Invariant Sets for Assume-Guarantee Contracts

Antoine Girard, Alessio Iovine, Sofiane Benberkane

Invariant Sets for Assume-Guarantee Contracts

Antoine Girard, *Senior Member, IEEE*, Alessio Iovine, *Member, IEEE*, Sofiane Benberkane

***Abstract*—Contract theory is a powerful tool to reason on systems that are interacting with an external environment, possibly made of other systems. Formally, a contract is usually given by assumptions and guarantees, which specify the expected behavior of the system (the guarantees) in a certain context (the assumptions). In this work, we present a verification framework for discrete-time dynamical systems with assume-guarantee contracts. We first introduce a class of assume-guarantee contracts with their satisfaction semantics parameterized by a time-horizon over which assumptions are evaluated. We then show that the problem of verifying whether such contracts are satisfied is equivalent to show the existence of a positive invariant set for an auxiliary system. This allows us to leverage the extensive literature on invariant set computation. A simple illustrative example is provided to show the effectiveness of our approach.**

***Index Terms*—Invariant sets, Assume-guarantee contracts, Verification.**

I. Introduction

Modern applications require engineering systems to be composed of several subsystems (agents) describing both physical behaviours and information technology components. Therefore, they are usually modeled as Cyber-Physical Systems (CPSs) [1], and this strongly complexify both system's design and performance. Indeed, there is an explosion of requirements and specifications, as the several agents need to be designed to operate in predictable ways with the deployed system.

Contract theory is a powerful tool that allows to formally define and verify the specifications that modern systems and CPSs have to satisfy [2], [3]. In fact, contracts provide a compositional approach based on modularity, granting the possibility to obtain a verification framework. Developed in computer science [4], in the last decades contracts have been considered for engineering applications. The main one has been the design of electronics components for correct-by-construction system-level composition [5]. In circuits, no dynamics was taken into account, and the definition of contracts aimed at guaranteeing circuit performance. However, recently several contributions appeared in the control community on assume-guarantee contracts, with the goal to better deal with large-scale systems via leveraging the assume-guarantee properties of contracts for dynamical systems to describe the interaction among the several agents, and with respect to the environment. In a control-oriented perspective, contracts are regarded as formal characterizations of control specifications [6], and their utilisation is expected to allow considering Plug&Play situations and a dynamic change of the system's structure and/or of its components.

In the recent literature, contracts for continuous-time [7] and discrete-time [8], [9] systems have been developed, targeting particularly linear systems [6], [8], [10] but also nonlinear ones [7], [9]. Several kind of specifications, as contract refinement for comparing contracts (see [8], [10]) or weak and strong satisfaction for dealing with agents' interconnection (see [7], [11]), are suggested. The contribution of the present paper relies in the discrete-time domain, and no linearity conditions are requested for the considered dynamics. Diversely from existing approaches, the satisfaction semantics is parameterized by a time-horizon over which assumptions are evaluated.

The great challenge in dealing with assume-guarantee contracts relies in obtaining numerical tools whose computational complexity does not explode with respect to the size of the system, and that adapt to small changes on the variables without re-running the whole calculation. Current approaches based on symbolic controllers and/or finite transition systems [11], [12] suffer of poor performance in case of high dimension systems. In the present paper, we focus on the utilisation of invariant sets (see [13], [14]) for verification of assume-guarantee contracts. Set invariance offers the possibility to use powerful algorithms (see [15], [16], [17], [18]) for providing feasible solutions in reasonable time. Therefore, we first describe a verification approach for discrete-time dynamical system based on assume-guarantee contracts, and then investigate the existence of invariant sets for verification. Three different types of satisfactions a system can verify for a given contracts are listed, together with the necessary and sufficient conditions for satisfaction. Differently from [9] and [19], we generalise the assume-guarantee reasoning via invariant sets without the restriction to consider Signal Temporal Logic to describe contracts, and we do not address a specific method for feasibility verification. Indeed, the suggested tests are general with respect to the computation methods for the required maximal invariant sets. Contrarily to [20], the specifications considered in the present paper can involve system dynamics.

The sequel of the paper is organised as follows. Section II describes the modeling of the systems and contracts we consider. Section III introduces the different satisfactions, while in Section IV an example is produced. Section V provides conclusive remarks. Some results are stated without proofs, which can be found in the appendix.

Notations: We denote with $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{N}$ the set of reals, non negative reals and natural numbers. We define the norm of $X \subseteq \mathbb{R}^n$ as $||X||_\infty = \sup_{x \in X} \|x\|$. Given a set Z, we denote

Antoine Girard, Alessio Iovine and Sofiane Benberkane are with the Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France. E-mail: name.surname@l2s.centralesupelec.fr

This project has received funding from the H2020-EU.1.1. research and innovation programme(s) – ERC-2016-COG under grant agreement No 725144, and from the Agence Nationale de la Recherche (ANR) under Grant HANDY ANR-18-CE40-0010.

the set of subsets of Z by 2^Z, which includes Z itself and the empty set $\emptyset$. Given a transition relation $F : Z \to 2^Z$, and $Z' \subseteq Z$, $F(Z') = \bigcup_{z \in Z'} F(z)$. For $z \in Z$, $F^0(z) = \{z\}$ and for $\delta \in \mathbb{N} \setminus \{0\}$, $F^\delta(z) = F(F^{\delta-1}(z))$. We define the *robust predecessors* of Z' by $\text{pre}_F(Z') = \{z \in Z |\ F(z) \subseteq Z'\}$. We denote by $\text{max-inv}_F(Z')$ the *maximal invariant subset* of Z' for F, i.e. the largest subset $Z'' \subseteq Z'$ such that $F(Z'') \subseteq Z''$.

II. Modeling and Formulation

In this section, we introduce a general class of discrete-time systems to be used in the paper. We then define a class of contracts and several associated semantics for contract satisfaction. Finally, we formulate the problem of contract verification under consideration in this paper.

A. Systems

In this paper, we will work with the following class of discrete-time systems:

Definition 1. A *system* is a tuple $\mathcal{S} = (Z, F, Z_0)$, where

- Z is a set of states;
- $F : Z \to 2^Z$ is a transition relation;
- $Z_0 \subseteq Z$ is a set of initial states.

