Contract Based Design of Symbolic Controllers for Interconnected Multiperiodic Sampled-Data Systems

Adnane Saoud, Antoine Girard, Laurent Fribourg

Contract Based Design of Symbolic Controllers for Interconnected Multiperiodic Sampled-Data Systems*

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

***Abstract*— This paper deals with the synthesis of symbolic controllers for interconnected sampled-data systems where each component has its own sampling period. A compositional approach based on continuous-time assume-guarantee contracts is used. We provide sufficient conditions guaranteeing for a sampled-data system, satisfaction of an assume-guarantee contract and completeness of trajectories. Then, compositional results can be used to reason about interconnection of multiperiodic sampled-data systems. We then show how discrete abstractions and symbolic control techniques can be applied to enforce the satisfaction of contracts and ensure completeness of trajectories. Finally, theoretical results are applied to a vehicle platooning problem on a circular road, which show the effectiveness of our approach.**

I. INTRODUCTION

The use of symbolic models for the control of continuous and hybrid systems has attracted considerable attention in the past decade (see [1] and the references therein). A symbolic model (also called discrete abstraction) is a dynamical system with a finite number of states and related to the original system by some formal behavioral relationship (e.g. simulation, bisimulation and their alternating/approximate versions), which makes it possible to refine a symbolic controller, designed for the abstraction, into a concrete one that can be used on the original system. Symbolic controllers can be synthesized using techniques developed in the areas of supervisory control of discrete event systems [2] and algorithmic game theory [3]. Symbolic models are often obtained through discretization of the state-space and of the time (if the original system is continuous-time), see e.g. [4], [5].

Due to discretization of the state-space, these abstraction techniques suffer from the curse of dimensionality (the number of symbolic states increases exponentially with respect to the state-space dimension). For large systems made of interconnected components, a way to tackle the lack of scalability is to develop compositional methods for abstraction or symbolic controller synthesis (see e.g. [6], [7], [8], [9], [10], [11], [12]). The authors in [6] proposed a compositional abstraction based on the notion of interconnection-compatible approximate bisimulation. In [13], the notion of (approximate) disturbance simulation was used for compositional abstraction of continuous-time systems, where the states of the neighbouring components were modeled as disturbance signals. The results in [10] provide compositional constructions of approximately bisimilar finite abstractions for networks of discrete-time control systems under some incremental stability properties and using a small-gain type conditions.The authors in ([7], [9], and [11]) use assume-guarantee reasoning and contract based design to provide compositional synthesis.

Existing approaches assume that sampling periods of all components are equal. In this paper, we use a compositional approach to symbolic controller synthesis, based on *continuous-time assume-guarantee contracts* [14], which makes it possible to reason on the interconnection of sampled-data systems (such as those synthesized using symbolic control techniques) where we have different components with different sampling periods (multiperiodic sampling). We rely on a notion of strong satisfaction of such assume-guarantee contracts introduced in [15], which allows us to deal with cascade and feedback compositions. We first provide a simple criteria for a sampled-data system to strongly satisfy an assume-guarantee contract and ensure the completeness of maximal trajectories. We then show how symbolic control techniques can be applied to enforce those criteria. We illustrate our approach with several numerical experiments on a vehicle platooning problem [16].

The paper is organized as follows. In Section II, we briefly present the general framework introduced in [15], for compositional reasoning using assume-guarantee contracts. Then, we instantiate this framework to reason about multiperiodic interconnections of sampled-data systems. In Section III we show how symbolic control techniques can be used to enforce the specified assume-guarantee contracts and ensure completeness of trajectories. In Section IV, we apply the theoretical framework to a vehicle platooning problem. The proofs for the lemmas, propositions and theorems can be found in the appendix.

Notations: $\mathbb{R}$, $\mathbb{R}_0^+$, $\mathbb{R}^+$ denote the set or reals, nonnegative reals and positive reals respectively. 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 $I \in \mathbb{I}(\mathbb{R}_0^+)$ and a metric space X, $C(I,X)$ denote the set of continuous functions from I to X. $\mathbb{N}$ denote the set of nonnegative integers. Given two sets A and B, a set-valued map $f : A \rightrightarrows B$ is a map from A to the set of subsets of B, its domain is $\text{dom}(f) = \{a \in A |\ f(a) \neq \emptyset\}$. For $x \in \mathbb{R}^n$, $\|x\|$ denotes the Euclidean norm of x. For $\varepsilon \in \mathbb{R}^+$, $A \subseteq \mathbb{R}^n$ the ε-expansion

*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]LSV, CNRS, ENS Paris-Saclay, 61, avenue du Président Wilson, 94235 Cachan Cedex, France. fribourg@lsv.fr

of A is $\mathcal{B}_\varepsilon(A) = \{y \in \mathbb{R}^n \mid \exists x \in A, \|x - y\| \leq \varepsilon\}$.

II. Contracts for sampled-data systems

A. Systems and contracts

In this paper, we deal with sampled-data systems consisting of continuous-time systems with periodic controllers. In this section, we present a broader class of systems and associated assume-guarantee contracts, introduced in [15], which will allow us to reason on interconnection of sampled-data systems, even when components have different sampling periods. The results are stated without proofs, which can be found in [15].

1) Systems and interconnections:

Definition 1: A *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 external inputs, states, and outputs;
- $\mathcal{T}$ is a set of trajectories $(w, x, y) : I \to W \times X \times Y$ where $I \in \mathbb{I}(\mathbb{R}_0^+)$ and $y \in C(I, Y)$.

Given two trajectories $(w, x, y) : I \to W \times X \times Y$ and $(w', x', y') : I' \to W \times X \times Y$ in $\mathcal{T}$, (w, x, y) is said to be a *prefix* of (w', x', y') if $I \subseteq I'$ and for all $t \in I$, $w(t) = w'(t)$, $x(t) = x'(t)$ and $y(t) = y'(t)$. A trajectory $(w, x, y) \in \mathcal{T}$ is said to be *maximal* if there does not exist any trajectory $(w', x', y') \in \mathcal{T}$ such that $(w', x', y') \neq (w, x, y)$ and (w, x, y) is a prefix of (w', x', y'). A trajectory $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ is said to be *complete* if $I = \mathbb{R}_0^+$.

We consider elementary interconnections of systems that can be described using cascade and feedback compositions and formally defined as follows.

