the contract $\mathcal{C}_i = ([0, b], [0, b], [0, b])$. By Theorem 3, $[0, b]^2$ is an invariant of $\Sigma_1 ||_c \Sigma_2$ relative to the contract $\mathcal{C}_c = ([0, b], [0, b]^2, [0, b])$. Let $(\Sigma_1 ||_c \Sigma_2)_f = (X_1 \times X_2, \mathcal{T}_f)$, the

[3]Given a map $h : \mathbb{R}^n \to \mathbb{R}^p$, the domain of h is denoted $dom(h)$ and consists of elements $x \in \mathbb{R}^n$ such that $h(x)$ is defined.

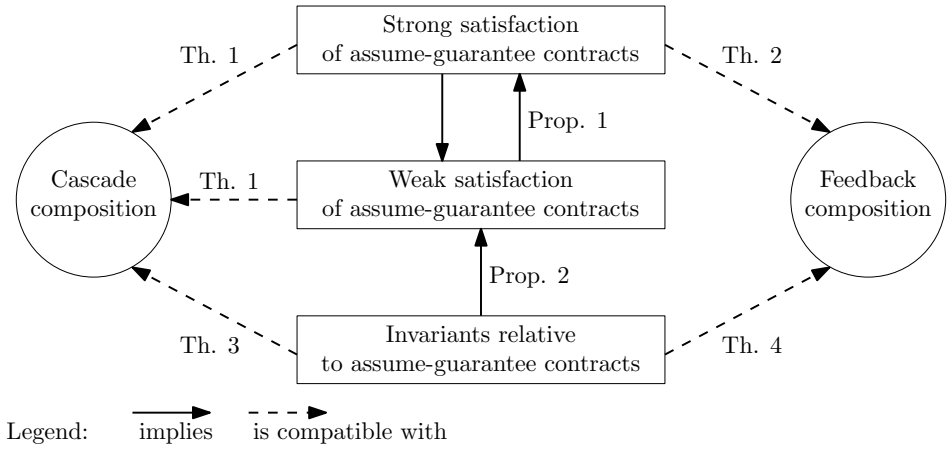

Fig. 2. Summary of main results in the paper

trajectories $x : I \to X$ in $\mathcal{T}_f$ are the solutions of the differential equation:

$$\begin{cases} \dot{x}_1(t) &= -a_1 x_1(t) + a_1 x_2(t), \\ \dot{x}_2(t) &= -a_2 x_2(t) + a_2 x_1(t), \end{cases}$$

where $x(t) = (x_1(t), x_2(t))$ and $x(0) \in [0, b_1] \times [0, b_2]$. By Theorem 4, it follows that for all $t \in I$, $x(t) \in [0, b]^2$.

V. Conclusion

In this paper, we proposed a contract based approach for verifying compositionally invariance properties of discrete-time and continuous-time interconnected systems. The main notions considered in the paper and their relationships are sketched in Figure 2. The main contributions are summarized below. We introduced a notion of assume-guarantee contracts equipped with a weak and a strong semantics. We showed that:

- both semantics are compatible with cascade composition (Theorem 1);
- strong semantics is required to reason on feedback composition (Theorem 2 and Example 2);
- strong satisfaction of a contract can sometimes be obtained from weak satisfaction (Proposition 1).

We then developed specific results for systems described by differential inclusions. We showed that:

- sufficient conditions for weak satisfaction of contracts can be given using invariant sets (Proposition 2);
- invariants are compatible with both cascade and feedback compositions (Theorems 3 and 4).

In future work, we will extend our framework to deal with other types of properties, beyond simple invariance properties considered in this paper.

References

[Aub09] J.-P. Aubin. *Viability theory*. Springer Science & Business Media, 2009.

[BCN+15] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. Henzinger, and K. Larsen. Contracts for systems design: Theory. Technical report, INRIA, 2015.

[Bla99] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[BM08] F. Blanchini and S. Miani. *Set-theoretic methods in control*. Birkhäuser Boston, 2008.

[CA15] S. Coogan and M. Arcak. A dissipativity approach to safety verification for interconnected systems. *IEEE Transactions on Automatic Control*, 60(6):1722–1727, 2015.

[CVZ+12] C. Conte, N.R. Voellmy, M.N. Zeilinger, M. Morari, and C.N. Jones. Distributed synthesis and control of constrained linear systems. In *American Control Conference*, pages 6017–6022, 2012.

[KAS17] E.S. Kim, M. Arcak, and S.A. Seshia. A small gain theorem for parametric assume-guarantee contracts. In *International Conference on Hybrid Systems: Computation and Control*, pages 207–216, 2017.

[KVDS09] Florian Kerber and Arjan Van Der Schaft. Assume-guarantee reasoning for linear dynamical systems. In *Control Conference (ECC), 2009 European*, pages 5015–5020. IEEE, 2009.

[LFM+16] A. Le Coënt, L. Fribourg, N. Markey, F. De Vuyst, and L. Chamoin. Distributed synthesis of state-dependent switching control. In *International Workshop on Reachability Problems*, pages 119–133, 2016.

[MGW15] P.-J. Meyer, A. Girard, and E. Witrant. Safety control with performance guarantees of cooperative systems using compositional abstractions. In *Conference on Analysis and Design of Hybrid Systems*, pages 317–322, 2015.

[NO16] P. Nilsson and N. Ozay. Synthesis of separable controlled invariant sets for modular local control design. In *American Control Conference*, pages 5656–5663, 2016.

[RKF10] S.V. Raković, B. Kern, and R. Findeisen. Practical set invariance for decentralized discrete time systems. In *IEEE Conference on Decision and Control*, pages 3283–3288, 2010.

[SPW12] C. Sloth, G.J. Pappas, and R. Wisniewski. Compositional safety analysis using barrier certificates. In *International Conference on Hybrid Systems: Computation and Control*, pages 15–24, 2012.

[VdS04] AJ Van der Schaft. Equivalence of dynamical systems by bisimulation. *IEEE transactions on automatic control*, 49(12):2160–2172, 2004.