A *trajectory* of $\mathcal{S}$ is a sequence $(z_t)_{t=0}^T$ where $T \in \mathbb{N} \cup \{\infty\}$ such that

$$z_0 \in Z_0 \text{ and } z_{t+1} \in F(z_t), \forall t \in \mathbb{N}_{<T}. \tag{1}$$

The trajectory is *maximal* if $T = \infty$ or if $F(x_T) = \emptyset$. It is *complete* if $T = \infty$. The set of maximal trajectories of $\mathcal{S}$ is denoted $\mathcal{T}_{\max}(\mathcal{S})$. $\mathcal{S}$ is *forward-complete* if all maximal trajectories are complete.

To show the generality of Definition 1, let us consider a typical discrete-time dynamical system with external input $w_t \in W$, state $x_t \in X$, and output $y_t \in Y$, written in the classical form:

$$\begin{cases} x_{t+1} &= f(x_t, w_t),\ x_0 \in X_0 \\ y_t &= g(x_t, w_t) \end{cases},\ t \in \mathbb{N}.$$

The system above can be written under the form of Definition 1 by considering the extended state $z_t = (w_t, x_t, y_t)$. Then, the dynamics of z_t is described by system $\mathcal{S} = (Z, F, Z_0)$ where $Z = W \times X \times Y$, the transition relation is given for all $z = (w, x, y) \in Z$ by

$$F(z) = \left\{ (w^+, x^+, y^+) \in Z \;\middle|\; \begin{array}{c} w^+ \in W,\ x^+ = f(x, w), \\ y^+ = g(x^+, w^+) \end{array} \right\}$$

and the set of initial states is

$$Z_0 = \left\{ (w_0, x_0, y_0) \in Z \;\middle|\; \begin{array}{c} w_0 \in W,\ x_0 \in X_0, \\ y_0 = g(x_0, w_0) \end{array} \right\}.$$

Of course, Definition 1 allows us to also consider other types of systems, such as systems with state constraints. Let us remark that in our formalism, we do not make an explicit distinction between input, state, and output variables. Also, we do not make any assumption on the set of states Z, which can be finite or infinite; discrete, continuous or hybrid.

In the following, we will make the standing assumption that the system $\mathcal{S}$ under consideration is forward-complete.

B. Assume-Guarantee Contracts

In this paper, we consider a class of assume-guarantee contracts defined as follows.

Definition 2. Let $\mathcal{S} = (Z, F, Z_0)$ be a system. An *assume-guarantee contract* (AG-contract) for $\mathcal{S}$ is a pair $\mathcal{C} = (F_A, F_G)$ where $F_A : Z \to 2^Z$ and $F_G : Z \to 2^Z$ are transition relations representing assumptions and guarantees respectively.

An AG-contract is a specification which states guarantees that should be fulfilled whenever the assumptions hold. We use the notation $\mathcal{S} \models \mathcal{C}$ to notify that a system $\mathcal{S}$ satisfies a contract $\mathcal{C}$. However, in this paper we will consider several semantics for contract satisfaction, which are formalized in the following definition:

Definition 3. Consider a system $\mathcal{S} = (Z, F, Z_0)$ and an AG-contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$. For $\delta \in \mathbb{N}$, we define the *δ-satisfaction* of $\mathcal{C}$ by $\mathcal{S}$ as follows:

- For $\delta \in \mathbb{N}$, $\mathcal{S} \models_\delta \mathcal{C}$ if for all $(z_t)_{t=0}^\infty \in \mathcal{T}_{\max}(\mathcal{S})$, it holds for all $t \in \mathbb{N}$:

$$\big(\forall s \in \mathbb{N} \cap \{t-\delta, \dots, t\},\ z_{s+1} \in F_A(z_s)\big) \implies z_{t+1} \in F_G(z_t).$$

- For $\delta = \infty$, $\mathcal{S} \models_\infty \mathcal{C}$ if for all $(z_t)_{t=0}^\infty \in \mathcal{T}_{\max}(\mathcal{S})$, it holds for all $t \in \mathbb{N}$:

$$\big(\forall s \in \mathbb{N}_{\le t},\ z_{s+1} \in F_A(z_s)\big) \implies z_{t+1} \in F_G(z_t).$$

Intuitively, δ-satisfaction states that if the assumptions are satisfied on the time window $\mathbb{N} \cap \{t-\delta, \dots, t\}$, then the guarantee needs to be fulfilled at time t. The parameter δ can be thought about as a time-horizon defining the size of the sliding window on which the contract assumptions are evaluated.

It is worthwhile to point out the following major difference between δ-satisfaction (for $\delta \in \mathbb{N}$) and ∞-satisfaction (for $\delta = \infty$). In ∞-satisfaction, if the assumption happens to be violated at some time instant (i.e. if there exists $t \in \mathbb{N}$ such that $z_{t+1} \notin F_A(z_t)$), then there is no obligation of ensuring the guarantee anytime after that instant. In contrast, with the δ-satisfaction, if the assumption becomes true again over a period of $\delta + 1$ time steps, then the guarantees needs to be fulfilled again. Hence, δ-satisfaction, for $\delta \in \mathbb{N}$, makes it possible to specify behaviors that are more resilient to assumption violations than ∞-satisfaction. Actually the following result shows that Definition 3 defines a hierarchy of contract satisfaction semantics parameterized by δ: 0-satisfaction being the strongest semantics (corresponding to the weakest assumption) and ∞-satisfaction being the weakest semantics (corresponding to the strongest assumption).