Definition 2: 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, with $Y_1 \subseteq W_2$. 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 3: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a system with $Y \subseteq W$. 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 $y = w$.

Note that systems obtained by 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 $x : I \to X$. Other system interconnections considered in this paper are defined using cascade and feedback compositions as shown in Figure 1.

2) Assume-guarantee contracts: Contracts make it possible to reason about the interconnection of systems based on properties of its components [14]. In this paper, we consider the following type of contracts:

Definition 4: Let $\Sigma = (W, X, Y, \mathcal{T})$ be a system, an *assume-guarantee contract* for Σ is a tuple $\mathcal{C} = (A_W, G_X, G_Y)$ where:

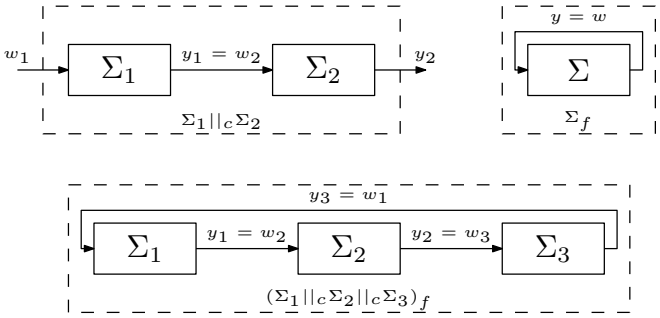

Fig. 1. Cascade, feedback compositions and an example of interconnection of systems

- $A_W \subseteq W$ 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 *strongly satisfies* contract $\mathcal{C}$, 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 $s \in [0, t+\delta] \cap I$, $y(s) \in G_Y$.

An assume-guarantee contract states that if the system's input belongs to A_W up to a time instant t, then the system's state belongs to G_X at least until t, and the system's output belongs to G_Y until $t + \delta$ with $\delta > 0$ (or $\delta = 0$ in case of *weak satisfaction*, see [15]).

3) Compositional reasoning: We now provide results allowing to reason about cascade and feedback compositions of systems:

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 $\mathcal{C}_c = (A_{W_1}, G_{X_1} \times G_{X_2}, G_{Y_2})$. If $\Sigma_1 \models_s \mathcal{C}_1$ and $\Sigma_2 \models_s \mathcal{C}_2$, then $\Sigma_1 ||_c \Sigma_2 \models_s \mathcal{C}_c$.

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 $t \in I$, $x(t) \in G_X$.

Remark 1: While weak satisfaction of assume-guarantee contracts is sufficient to reason about cascade composition, strong satisfaction as given in Definition 4 is critical to reason about feedback composition.

B. Sampled-data systems

In this section, we introduce the class of sampled-data systems and show that these can be embedded in the framework presented above. We then provide sufficient conditions for

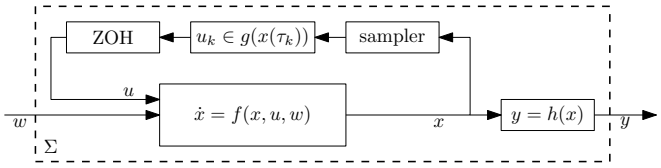

Fig. 2. Sampled-data system

sampled-data systems to satisfy assume-guarantee contracts and ensure completeness of maximal trajectories.

Definition 5: A *sampled-data system* is a tuple $\Sigma = (W, X, Y, U, f, g, h, \tau)$ where

- $W \subseteq \mathbb{R}^m$, $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^p$, are the sets of external inputs, states, and outputs;
- $U \subseteq \mathbb{R}^q$ is the set of internal inputs;
- $f : X \times U \times W \to \mathbb{R}^n$ is a map, $g : X \rightrightarrows U$ is a set valued-map, and $h : X \to Y$ is a continuous map;
- $\tau \in \mathbb{R}^+$ is the sampling period.

A pictural representation of a sampled-data system is shown in Figure 2. In this paper, we make the following assumption:

Assumption 1: For all $x_0 \in \text{dom}(g)$, $u \in g(x_0)$, $w \in C([0, \tau], W)$, there exists a unique solution $x : [0, \tau] \to X$ to the differential equation:

$$\dot{x}(t) = f(x(t), u, w(t)),\ x(0) = x_0. \tag{1}$$

We use the notation $x = \chi(., x_0, u, w)$ to denote to the solution of (1).

Let us remark that f need not be continuous, so we consider solutions of differential equations in the Caratheodory sense (see e.g. [17]).

The sequence of *sampling instants* $(\tau_k)_{k\in\mathbb{N}}$ is given by $\tau_k = k\tau$, for $k \in \mathbb{N}$. The initial sampling instant τ_0 coincides with the initial time 0. Sampled-data systems can be seen as systems in the sense of Definition 1 where a trajectory in $\mathcal{T}$ is a triple $(w, x, y) : I \to W \times X \times Y$, where $I = [0, \tau_{l+1}]$ with $l \in \mathbb{N}$ or $l = +\infty$ (then $I = \mathbb{R}_0^+$), w and y are continuous, x is absolutely continuous, and for all $k \in \mathbb{N}$ with $k \leq l$, $x(\tau_k) \in \text{dom}(g)$, and there exists $u_k \in g(x(\tau_k))$ such that

$$\begin{cases} \dot{x}(t) = f(x(t), u_k, w(t)), & \text{for almost all } t \in [\tau_k, \tau_{k+1}] \\ y(t) = h(x(t)), & \text{for all } t \in [\tau_k, \tau_{k+1}] \end{cases}$$

Let us remark that in particular, $x(0) = x(\tau_0) \in \text{dom}(g)$.

Assumption 1 guarantees that trajectories of Σ are well-defined between the sampling instants: given $x(\tau_k) \in \text{dom}(g)$, $u_k \in g(x(\tau_k))$, and values of w on $[\tau_k, \tau_{k+1}]$, x and y can be defined on $[\tau_k, \tau_{k+1}]$. Then, it follows that maximal trajectories of Σ are either complete (i.e. $l = +\infty$) or incomplete (i.e. $l \in \mathbb{N}$) with $x(\tau_{l+1}) \notin \text{dom}(g)$.

Cascade and feedback composition of sampled systems are defined according to Definitions 2 and 3. Let us remark that components have generally different sampling periods, and thus interconnection of sampled systems may not be definable in the formalism of Definition 5.

Remark 2: In this paper, it is assumed that all sampled systems have the same initial sampling time $\tau_0 = 0$. This restriction is made for the sake of simplicity and the following results could be generalized to interconnections of sampled systems with an initial clock drift ($\tau_0 \in [0, \tau)$).

An assume-guarantee contract $\mathcal{C} = (A_W, G_X, G_Y)$ for sampled-data systems is given by Definition 4. The following result, gives sufficient conditions for strong satisfaction of contracts:

Proposition 1: Let $\Sigma = (W, X, Y, U, f, g, h, \tau)$ be a sampled-data system satisfying Assumption 1, and let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ with $h(G_X) \subseteq G_Y$ and $\text{dom}(g) \subseteq G_X$. Let us assume that there exists $\varepsilon > 0$ such that for all $x_0 \in \text{dom}(g)$, $u \in g(x_0)$ and $w \in C([0, \tau], W)$, $x = \chi(., x_0, u, w)$ satisfies:

$$(\forall t \in [0, \tau],\ w(t) \in A_W) \implies (\forall t \in [0, \tau],\ x(t) \in G_X); \tag{2}$$

$$(\forall t \in [0, \tau],\ w(t) \in \mathcal{B}_\varepsilon(A_W) \implies (\forall t \in [0, \tau],\ h(x(t)) \in G_Y). \tag{3}$$

Then, $\Sigma \models_s \mathcal{C}$.

The following result complements the previous one by providing sufficient conditions for the existence of complete trajectories of a sampled-data system:

Proposition 2: Let $\Sigma = (W, X, Y, U, f, g, h, \tau)$ be a sampled-data system satisfying Assumption 1, and let $\mathcal{C} = (A_W, G_X, G_Y)$ be an assume-guarantee contract for Σ. Let us assume that for all $x_0 \in \text{dom}(g)$, $u \in g(x_0)$ and $w \in C([0, \tau], W)$, $x = \chi(., x_0, u, w)$ satisfies:

$$(\forall t \in [0, \tau],\ w(t) \in A_W) \implies (x(\tau) \in \text{dom}(g)). \tag{4}$$

Then, all maximal trajectories $(w, x, y) : I \to W \times X \times Y$ in $\mathcal{T}$ such that for all $t \in I$, $w(t) \in A_W$, are complete (i.e. $I = \mathbb{R}_0^+$).

Propositions 1 and 2 provide simple criteria guaranteeing for a sampled-data system, strong satisfaction of an assume-guarantee contract and completeness of trajectories. Intuitively, Proposition 1 gives conditions on the behavior between the sampling instants, while Proposition 2 gives conditions on the behavior at the sampling instants. Then, Theorems 1 and 2 allow us to reason about interconnection of sampled-data systems.

Given a sampled data system and an assume-guarantee contract, in the following we show how symbolic control techniques can be used to enforce the strong satisfaction of such contract while ensuring the completeness of the maximal trajectories. Hence, the design problem can be formulated as follows:

Problem 1: For sampled-data system $\Sigma = (W, X, Y, U, f, g, h, \tau)$, and $\tau > 0$, and for assume-guarantee contract $\mathcal{C} = (A_W, G_X, G_Y)$ with $h(G_X) \subseteq G_Y$, design a control map $g : X \rightrightarrows U$ such that $\Sigma \models_s \mathcal{C}$ and all maximal trajectories $(w, x, y) : I \to W \times X \times Y$ of Σ such that for all $t \in I$, $w(t) \in A_W$, are complete.

In the following, we provide a solution to Problem 1, based on conditions given by Propositions 1 and 2 and symbolic control techniques.

III. Symbolic control design

In this section, we design a control map $g : X \rightrightarrows U$, which is a solution to Problem 1.

A. Symbolic model

In this part, we show how to compute a symbolic abstraction, which guarantees by design the fulfilment of the conditions of Proposition 1 for strong satisfaction of the assume-guarantee contracts.

Our symbolic abstraction is given by a transition system $\mathcal{A} = (X_d, U_d, \Delta)$ where X_d and U_d are finite sets of states and inputs, and $\Delta : X_d \times U_d \rightrightarrows X_d$ is a transition relation.

1) Discretization: Our approach is based on a discretization of the state-space and input sets. We discretize the set of inputs U into $n_u \geq 2$ values, the discrete input set is given by: $U_d = \{\mathsf{u}_\ell |\ \ell = 0, \ldots, n_u - 1\}$. We discretize the state-space into $n_x \geq 1$ using a finite partition X_d of the set G_X given by: $X_d = \{\mathsf{x}_\ell |\ \ell = 0, \ldots, n_x - 1\}$. We define the quantizer $Q_{X_d} : G_X \to X_d$ associated to the partition X_d as follows: for $x \in G_X$ and $q \in X_d$, $Q_{X_d}(x) = q$ if and only if $x \in q$.

For a state of the abstraction $q \in X_d$, we denote the set of *enabled* inputs by $\text{enab}_\Delta(q) = \{u \in U_d |\ \Delta(q,u) \neq \emptyset\}$. We denote the set of *non-blocking* states by $\text{nb}_\Delta = \{q \in X_d |\ \text{enab}_\Delta(q) \neq \emptyset\}$.

2) Transition relation: We define the reachable set of (1) from a set of initial states $X_0 \subseteq X$ at $s \in \mathbb{R}_0^+$ under the constant control input $u \in U$ and a subset of disturbance inputs $W^* \subseteq W$ by:

$$R_s(X_0, u, W^*) = \{\chi(s, x_0, u, w) \;\Big|\; x_0 \in X_0,\ w : [0,s] \to W^*\}$$

Similarly the reachable set of (1) from a set of initial states $X_0 \subseteq X$ on $[0,t] \subseteq \mathbb{R}_0^+$ under the constant control input $u \in U$ and a subset of disturbance inputs $W^* \subseteq W$ is given by: $R_{[0,t]}(X_0, u, W^*) = \bigcup_{s \in [0,t]} R_s(X_0, u, W^*)$.

We suppose that we are able to compute an over-approximation of the reachable set denoted $\mathcal{R}$ (several methods exist for the computation of over-approximation of reachable sets for linear systems [18], monotone systems [19] or general nonlinear systems [20]).