Proposition 1. *The following properties hold:*

- *For all $\delta_1, \delta_2 \in \mathbb{N}$ with $\delta_1 \le \delta_2$, if $\mathcal{S} \models_{\delta_1} \mathcal{C}$ then $\mathcal{S} \models_{\delta_2} \mathcal{C}$.*
- *For all $\delta \in \mathbb{N}$, if $\mathcal{S} \models_\delta \mathcal{C}$ then $\mathcal{S} \models_\infty \mathcal{C}$.*

Remark 1. In this paper, we will pay a specific attention to the particular case $\delta = 0$. Note that for $\delta = 0$, Definition 3

boils down to $\mathcal{S} \models_0 \mathcal{C}$ if for all $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$, it holds for all time $t \in \mathbb{N}$:

$$z_{t+1} \in F_A(z_t) \implies z_{t+1} \in F_G(z_t).$$

Remark 2. For $\delta = +\infty$, our framework can be seen as a generalization of invariance AG-contracts introduced in [20], by considering, for a subset $Z_A \subseteq Z$, F_A of the form:

$$F_A(z) = \begin{cases} Z & \text{if } z \in Z_A \\ \emptyset & \text{if } z \notin Z_A \end{cases}$$

and for a subset $Z_G \subseteq Z$, F_G of the form:

$$F_G(z) = Z_G, \text{ or } F_G(z) = \begin{cases} Z & \text{if } z \in Z_G \\ \emptyset & \text{if } z \notin Z_G \end{cases}$$

for strong and weak satisfaction semantics (as defined in [20]), respectively.

We now formulate the problem of contract verification that we consider in this paper:

Problem 1. Given a system $\mathcal{S} = (Z, F, Z_0)$, an AG-contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$, and $\delta \in \mathbb{N} \cup \{\infty\}$, verify if $\mathcal{S} \models_\delta \mathcal{C}$.

We end this section with a technical result that will be instrumental for further developments:

Proposition 2. *Consider a set Z, transition relation F and an AG-contract $\mathcal{C} = (F_A, F_G)$. For $\delta \in \mathbb{N} \cup \{\infty\}$, there exists a (possibly empty) maximal set of initial states $Z_0^* \subseteq Z$ such that:*

- *$\mathcal{S}^* \models_\delta \mathcal{C}$ where $\mathcal{S}^* = (Z, F, Z_0^*)$, and*
- *for all system $\mathcal{S} = (Z, F, Z_0)$ such that $\mathcal{S} \models_\delta \mathcal{C}$ it holds $Z_0 \subseteq Z_0^*$.*

C. Illustrative Example

In this section, we present a simple example to illustrate the main features of our framework. We consider a car-following situation between two vehicles, we model the distance between the follower vehicle and its leader as the state variable $x_t \in X \subseteq \mathbb{R}$, and consider the external input $w_t \in W \subseteq \mathbb{R}$ describing the desired reference deriving from the closed loop. Therefore, according to Definition 1 we define the extended state $z_t = (w_t, x_t)$ and the corresponding system $\mathcal{S} = (Z, F, Z_0)$, where $Z = W \times X$, $Z_0 \subseteq Z$ and the transition relation is

$$F : x_{t+1} = x_t + \lambda(w_t - x_t), \tag{2}$$

with $\lambda \in (0, 1)$. We assume that $W \subseteq X$ and that X is convex, so that the system $\mathcal{S}$ is forward-complete. For the described system, we suggest the following AG-contracts of interest.

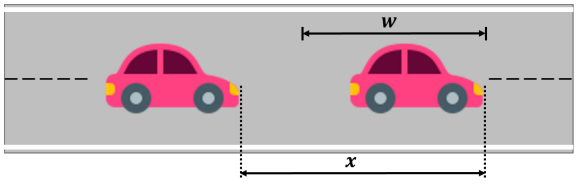

Fig. 1. The reference framework of the considered car-following situation in the example.

Contract 1. An AG-contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$ is defined as composed by:

- the assumption of bounded variation of the distance reference over time, i.e.

$$F_A : |w_{t+1} - w_t| \leq D_0, \tag{3}$$

  where $D_0 \in \mathbb{R}^+$;
- the guarantee to have a bounded variation of the distance over time while having a bounded difference between the distance and the reference, i.e.

$$F_G : |x_{t+1} - x_t| \leq D_1 \wedge |x_{t+1} - w_{t+1}| \leq D_2, \tag{4}$$

  where $D_1 \in \mathbb{R}^+$, $D_2 \in \mathbb{R}^+$.

III. Characterisation using Invariant Sets

In this section, we provide theoretical results for verifying contracts based on the notion of invariant sets. We first consider the simpler cases $\delta = 0$ and $\delta = +\infty$. Then, we present an approach for the case $\delta \in \mathbb{N}$, with $\delta \neq 0$.

A. 0-satisfaction and ∞-satisfaction

To characterize the initial states for which the contract is satisfied, let us define the set $Z_{\mathcal{C}}^0$ given by

$$Z_{\mathcal{C}}^0 = \{z \in Z |\ F_{S \cap A}(z) \subseteq F_G(z)\}, \tag{5}$$

where the transition relation $F_{S\cap A} : Z \to 2^Z$ is defined by

$$\forall z \in Z,\ F_{S\cap A}(z) = F(z) \cap F_A(z).$$

We first deal with 0-satisfaction:

Theorem 1. *Consider a system $\mathcal{S} = (Z, F, Z_0)$ and a contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$. Then, $\mathcal{S} \models_0 \mathcal{C}$ if and only if there exists $Z_{\mathcal{C}} \subseteq Z$ such that the following hold*

$$Z_0 \subseteq Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0, \tag{6}$$

$$F(Z_{\mathcal{C}}) \subseteq Z_{\mathcal{C}}. \tag{7}$$

Proof. We start by proving the "if" part. Consider $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$. Since $z_0 \in Z_0 \subseteq Z_{\mathcal{C}}$ by (6), we obtain by (1) and (7), that $z_t \in Z_{\mathcal{C}}$ for all $t \in \mathbb{N}$. Then, let us assume that for some $t \in \mathbb{N}$, $z_{t+1} \in F_A(z_t)$, then from (1) it holds $z_{t+1} \in F(z_t) \cap F_A(z_t) = F_{S\cap A}(z_t)$. Since $z_t \in Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0$ by (6), we get from (5) that $z_{t+1} \in F_G(z_t)$. Therefore, $\mathcal{S} \models_0 \mathcal{C}$.

We now prove the "only if" part. For that purpose, let us assume that $\mathcal{S} \models_0 \mathcal{C}$. From Proposition 2, we know that there exists $Z_0^* \subseteq Z$, a maximal set of initial states such that $\mathcal{S}^* \models_0 \mathcal{C}$ where $\mathcal{S}^* = (Z, F, Z_0^*)$. Let us prove that the conditions of Theorem 1 hold for $Z_{\mathcal{C}} = Z_0^*$.

By maximality we get $Z_0 \subseteq Z_0^*$. Then, let us consider $z_0 \in Z_0^*$. If $F_{S\cap A}(z_0) = \emptyset$, then from (5), $z_0 \in Z_{\mathcal{C}}^0$. If $F_{S\cap A}(z_0) \neq \emptyset$, let $z_1 \in F_{S\cap A}(z_0)$. Then, since $\mathcal{S}^* \models_0 \mathcal{C}$, we get that $z_1 \in F_G(z_0)$. Therefore, $F_{S\cap A}(z_0) \subseteq F_G(z_0)$ and from (5), $z_0 \in Z_{\mathcal{C}}^0$. Hence, $Z_0^* \subseteq Z_{\mathcal{C}}^0$ and (6) holds for $Z_{\mathcal{C}} = Z_0^*$.

Let $\mathcal{S}' = (Z, F, Z_0')$ where $Z_0' = F(Z_0^*)$ and let us show that we have $\mathcal{S}' \models_0 \mathcal{C}$. Let $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S}')$, since $z_0 \in Z_0' = F(Z_0^*)$ there exists $z_{-1} \in Z_0^*$ such that $z_0 \in F(z_{-1})$.

Then $(z_{t-1})_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S}^*)$. Let $t \in \mathbb{N}$, and let us assume that $z_{t+1} \in F_A(z_t)$. Since $\mathcal{S}^* \models_0 \mathcal{C}$, we get $z_{t+1} \in F_G(z_t)$. Hence, $\mathcal{S}' \models_0 \mathcal{C}$. By maximality, this implies that $Z_0' \subseteq Z_0^*$. Hence, $F(Z_0^*) \subseteq Z_0^*$ and (7) holds for $Z_{\mathcal{C}} = Z_0^*$. □

A similar result can be established for ∞-satisfaction:

Theorem 2. *Consider a system $\mathcal{S} = (Z, F, Z_0)$ and a contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$. Then, $\mathcal{S} \models_\infty \mathcal{C}$ if and only if there exists $Z_{\mathcal{C}} \subseteq Z$ such that the following hold*

$$Z_0 \subseteq Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0, \tag{8}$$

$$F_{S\cap A}(Z_{\mathcal{C}}) \subseteq Z_{\mathcal{C}}. \tag{9}$$

Proof. We start by proving the "if" part. Consider $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$ and let $t \in \mathbb{N}$ such that for all $s \in \mathbb{N}_{\leq t}$, $z_{s+1} \in F_A(z_s)$. Then, from (1) it holds for all $s \in \mathbb{N}_{\leq t}$, $z_{s+1} \in F(z_s) \cap F_A(z_s) = F_{S\cap A}(z_s)$. Since $z_0 \in Z_0 \subseteq Z_{\mathcal{C}}$ by (8), we obtain by (9), that $z_t \in Z_{\mathcal{C}}$. Moreover, we already showed that $z_{t+1} \in F_{S\cap A}(z_t)$. Since $z_t \in Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0$ by (8), we get from (5) that $z_{t+1} \in F_G(z_t)$. Therefore, $\mathcal{S} \models_\infty \mathcal{C}$.

We now prove the "only if" part. For that purpose, let us assume that $\mathcal{S} \models_\infty \mathcal{C}$. From Proposition 2, we know that there exists $Z_0^* \subseteq Z$, a maximal set of initial states such that $\mathcal{S}^* \models_\infty \mathcal{C}$ where $\mathcal{S}^* = (Z, F, Z_0^*)$. Let us prove that the conditions of Theorem 2 hold for $Z_{\mathcal{C}} = Z_0^*$. The proof that (8) holds is identical to the proof that (6) holds in Theorem 1.

Let $\mathcal{S}' = (Z, F, Z_0')$ where $Z_0' = F_{S\cap A}(Z_0^*)$ and let us show that we have $\mathcal{S}' \models_0 \mathcal{C}$. Let $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S}')$, since $z_0 \in Z_0' = F_{S\cap A}(Z_0^*)$ there exists $z_{-1} \in Z_0^*$ such that $z_0 \in F_{S\cap A}(z_{-1})$. Then, since $F_{S\cap A}(z_{-1}) \subseteq F(z_{-1})$, we get that $(z_{t-1})_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S}^*)$. Let $t \in \mathbb{N}$, and let us assume that for all $s \in \mathbb{N}_{\leq t}$, $z_{s+1} \in F_A(z_s)$. Since $F_{S\cap A}(z_{-1}) \subseteq F_A(z_{-1})$, we get, for all $s \in \mathbb{N}_{\leq t+1}$, $z_s \in F_A(z_{s-1})$. Since $\mathcal{S}^* \models_\infty \mathcal{C}$, we get $z_{t+1} \in F_G(z_t)$. Hence, $\mathcal{S}' \models_\infty \mathcal{C}$. By maximality, this implies that $Z_0' \subseteq Z_0^*$. Hence, $F_{S\cap A}(Z_0^*) \subseteq Z_0^*$ and (9) holds for $Z_{\mathcal{C}} = Z_0^*$. □

Hence we can see that for $\delta = 0$ and $\delta = \infty$, Problem 1 can be solved by computing subsets of $Z_{\mathcal{C}}^0$ that are invariant for the maps F and $F_{S\cap A}$, respectively. If the initial set Z_0 is included in the computed invariant subset then we can certify that the contract is satisfied. Moreover, this inclusion test is necessary and sufficient if one is able to compute the maximal invariant subsets of $Z_{\mathcal{C}}^0$, max-inv$_F$ $\left(Z_{\mathcal{C}}^0\right)$ and max-inv$_{F_{S\cap A}}$ $\left(Z_{\mathcal{C}}^0\right)$, respectively.