The transition relation $\Delta : X_d \times U_d \rightrightarrows X_d$, abstracting the dynamics of the sampled-data system $\Sigma = (W, X, Y, U, f, g, h, \tau)$ is formally defined as follows.

Let $\varepsilon > 0$ arbitrarily small, $q \in X_d$ and $u \in U_d$, $q' \in \Delta(q,u)$ if and only if:

$$\begin{gathered} \mathcal{R}_{[0,\tau]}(q, u, A_W) \subseteq G_X; \\ h(\mathcal{R}_{[0,\tau]}(q, u, \mathcal{B}_\varepsilon(A_W))) \subseteq G_Y; \\ q' \cap \mathcal{R}_\tau(q, u, A_W) \neq \emptyset. \end{gathered} \tag{5}$$

Let us remark that for $q \in X_d$, $u \in \text{enab}_\Delta(q)$ if and only if the first two conditions of the transition relation (5) hold. The parameter ε used in this construction of the transition relation can be freely chosen but is critical to ensure the strong satisfaction of the contract using the criterion of Proposition 1.

The following Lemma establishes the formal behavioral relationship between the dynamics of $\mathcal{A}$ and Σ:

Lemma 1: Let Σ and $\mathcal{C}$ be as in Problem 1. Let $\mathcal{A} = (X_d, U_d, \Delta)$ be constructed as in Section III-A . Let $q \in \text{nb}_\Delta$, $x_0 \in q$, $u \in \text{enab}_\Delta(q)$, $w \in C([0,\tau], W)$ such that for all $t \in [0,\tau]$, $w(t) \in A_W$, and $x = \chi(., x_0, u, w)$. Then, there exists $q' \in \Delta(q,u)$ such that $x(\tau) \in q'$.

Intuitively, the previous Lemma shows that $\mathcal{A}$ relates formally to the uncontrolled (i.e. with $g(x) = U$ for all $x \in U$) dynamics of Σ at sampling times with external inputs constrained in A_W by an alternating simulation relation [1]. The next proposition provides a simple condition relating the control map g to be designed to the symbolic abstraction $\mathcal{A}$, which guarantees the strong satisfaction of assume-guarantee contracts:

Proposition 3: Let Σ and $\mathcal{C}$ be as in Problem 1. Let $\mathcal{A} = (X_d, U_d, \Delta)$ be constructed as in Section III-A. If the control map $g : X \rightrightarrows U$ satisfies:

$$\text{dom}(g) \subseteq G_X \text{ and } \forall x \in G_X,\ g(x) \subseteq \text{enab}_\Delta(Q_{X_d}(x)), \tag{6}$$

then, $\Sigma \models_s \mathcal{C}$.

B. Symbolic controller synthesis

In this section, we show how to design the control map $g : X \rightrightarrows U$, solving Problem 1. We state the main result of this section:

Theorem 3: Let Σ and $\mathcal{C}$ be as in Problem 1. Let $\mathcal{A} = (X_d, U_d, \Delta)$ be constructed as in Section III-A. Let the discrete controller $\Theta : X_d \rightrightarrows U_d$ for the abstraction $\mathcal{A}$ satisfying:

$$\forall q \in X_d,\ \Theta(q) \subseteq \text{enab}_\Delta(q), \tag{7}$$

$$\forall q \in \text{dom}\Theta,\ \forall u \in \Theta(q),\ \Delta(q,u) \subseteq \text{dom}(\Theta), \tag{8}$$

Let the control map $g : X \rightrightarrows U$ of Σ defined by:

$$\text{dom}(g) \subseteq G_X \text{ and } \forall x \in G_X,\ g(x) = \Theta(Q_{X_d}(x)) \tag{9}$$

Then, $\Sigma \models_s \mathcal{C}$ and all maximal trajectories $(w, x, y) : I \to W \times X \times Y$ of Σ such that for all $t \in I$, $w(t) \in A_W$, are complete.

The previous result establishes the conditions that the set-valued map $\Theta : X_d \rightrightarrows U_d$ has to satisfy in order to solve Problem 1. Let us remark that these conditions actually state that Θ is a discrete safety controller for the abstraction $\mathcal{A}$ keeping the trajectories of $\mathcal{A}$ in nb_Δ. Thus, Θ can be synthesized by computing the maximal controlled invariant of $\mathcal{A}$ in nb_Δ, which can be done by a maximal fixed point computation (see e.g. [1]).

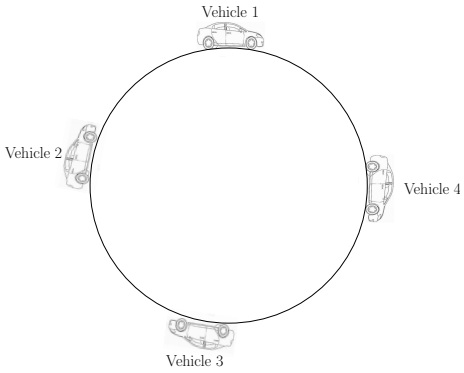

Fig. 3. A platoon of 4 vehicles on a circular road

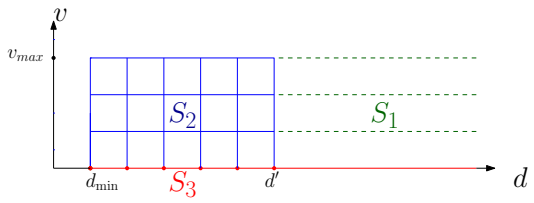

Fig. 4. Partition of $G_X = [d_{\min}, +\infty) \times [0, v_{\max}]$ with $n_d = 5$ and $n_v = 3$.

IV. Vehicle platooning example

A. Model description

In the following, we consider a platoon where each vehicle is modeled as a nonlinear and nonsmooth control system. We shall adapt the model from [16]:

$$M\dot{v} = \alpha(F, v) = \begin{cases} F - f_0 - f_1 v - f_2 v^2 & \text{if} \quad v > 0 \\ \max(F - f_0, 0) & \text{if} \quad v = 0 \end{cases} \tag{10}$$

where $M > 0$ represent the mass of the vehicle, v its velocity, F is the net engine torque applied to the wheels and the term $f_0 + f_1 v + f_2 v^2$ include the rolling resistance and aerodynamics ($f_0, f_1, f_2 \in \mathbb{R}^+$). In this equation, F is the control input and satisfies $F \in [F_{\min}, F_{\max}]$, where $F_{\min} < 0 < F_{\max}$.