The computation of (maximal) invariant sets for dynamical systems is a problem that has been extensively considered in the literature [13]. For example, the existence of positively invariant sets for ensuring stability of linear delay-difference equations is investigated in [21]. In [22], a methodology for constructing inner approximations of the maximal positively invariant set for a polynomial dynamical system with semi-algebraic constraints is suggested. An interval approach to compute invariant sets is suggested in [23], to estimate the largest invariant of a subset of the state space of a nonlinear continuous-time dynamical system. Rather than classical control approaches, also modern data-driven ones consider invariant sets, e.g. as described in [24], where a data-driven method for computing an approximation of a robust control invariant set from experimental data is proposed, or in [25], where the problem of invariant set computation for black-box switched linear systems using merely a finite set of observations of system trajectories is investigated. Due to the necessity to deal with large-scale systems, scalable approaches for computing invariant sets are targeted too [26].

B. δ-satisfaction

We now consider the case $\delta \in \mathbb{N}$, with $\delta \neq 0$. In this case, the δ-satisfaction of a contract can be verified by computing two invariant sets, one for the map F and another one for the map $F_{S\cap A}$ as shown in the following result:

Theorem 3. *Consider a system $\mathcal{S} = (Z, F, Z_0)$, a contract $\mathcal{C} = (F_A, F_G)$ for $\mathcal{S}$ and $\delta \in \mathbb{N} \setminus \{0\}$. Then, $\mathcal{S} \models_\delta \mathcal{C}$ if and only if there exist $Z_{\mathcal{C}} \subseteq Z$ and $Z_{\mathcal{C}}' \subseteq Z$ such that the following hold*

$$Z_0 \subseteq Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0, \tag{10}$$

$$F_{S\cap A}(Z_{\mathcal{C}}) \subseteq Z_{\mathcal{C}}, \tag{11}$$

$$Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}', \tag{12}$$

$$F(Z_{\mathcal{C}}') \subseteq Z_{\mathcal{C}}', \tag{13}$$

$$F_{S\cap A}^{\delta}(Z_{\mathcal{C}}') \subseteq Z_{\mathcal{C}}. \tag{14}$$

Proof. We start by proving the "if" part. Consider $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$ and let $t \in \mathbb{N}$ such that for all $s \in \mathbb{N} \cap \{t-\delta, \ldots, t\}$, $z_{s+1} \in F_A(z_s)$. Let us first show that $z_t \in Z_{\mathcal{C}}$. We consider two different cases.

- $t \leq \delta$: Then, from (1) it holds for all $s \in \mathbb{N}_{\leq t}$, $z_{s+1} \in F(z_s) \cap F_A(z_s) = F_{S\cap A}(z_s)$. Since $z_0 \in Z_0 \subseteq Z_{\mathcal{C}}$ by (10), we obtain by (11), that $z_t \in Z_{\mathcal{C}}$.
- $t > \delta$: Since $z_0 \in Z_0 \subseteq Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}'$ by (10) and (12), we obtain by (1) and (13), that $z_{t-\delta} \in Z_{\mathcal{C}}'$. From (1), we get for all $s \in \mathbb{N} \cap \{t-\delta, \ldots, t\}$, $z_{s+1} \in F(z_s) \cap F_A(z_s) = F_{S\cap A}(z_s)$. Therefore, we get from (14) that $z_t \in Z_{\mathcal{C}}$.

In both cases, we already showed that $z_{t+1} \in F_{S\cap A}(z_t)$. Since $z_t \in Z_{\mathcal{C}} \subseteq Z_{\mathcal{C}}^0$ by (10), we get from (5) that $z_{t+1} \in F_G(z_t)$. Therefore, $\mathcal{S} \models_\delta \mathcal{C}$.

We now prove the "only if" part. For that purpose, let us assume that $\mathcal{S} \models_\delta \mathcal{C}$. From Proposition 2, we know that there exists $Z_0^* \subseteq Z$, a maximal set of initial states such that $\mathcal{S}^* \models_\delta \mathcal{C}$ where $\mathcal{S}^* = (Z, F, Z_0^*)$. Let us prove that the conditions of Theorem 2 hold for $Z_{\mathcal{C}} = Z_0^*$ and $Z_{\mathcal{C}}' = \text{reach}(\mathcal{S}^*)$, where

$$\text{reach}(\mathcal{S}^*) = \left\{ z \in Z \,\middle|\, \exists \tau \in \mathbb{N}, (z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S}^*), z = z_\tau \right\}. \tag{15}$$

The proof that (10) holds is identical to the proof that (6) holds in Theorem 1. Similarly, (11) can be proved along the same lines as (9) in Theorem 2.

Then, it is clear from (15) that $Z_0^* \subseteq \text{reach}(\mathcal{S}^*)$. Therefore, (12) holds for $Z_{\mathcal{C}} = Z_0^*$ and $Z_{\mathcal{C}}' = \text{reach}(\mathcal{S}^*)$. It is also easy to prove from (15), that $F(\text{reach}(\mathcal{S}^*)) \subseteq \text{reach}(\mathcal{S}^*)$. Hence, (13) holds for $Z_{\mathcal{C}}' = \text{reach}(\mathcal{S}^*)$.

It remains to show that (14) holds. For that purpose, let $\mathcal{S}' = (Z, F, Z_0')$ where $Z_0' = F_{S\cap A}^{\delta}(\text{reach}(\mathcal{S}^*))$ and let us

show that we have $\mathcal{S}' \models_\delta \mathcal{C}$. Let $(z_t)_{t=0}^\infty \in \mathcal{T}_{\max}(\mathcal{S}')$, since $z_0 \in Z_0' = F^\delta_{S\cap A}(\text{reach}(\mathcal{S}^*))$, there exist $(z'_t)_{t=0}^\infty \in \mathcal{T}_{\max}(\mathcal{S}^*)$ and $\tau \geq \delta$, such that $z'_\tau = z_0$ and for all $s \in \{\tau-\delta, \dots, \tau-1\}$, $z'_{s+1} \in F_A(z'_s)$. Let $t \in \mathbb{N}$, and let us assume that for all $s \in \mathbb{N} \cap \{t-\delta, \dots, t\}$, $z_{s+1} \in F_A(z_s)$. Then, for $s \in \mathbb{N}$, let

$$z^*_s = \begin{cases} z'_s & \text{if } 0 \leq s < \tau, \\ z_{s-\tau} & \text{if } \tau \leq s. \end{cases}$$