Contrarily to [16], we have added the second equation to eliminate the unrealistic behaviour where the vehicle is moving backward (i.e $v(t) \geq 0$ for all $t \in \mathbb{R}_0^+$).

In this paper, we deal with a platoon of m vehicles in a circular road (see Figure 3). The dynamic of each vehicle $i \in \{1, \ldots, m\}$ is given by:

$$\begin{cases} \dot{d}_i &= v_{i-1} - v_i \\ M\dot{v}_i &= \alpha(F_i, v_i). \end{cases} \tag{11}$$

with the convention that $v_0 = v_m$, where $d_i \geq 0$ represents the relative distance between vehicle i and the preceding vehicle $i-1$, v_i its velocity and F_i its control input.

We can see that the dynamic of the vehicle is not continuous, however it can be easily shown that we have the existence and uniqueness of solution and Assumption 1 is satisfied.

Remark 3: We assume that all vehicles are identical only to keep notations simple. However, our approach can be extended directly to heterogeneous vehicles with α_i depending on the vehicle parameters $(M_i, f_{0i}, f_{1i}, f_{2i})$.

B. Problem formulation and solution strategy

Our goal is to synthesize controllers, giving values of input F_i, for all vehicles of a platoon such that the velocity of each vehicle remains between 0 and $v_{\max}$, and the relative distance between two vehicles remains larger than $d_{\min} \geq 0$:

$$\forall i \in \{1, \ldots, m\},\ \forall t \in \mathbb{R}_0^+,\ v_i(t) \in [0, v_{\max}] \\ \text{and} \quad d_i(t) \in [d_{\min}, +\infty) \tag{12}$$

Since, we are using symbolic control techniques, the dynamics of vehicle i can then be described by a sampled-data system $\Sigma_i = (W, X, Y, U, f, g_i, h, \tau_i)$ where the external input $w_i = v_{i-1}$, the state $x_i = (d_i, v_i)^T$, the output $y_i = v_i$, the dynamic of the vehicle f is given by (11) and $W = \mathbb{R}_0^+,\ X = \mathbb{R} \times \mathbb{R}_0^+,\ Y = \mathbb{R}_0^+,\ U = [F_{\min}, F_{\max}]$.

Then, the dynamics of the vehicle platoon on a cyclic road is given by the feedback-cascade composition $(\Sigma_1 ||_c \ldots ||_c \Sigma_m)_f$. Therefore, in view of Theorems 1 and 2, the control objective (12) can be achieved by assigning a suitable contract $\mathcal{C}$ to each vehicle in the platoon and resolving Problem 1 for the system Σ_i and the contract $\mathcal{C}$.

We assign the assume-guarantee contracts $\mathcal{C} = (A_W, G_X, G_Y)$ to systems Σ_i where $A_W = G_Y = [0, v_{\max}]$ and $G_X = [d_{\min}, +\infty) \times [0, v_{\max}]$. We use the symbolic approach presented in Section III-A to construct an abstraction $\mathcal{A}$ of Σ_i which guarantees by design the strong satisfaction of the contract $\mathcal{C}$. Then, a safety controller Θ is synthesized for the abstraction $\mathcal{A}$ and refined into a controller $g : X \rightrightarrows U$ for the system Σ_i ensuring the completeness of maximal trajectories, using the approach presented in III-B. First, we explain the partitioning technique used for this problem.

C. Abstraction

Given the state space G_X and let $d' > d_{\min}$, we have that $G_X = S_1 \cup S_2 \cup S_3$, where: $S_1 = [d', +\infty) \times (0, v_{\max}]$, $S_2 = [d_{\min}, d'] \times (0, v_{\max}]$ and $S_3 = [d_{\min}, +\infty) \times \{0\}$, as shown in figure 4. Using n_v and n_d as abstraction parameters for velocity and distance axis respectively, partitions of S_1, S_2 and S_3 are constructed as follows:

- We use unbounded regions for the partition of the set S_1. Let us remark that this is necessary to cover the unbounded set G_X with a finite number of subsets;
- We construct a partition of S_2 using a uniform grid;
- We use regions with empty interior (flat symbols) for the set S_3. This is necessary to discriminate the case when the velocity is 0 from the case when it belongs to $(0, v_{\max}]$. For instance, if the leading vehicle stops and remains motionless, it is necessary to stop the following vehicle. Not being able to discriminate the

case when the velocity is 0 from the case when it is (even slightly) positive would result in uncontrollable symbolic abstraction. Moreover, the partition of the set S_3 contains an unbounded region corresponding to $[d', +\infty) \times \{0\}$.

Remark 4: We can see that our partition differs from the classical partitions used in the literature. Indeed the problem cannot be solved using a uniform partition for the reasons stated above. This constraints are specific to this particular problem. The approach of the paper can also be applied to other systems for which a simple uniform partition can be used.

The input space $U = [F_{\min}, F_{\max}]$ is uniformly discretized into n_u values. The transition relation is constructed based on (5) where we used the monotonicity of the system to construct an overapproximation of the reachable set.

D. Numerical results

In this section, we illustrate our results using numerical simulations. We use the numerical values from [21] for the vehicle parameters. These values as well as the contract parameters are shown in Table I.

TABLE I
VEHICLE AND CONTRACT PARAMETERS

Parameter	Value	Unit
M	1370	Kg
f_0	51.0709	N
f_1	0.3494	Ns/m
f_2	0.4161	Ns^2/m^2
F_{min}	-4031.9	mKg/s^2
F_{max}	2687.9	mKg/s^2
d_{max}	-10	m
v_{max}	15	m/s

We compute the symbolic abstraction $\mathcal{A}$ using the approach described in Section III-A, with the partition technique presented in Section IV-C. For discrete controller synthesis, the maximal fixed point computation allows us to determine the most permissive safety controller. The controller Θ is obtained after determinization of the most permissive safety controller by selecting the maximal safe input. Intuitively, it means that the vehicles drive as fast as possible while guaranteeing satisfaction of assume-guarantee contracts.