Then, since $z'_\tau = z_0$, we get that $(z^*_s)_{s=0}^\infty \in \mathcal{T}_{\max}(\mathcal{S}^*)$. Moreover, for all $s \in \mathbb{N}\cap\{t+\tau-\delta, \dots, t+\tau\}$, $z^*_{s+1} \in F_A(z^*_s)$. Since $\mathcal{S}^* \models_\delta \mathcal{C}$, we get that $z^*_{t+\tau+1} \in F_G(z^*_{t+\tau})$. This gives us $z_{t+1} \in F_G(z_t)$. Hence, $\mathcal{S}' \models_\delta \mathcal{C}$. Then, by maximality, this gives $Z_0' \subseteq Z_0^*$. Therefore (14) holds for $Z_\mathcal{C} = Z_0^*$ and $Z'_\mathcal{C} = \text{reach}(\mathcal{S}^*)$. □

Remark 3. It is interesting to note that conditions (10) and (11) in Theorem 3 are the same as conditions (8) and (9) in Theorem 2. This shows that for any $\delta \in \mathbb{N} \setminus \{0\}$, $\mathcal{S} \models_\delta \mathcal{C}$ implies $\mathcal{S} \models_\infty \mathcal{C}$, which is consistent with Proposition 1. Also, if conditions (6) and (7) in Theorem 1 are satisfied for some $Z_\mathcal{C} \subseteq Z$ then it can be shown that the conditions in Theorem 3 are satisfied with $Z_\mathcal{C} = Z'_\mathcal{C}$. This shows that for any $\delta \in \mathbb{N} \setminus \{0\}$, $\mathcal{S} \models_0 \mathcal{C}$ implies $\mathcal{S} \models_\delta \mathcal{C}$, which is also consistent with Proposition 1.

We end the section by presenting an approach to compute the sets $Z_\mathcal{C}$ and $Z'_\mathcal{C}$ satisfying the conditions of Theorem 3. Consider the sequences of sets $\{Z^k_\mathcal{C}\}_{k=0}^\infty$ and $\{Z'^k_\mathcal{C}\}_{k=0}^\infty$ where $Z^0_\mathcal{C}$ is given by (5) and for $k \in N$:

$$Z'^k_\mathcal{C} = \text{max-inv}_F\left(\text{pre}_{F^\delta_{S\cap A}}(Z^k_\mathcal{C})\right), \tag{16}$$

$$Z^{k+1}_\mathcal{C} = \text{max-inv}_{F_{S\cap A}}\left(Z^k_\mathcal{C} \cap Z'^k_\mathcal{C}\right). \tag{17}$$

Proposition 3. *Let $Z_0^* \subseteq Z$, the maximal set of initial states such that $\mathcal{S}^* \models_\delta \mathcal{C}$ where $\mathcal{S}^* = (Z, F, Z_0^*)$. The following proposition holds:*

- *For all $k \in \mathbb{N}$, $Z_0^* \subseteq Z^k_\mathcal{C}$,*
- *If for some $k \in \mathbb{N}$, $Z^{k+1}_\mathcal{C} = Z^k_\mathcal{C}$, then $Z_0^* = Z^k_\mathcal{C}$.*

From (17), it is clear that $Z^{k+1}_\mathcal{C} \subseteq Z^k_\mathcal{C}$ so we know that the sequence of sets $\{Z^k_\mathcal{C}\}_{k=0}^\infty$ converges to a fixed point. However, in general, there is no guarantee that this fixed point can be reached in a finite number of steps. Hence Proposition 3 provides a semi-algorithm to verify the δ-satisfaction of a contract. Numerical aspects of this approach will be explored in future research.

IV. Example

In this section, we illustrate how to verify the ∞-satisfaction and δ-satisfaction for Contract 1 in the example of Section II-C.

A. Example for the ∞-satisfaction

To prove $\mathcal{S} \models_\infty \mathcal{C}$, the main goal is to compute a set of states $Z_\mathcal{C}$ satisfying the conditions of Theorem 2. We shall search for such a set under the form

$$Z_\mathcal{C} = \{(x, w) \in Z \mid |x - w| \leq D\}, \tag{18}$$

where D is a constant to be determined.

Let us first compute a subset of $Z^0_\mathcal{C}$, the set of pairs (w_t, x_t) such that if (2), (3) hold then (4) holds. Let us remark that from (2),

$$|x_{t+1} - x_t| = |x_t + \lambda(w_t - x_t) - x_t| = \lambda|w_t - x_t|. \tag{19}$$

Then, for $|x_{t+1} - x_t| \leq D_1$ to hold in (4), it is sufficient that

$$|w_t - x_t| \leq \frac{D_1}{\lambda}. \tag{20}$$

Then, let us remark that from (2) and (3) we have

$$\begin{aligned} |x_{t+1} - w_{t+1}| &\leq |x_{t+1} - w_{t+1} - w_t + w_t| \\ &\leq |x_{t+1} - w_t| + |w_t - w_{t+1}| \\ &\leq |x_t + \lambda(w_t - x_t) - w_t| + D_0 \\ &\leq (1-\lambda)|x_t - w_t| + D_0. \end{aligned} \tag{21}$$

Therefore, for $|x_{t+1} - w_{t+1}| \leq D_2$ to hold in (4), it is sufficient that

$$|x_t - w_t| \leq \frac{D_2 - D_0}{1-\lambda}. \tag{22}$$

As a consequence, a subset of $Z^0_\mathcal{C}$ is computed as

$$\left\{(x, w) \in Z \;\middle|\; |x - w| \leq \frac{D_1}{\lambda} \wedge |x - w| \leq \frac{D_2 - D_0}{1-\lambda}\right\} \subseteq Z^0_\mathcal{C}. \tag{23}$$

Then, for $Z_\mathcal{C} \subseteq Z^0_\mathcal{C}$ to hold in (8), it is sufficient to consider a value for D such that

$$D \leq \min\left\{\frac{D_1}{\lambda}, \frac{D_2 - D_0}{1-\lambda}\right\}. \tag{24}$$