Figure 5 represents the resulting controller g for sampling period $\tau = 0.5$, parameter of the construction of the transition relation $\varepsilon = \frac{v_{\max}}{1000}$ and the following values of abstraction parameters: $n_u = 10$, $d' = 70$, $n_d = 70$, $n_v = 30$. The computation time for generating the symbolic abstraction and synthesizing the controller is about 1 minute (implementation in MATLAB, Processor 2.7 GHz Intel Core i5, Memory 8 GB 1867 MHz DDR3).

The choice of the abstraction parameters is important, of course the larger n_u, n_d and n_v, the more accurate the abstraction. In particular, small values of these parameters may lead to uncontrollable abstractions (i.e. the maximal controlled invariant of $\mathcal{A}$ is empty). The choice of parameter

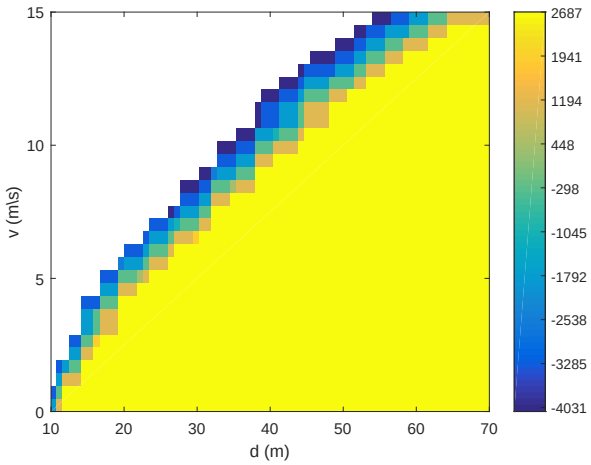

Fig. 5. Synthesized control map g.

d' also has an influence, if d' too close to the value $d_{\min}$, then the vehicles will not be able to drive at maximal speed. On Figure 5, we can see that if we modify and set $d' = 50$, $n_d = 50$, then the vehicles speed will never exceed $13m/s$.

For numerical simulations, we consider a platoon of 20 vehicles. We consider identical vehicles, with parameters given by Table I, to emphasize the effect of the sampling periods. However the same approach can be applied even if we have heterogeneous vehicles.

1) Periodic sampling: We consider that all the vehicles have the same sampling period $\tau = 0.5$, and the same abstraction parameters. Note that these parameters are the same as the ones used for computing the controller shown on Figure 5.

Figure 6 shows the simulation results for given initial conditions. One can check that distances between vehicles are always greater than 10 m and that velocities remain between 0 and 15 m/s at all time, so the overall objective is satisfied. It is interesting to remark that after a transient period, the vehicles distribute themselves uniformly on the road (i.e. the distances between vehicles are all equal) and drive at almost constant speed.

2) Multiperiodic sampling: We consider 20 vehicles with different sampling periods, where 7 vehicles have the sampling periods in $[0.5, 0.62]$, 6 vehicles have the sampling periods in $[1.3, 1.4]$ and 7 vehicles have their sampling periods in $[2, 2.12]$.

Figure 7 shows the simulation results. One can check that distances between vehicles are always greater than 10 m and that velocities remain between 0 and 15 m/s at all time, so the overall objective is satisfied despite multiperiodic sampling. Similar to the periodic sampling case, we remark that after a transient period, the vehicles drive at almost constant speed. However, it is interesting to note that the final speed is smaller than in the periodic sampling case. An even more significant difference is seen on the inter-vehicle distances. Indeed, the vehicles do not distribute uniformly on the road. On this simulation, one can see that the vehicles

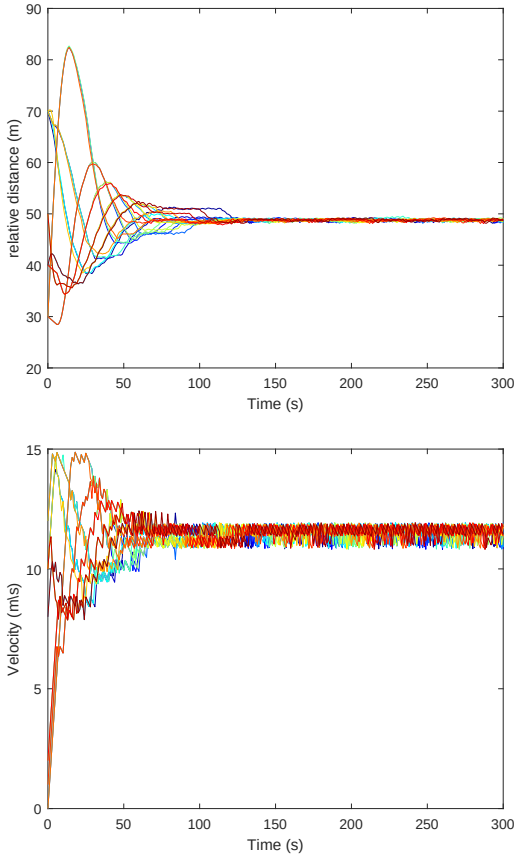

Fig. 6. Simulation results of a platoon of 20 vehicles on a circular road with the same sampling period: inter-vehicle distance (top), velocities (bottom).

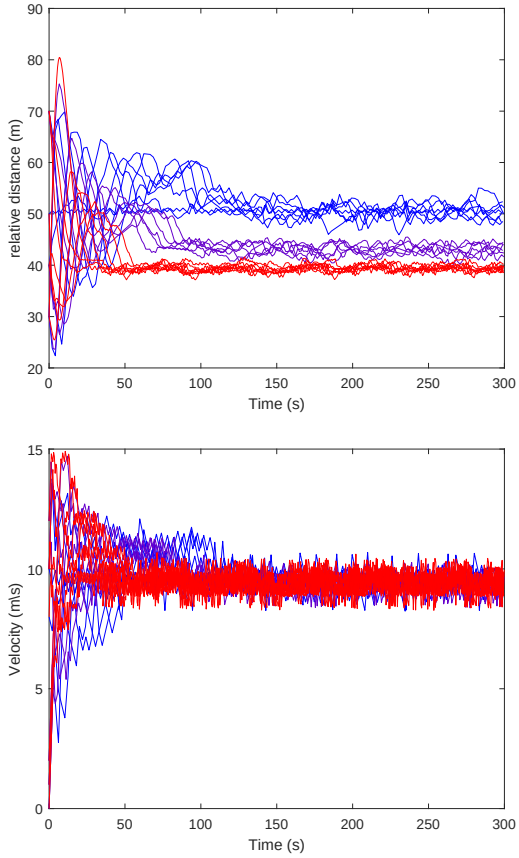

Fig. 7. Simulation results of a platoon of 20 vehicles on a circular road with different sampling periods: inter-vehicle distance (top), velocities (bottom)(red: vehicles with different sampling periods in $[0.5, 0.62]$, purple: vehicles with different sampling periods in $[1.3, 1.4]$, blue: vehicles with different sampling periods in $[2, 2.12]$).

with larger sampling period need to keep a larger distance to the front vehicle, which can be explained by the fact, that they need more time to react.