Furthermore, for verifying (9), let us assume (2), (3) and

$$|x_t - w_t| \leq D. \tag{25}$$

Then, from (2) and (3), we obtain again (21), which gives with (25)

$$|x_{t+1} - w_{t+1}| \leq (1-\lambda)D + D_0. \tag{26}$$

To satisfy (9), we need to have

$$|x_{t+1} - w_{t+1}| \leq D. \tag{27}$$

It is therefore sufficient that

$$D \geq \frac{D_0}{\lambda}. \tag{28}$$

Then, for any value D satisfying (24) and (28), the set $Z_\mathcal{C}$ satisfies the conditions of Theorem 2. We remark that to find such a value D, it is required that $D_0 \leq D_1$ and $D_0 \leq \lambda D_2$. In such a case, we get $\mathcal{S} \models_\infty \mathcal{C}$, for any set of initial states $Z_0 \subseteq Z_\mathcal{C}$.

B. Example for the δ-satisfaction

To prove $\mathcal{S} \models_\delta \mathcal{C}$, we first need the additional hypotheses that the sets X and W are bounded, i.e. $||X||_\infty \leq B$ and $||W||_\infty \leq B$, with $B \in \mathbb{R}^+$.

We want to prove that the conditions of Theorem 3 are satisfied by the sets $Z_\mathcal{C}$ given by (18) and $Z'_\mathcal{C}$ given by

$$Z'_\mathcal{C} = W \times X = Z. \tag{29}$$

It follows from the previous section that (10) and (11) are satisfied if (24) and (28) hold. Moreover, (12) and (13) are clearly satisfied since $Z'_\mathcal{C} = Z$. It thus remains to find conditions that ensure (14). Let us consider $(w_0, x_0) \in Z'_\mathcal{C}$ and assume (2), (3) hold for $t = 0, \ldots, \delta - 1$. Then

$$|x_{t+1} - w_{t+1}| \leq (1-\lambda)|x_t - w_t| + D_0, \tag{30}$$

which by induction gives

$$\begin{aligned} |x_\delta - w_\delta| \leq & (1-\lambda)^\delta |x_0 - w_0| \\ & + \underbrace{\left((1-\lambda)^{\delta-1} + \ldots + (1-\lambda) + 1\right)}_{\text{geometric series}} D_0 \\ \leq & (1-\lambda)^\delta |x_0 - w_0| + \frac{1}{\lambda} D_0 \\ \leq & (1-\lambda)^\delta 2B + \frac{1}{\lambda} D_0. \end{aligned} \tag{31}$$

For (14) to hold, we need to have $|x_\delta - w_\delta| \leq D$ and therefore it is sufficient that

$$D \geq (1-\lambda)^\delta 2B + \frac{1}{\lambda} D_0. \tag{32}$$

Then, for any value D satisfying (24) and (32), the sets $Z_\mathcal{C}$ and $Z'_\mathcal{C}$ satisfy the conditions of Theorem 3. In such a case, we get $\mathcal{S} \models_\delta \mathcal{C}$, for any set of initial states $Z_0 \subseteq Z_\mathcal{C}$.

V. Conclusions

The present paper suggests the certification of the existence of positive invariance sets as verification framework for the satisfaction of assume-guarantee contracts for discrete-time dynamical systems. A hierarchy of contract satisfaction semantics, that is parameterized by a time-horizon over which assumptions are evaluated, is defined and proved. Finally, the theoretical results are applied to a simple example.

Future research shall focus on numerical aspects of the approach, in particular for δ-satisfaction. Applications of our framework to challenging problems from power systems or multi-agent robotics will also be considered. Finally, we plan to extend our verification framework to develop techniques for synthesizing controllers from contracts.

References

[1] P. Derler, E. A. Lee, and A. Sangiovanni Vincentelli, "Modeling cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[2] 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 system design," *Foundations and Trends in Electronic Design Automation*, vol. 12, no. 2-3, pp. 124–400, 2018.

[3] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, "Taming Dr. Frankenstein: Contract-based design for cyber-physical systems," *European Journal of Control*, vol. 18, no. 3, pp. 217–238, 2012.

[4] B. Meyer, "Applying 'design by contract'," *Computer*, vol. 25, no. 10, pp. 40–51, 1992.

[5] A. Sangiovanni-Vincentelli, "Quo vadis, SLD? Reasoning about the trends and challenges of system level design," *Proceedings of the IEEE*, vol. 95, no. 3, pp. 467–506, 2007.

[6] B. Besselink, K. H. Johansson, and A. Van Der Schaft, "Contracts as specifications for dynamical systems in driving variable form," in *European Control Conference*, pp. 263–268, 2019.

[7] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, p. 109910, 2021.

[8] M. Sharf, B. Besselink, A. Molin, Q. Zhao, and K. H. Johansson, "Assume/guarantee contracts for dynamical systems: Theory and computational tools," *IFAC-PapersOnLine*, vol. 54, no. 5, pp. 25–30, 2021.

[9] Y. Chen, J. Anderson, K. Kalsi, S. H. Low, and A. D. Ames, "Compositional set invariance in network systems with assume-guarantee contracts," in *American Control Conference*, pp. 1027–1034, 2019.

[10] B. Shali, A. van der Schaft, and B. Besselink, "Behavioural contracts for linear dynamical systems: input assumptions and output guarantees," in *European Control Conference*, pp. 567–572, 2021.

[11] A. Saoud, A. Girard, and L. Fribourg, "Contract-based design of symbolic controllers for safety in distributed multiperiodic sampled-data systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 3, pp. 1055–1070, 2020.

[12] P.-J. Meyer, A. Girard, and E. Witrant, "Compositional abstraction and safety synthesis using overlapping symbolic models," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1835–1841, 2018.

[13] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[14] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*. Systems & Control: Foundations & Applications, Birkhäuser Boston, 2007.

[15] M. Fiacchini, T. Alamo, and E. Camacho, "On the computation of convex robust control invariant sets for nonlinear systems," *Automatica*, vol. 46, no. 8, pp. 1334–1338, 2010.