V. Conclusion

In this paper, we have presented a compositional approach to the design of interconnected sampled-data systems, based on a notion of continuous-time assume-guarantee contracts. This approach makes it possible to deal with heterogeneous components with different sampling periods. Synthesis of the sampled-data controller is addressed using discrete abstraction and symbolic controller synthesis. This approach has been applied to the design of controllers for vehicle platooning and numerical results show the effectiveness of the approach and reveal some interesting behaviours of these vehicle platoons. In future work, we will develop more general contracts, which may include dynamical models of external inputs and study their composition. These contracts will be applied to vehicle platooning where a model of the front vehicle can be taken into account during controller synthesis. We will also extend the results from cascade and feedback interconnections, to different types of interconnections.

References

[1] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[2] C. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[3] R. Bloem, B. Jobstmann, N. Piterman, A. Pnueli, and Y. Sa'ar, "Synthesis of reactive (1) designs," *Journal of Computer and System Sciences*, vol. 78, no. 3, pp. 911–938, 2012.

[4] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2010.

[5] G. Reißig, "Computing abstractions of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 11, pp. 2583–2598, 2011.

[6] Y. Tazaki and J.-i. Imura, "Bisimilar finite abstractions of interconnected systems," *Hybrid Systems: Computation and Control*, pp. 514–527, 2008.

[7] E. Dallal and P. Tabuada, "On compositional symbolic controller synthesis inspired by small-gain theorems," in *IEEE Conference on Decision and Control*, pp. 6133–6138, 2015.

[8] E. Kim, M. Arcak, and S. Seshia, "Compositional controller synthesis for vehicular traffic networks," in *IEEE Conference on Decision and Control*, pp. 6165–6171, 2015.

[9] 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*, pp. 119–133, 2016.

[10] G. Pola, P. Pepe, and M. Di Benedetto, "Symbolic models for networks of control systems," *IEEE Transactions on Automatic Control*, vol. 61, pp. 3663–3668, November 2016.

[11] P.-J. Meyer, A. Girard, and E. Witrant, "Compositional abstraction and safety synthesis using overlapping symbolic models," *IEEE Transactions on Automatic Control*, 2017. To appear.
[12] A. Saoud, P. Jagtap, M. Zamani, and A. Girard, "Compositional abstraction-based synthesis for cascade discrete-time control systems," in *IFAC Conference on Analysis and Design of Hybrid Systems*, 2018.
[13] K. Mallik, A.-K. Schmuck, S. Soudjani, and R. Majumdar, "Compositional abstraction-based controller synthesis for continuous-time systems," *arXiv preprint arXiv:1612.08515*, 2016.
[14] 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," tech. rep., Inria Rennes Bretagne Atlantique; INRIA, 2015.
[15] A. Saoud, A. Girard, and L. Fribourg, "On the composition of discrete and continuous-time assume-guarantee contracts for invariance," in *European Control Conference*, 2018.
[16] P. Ioannou and C.-C. Chien, "Autonomous intelligent cruise control," *IEEE Transactions on Vehicular Technology*, vol. 42, no. 4, pp. 657–672, 1993.
[17] A. Filippov, *Differential Equations with Discontinuous Righthand Sides*. Kluwer Academic Publishers, 1985.
[18] C. Le Guernic and A. Girard, "Reachability analysis of linear systems using support functions," *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 250–262, 2010.
[19] N. Ramdani, N. Meslem, and Y. Candau, "Computing reachable sets for uncertain nonlinear monotone systems," *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 263–278, 2010.
[20] G. Reissig, A. Weber, and M. Rungger, "Feedback refinement relations for the synthesis of symbolic controllers," *IEEE Transactions on Automatic Control*, vol. 62, no. 4, pp. 1781–1796, 2017.
[21] P. Nilsson, O. Hussien, Y. Chen, A. Balkan, M. Rungger, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada, "Preliminary results on correct-by-construction control software synthesis for adaptive cruise control," *IEEE Conference on Decision and Control*, pp. 816–823, 2014.

APPENDIX

Proof of Proposition 1

Proof: Let $(w,x,y) : I \to W \times X \times Y$ be a trajectory of Σ. We have $h(x_0) \in h(\text{dom}(g)) \subseteq h(G_X) \subseteq G_Y$.

Let $t \in I$, such that for all $s \in [0,t]$, $w(s) \in A_W$, let $m \in \mathbb{N}$ such that $\tau_m \leq t < \tau_{m+1}$.

For $k \in \{0,\dots,m-1\}$, $\tau_k \in I$, $x(\tau_k) \in \text{dom}(g)$ and there exists $u_k \in g(x(\tau_k))$ such that for almost all $s \in [\tau_k, \tau_{k+1}]$, $\dot{x}(s) = f(x(s), u_k, w(s))$. Then, by (2), since for all $s \in [\tau_k, \tau_{k+1}]$, $w(s) \in A_W$, we have for all $s \in [\tau_k, \tau_{k+1}]$, $x(s) \in G_X$. By (3), we get that for all $s \in [\tau_k, \tau_{k+1}]$, $y(s) = h(x(s)) \in G_Y$. We also have $\tau_m \in I$, for which we consider two distinct cases.

If $I = [0, \tau_m]$, then $t = \tau_m$, and it follows from above that for all $s \in [0,t]$, $x(s) \in G_X$ and for any $\delta > 0$, for all $s \in [0,t] = [0, t+\delta] \cap I$, $y(s) \in G_Y$.