[16] D. Mayne, J. Rawlings, C. Rao, and P. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[17] Y. Li and J. Liu, "Invariance control synthesis for switched nonlinear systems: An interval analysis approach," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2206–2211, 2018.

[18] Z. Wang, R. M. Jungers, and C. J. Ong, "Computation of the maximal invariant set of discrete-time linear systems subject to a class of non-convex constraints," *Automatica*, vol. 125, p. 109463, 2021.

[19] Y. Chen, J. Anderson, K. Kalsi, A. D. Ames, and S. H. Low, "Safety-critical control synthesis for network systems with control barrier functions and assume-guarantee contracts," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 487–499, 2021.

[20] A. Saoud, A. Girard, and L. Fribourg, "On the composition of discrete and continuous-time assume-guarantee contracts for invariance," in *European Control Conference*, pp. 435–440, 2018.

[21] M.-T. Laraba, S. Olaru, S.-I. Niculescu, F. Blanchini, G. Giordano, D. Casagrande, and S. Miani, "Guide on set invariance for delay difference equations," *Annual Reviews in Control*, vol. 41, pp. 13–23, 2016.

[22] A. Oustry, M. Tacchi, and D. Henrion, "Inner approximations of the maximal positively invariant set for polynomial dynamical systems," *IEEE Control Systems Letters*, vol. 3, no. 3, pp. 733–738, 2019.

[23] T. Le Mézo, L. Jaulin, and B. Zerr, "An interval approach to compute invariant sets," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 4236–4242, 2017.

[24] Y. Chen and N. Ozay, "Data-driven computation of robust control invariant sets with concurrent model selection," *IEEE Transactions on Control Systems Technology*, vol. 30, no. 2, pp. 495–506, 2022.

[25] Z. Wang and R. M. Jungers, "A data-driven method for computing polyhedral invariant sets of black-box switched linear systems," *IEEE Control Systems Letters*, vol. 5, no. 5, pp. 1843–1848, 2021.

[26] T. Anevlavis, Z. Liu, N. Ozay, and P. Tabuada, "An enhanced hierarchy for (robust) controlled invariance," in *American Control Conference*, pp. 4860–4865, 2021.

APPENDIX

Proof of Proposition 1: If $\delta_1 \leq \delta_2$, then we get for all $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$ and for all $t \in \mathbb{N}$:

$$\begin{aligned}&\big(\forall s \in \mathbb{N} \cap \{t-\delta_2, \dots, t\},\ z_{s+1} \in F_A(z_s)\big)\\ &\quad\implies \big(\forall s \in \mathbb{N} \cap \{t-\delta_1, \dots, t\},\ z_{s+1} \in F_A(z_s)\big).\end{aligned}$$

It follows from above and from Definition 3 that $\mathcal{S} \models_{\delta_1} \mathcal{C}$ implies $\mathcal{S} \models_{\delta_2} \mathcal{C}$. Similarly, for any $\delta \in N$, we have for all $(z_t)_{t=0}^{\infty} \in \mathcal{T}_{\max}(\mathcal{S})$ and for all $t \in \mathbb{N}$:

$$\begin{aligned}&\big(\forall s \in \mathbb{N}_{\leq t},\ z_{s+1} \in F_A(z_s)\big)\\ &\quad\implies \big(\forall s \in \mathbb{N} \cap \{t-\delta, \dots, t\},\ z_{s+1} \in F_A(z_s)\big).\end{aligned}$$

It follows from above and from Definition 3 that $\mathcal{S} \models_{\delta} \mathcal{C}$ implies $\mathcal{S} \models_{\infty} \mathcal{C}$. □

Proof of Proposition 2: Consider $\Omega_0 \subseteq 2^Z$ the set consisting of all sets of initial states $Z_0 \subseteq Z$ such that $\mathcal{S} \models_{\delta} \mathcal{C}$ where $\mathcal{S} = (Z, F, Z_0)$. Then, let $Z_0^* = \bigcup_{Z_0 \in \Omega_0} Z_0$. Clearly, for all $Z_0 \in \Omega_0$, $Z_0 \subseteq Z_0^*$, which proves the second item of the proposition. Moreover, it is easy to check that $Z_0^* \in \Omega_0$, which proves the first item of the proposition. □

Proof of Proposition 3: From the proof of Theorem 3, we know that the conditions (10)-(14) hold for $Z_{\mathcal{C}} = Z_0^*$ and $Z'_{\mathcal{C}} = \text{reach}(\mathcal{S}^*)$. Then from (10), we get that $Z_0^* \subseteq Z_{\mathcal{C}}^0$. We now proceed by induction. Let us assume that for some $k \in \mathbb{N}$, $Z_0^* \subseteq Z_{\mathcal{C}}^k$. Then, from (13), (14) and (16), we get that

$$\text{reach}(\mathcal{S}^*) \subseteq \text{max-inv}_F \left(\text{pre}_{F^{\delta}_{S\cap A}}(Z_0^*)\right) \subseteq Z_{\mathcal{C}}'^k.$$

Then, from (11), (12) and (17), we get that

$$\begin{aligned}Z_0^* &\subseteq \text{max-inv}_{F_{S\cap A}}(Z_0^*)\\ &\subseteq \text{max-inv}_{F_{S\cap A}}(Z_0^* \cap \text{reach}(\mathcal{S}^*)) \subseteq Z_{\mathcal{C}}^{k+1}.\end{aligned}$$

Hence, the first item of the proposition holds.

If for some $k \in \mathbb{N}$, $Z_{\mathcal{C}}^{k+1} = Z_{\mathcal{C}}^k$, then it follows from (16) and (17) that the conditions of Theorem 3 hold for $Z_{\mathcal{C}} = Z_{\mathcal{C}}^k$ and $Z'_{\mathcal{C}} = Z_{\mathcal{C}}'^k$. Hence, from Theorem 3, the contract is satisfied for the set of initial states $Z_0 = Z_{\mathcal{C}}^k$. It then follows from the maximality of Z_0^* that $Z_{\mathcal{C}}^k \subseteq Z_0^*$. Together, with the first item of the proposition, we can deduce the second item. □