If $I \neq [0, \tau_m]$, then $[0, \tau_{m+1}] \subseteq I$, $x(\tau_m) \in \text{dom}(g)$ and there exists $u_m \in g(x(\tau_m))$ such that for almost all $s \in [\tau_m, \tau_{m+1}]$, $\dot{x}(s) = f(x(s), u_m, w(s))$. We have for all $s \in [\tau_m, t]$, $w(s) \in A_W$. Let us start by proving the guarantee on the state. Let $\bar{w} : [\tau_m, \tau_{m+1}] \to W$ given by $\bar{w}(s) = w(s)$ for $s \in [\tau_m, t]$ and $\bar{w}(s) = w(t)$ for $s \in [t, \tau_{m+1}]$. $\bar{w}$ is continuous and since for all $s \in [\tau_m, t]$, $w(s) \in A_W$, we have for all $s \in [\tau_m, \tau_{m+1}]$, $\bar{w}(s) \in A_W$. Then, let $\bar{x} : [\tau_m, \tau_{m+1}] \to X$ be the solution of the differential equation $\dot{\bar{x}}(s) = f(\bar{x}(s), u_m, \bar{w}(s))$ with $\bar{x}(\tau_m) = x(\tau_m)$. Then, by (2), we have for all $s \in [\tau_m, \tau_{m+1}]$, $\bar{x}(s) \in G_X$. Moreover, by Assumption 1, it follows that $\bar{x}(s) = x(s)$ for all $s \in [\tau_m, t]$. Hence, for all $s \in [0,t]$, $x(s) \in G_X$. For the guarantee on the output, using the fact that for all $s \in [\tau_m, t]$, $w(s) \in A_W$, from the continuity of w and for $\varepsilon > 0$, there exists $\delta > 0$ such that for all $s \in [\tau_m, t+\delta]$, $w(s) \in \mathcal{B}_\varepsilon(A_W)$. We suppose without loss of generality that $\delta < \tau_{m+1} - t$. Let $w^* : [\tau_m, \tau_{m+1}] \to W$ given by $w^*(s) = w(s)$ for $s \in [\tau_m, t+\delta]$ and $w^*(s) = w(t+\delta)$ for $s \in [t+\delta, \tau_{m+1}]$. w^* is continuous and since for all $s \in [\tau_m, t+\delta]$, $w(s) \in \mathcal{B}_\varepsilon(A_W)$, we have for all $s \in [\tau_m, \tau_{m+1}]$, $w^*(s) \in \mathcal{B}_\varepsilon(A_W)$. Then, using a similar reasoning to the guarantee on the states, we have for all $s \in [\tau_m, t+\delta] = [\tau_m, t+\delta] \cap I$, $h(x(s)) \in G_Y$. ■

Proof of Proposition 2

Proof: Let us consider a maximal trajectory $(w,x,y) : I \to W \times X \times Y$ in $\mathcal{T}$ such that for all $t \in I$, $w(t) \in A_W$, and let us assume that (w,x,y) is not complete (i.e. $I = [0, \tau_{l+1}]$ with $l \in \mathbb{N}$). Then, $x(\tau_l) \in \text{dom}(g)$, $u_l \in g(x(\tau_l))$ and for almost all $t \in [\tau_l, \tau_{l+1}]$, $\dot{x}(t) = f(x(t), u_l, w(t))$; it follows from (4) that $x(\tau_{l+1}) \in \text{dom}(g)$. Then, let:

- $\bar{w} : [0, \tau_{l+2}] \to W$ be a continuous function such that for all $t \in [0, \tau_{l+1}]$, $\bar{w}(t) = w(t)$;
- $\bar{x} : [0, \tau_{l+2}] \to X$ be an absolutely continuous function such that for all $t \in [0, \tau_{l+1}]$, $\bar{x}(t) = x(t)$, and for all $t \in [\tau_{l+1}, \tau_{l+2}]$, $\dot{\bar{x}}(t) = f(\bar{x}(t), u_{l+1}, \bar{w}(t))$, for a $u_{l+1} \in g(x(\tau_{l+1}))$, such a function exists by Assumption 1;
- $\bar{y} : [0, \tau_{l+2}] \to Y$ be a continuous function such that for all $t \in [0, \tau_{l+1}]$, $\bar{y}(t) = y(t)$, and for all $t \in [\tau_{l+1}, \tau_{l+2}]$, $\bar{y}(t) = h(\bar{x}(t))$.

Then, it is clear that $(\bar{w}, \bar{x}, \bar{y}) \in \mathcal{T}$ and that (w,x,y) is a prefix of $(\bar{w}, \bar{x}, \bar{y})$ which contradicts the maximality of (w,x,y). Hence, necessarily, (w,x,y) is complete. ■

Proof of Lemma 1

Proof: Let $q \in \text{nb}_\Delta$, $x_0 \in q$, $u \in \text{enab}_\Delta(q)$ and $w \in C([0,\tau], W)$ such that for all $t \in [0,\tau]$, $w(t) \in A_W$. We have $x(\tau) = \chi(\tau, x_0, u, w) \subseteq \mathcal{R}_\tau(q, u, A_W) \subseteq \mathcal{R}_{[0,\tau]}(q, u, A_W) \subseteq G_X$. Hence, using the definition of the transition relation Δ there exists $q' \in \Delta(q,u)$ satisfying $x(\tau) \in q'$. ■

Proof of Proposition 3

Proof: We prove the strong satisfaction of the contract using Proposition 1.

Let us remark that $\text{dom}(g) \subseteq G_X$. Then, let $x_0 \in \text{dom}(g)$, $u \in g(x_0)$, $w \in C([0,\tau], W)$ and $x = \chi(.., x_0, u, w)$. By (6), $u \in \text{enab}_\Delta(q_0)$ where $q_0 = Q_{X_d}(x_0)$. First, let us suppose that for all $t \in [0,\tau]$, $w(t) \in A_W$, we have for all $t \in [0,\tau]$, $x(t) = \chi(t, x_0, u, w) \in \mathcal{R}_t(q_0, u, A_W) \subseteq \mathcal{R}_{[0,\tau]}(q_0, u, A_W) \subseteq G_X$, where the second inclusion comes from the first condition in the definition of the transition relation. Now, let $\varepsilon > 0$ be as in the definition of transition relation (5) and assume that for all $t \in [0,\tau]$, $w(t) \in \mathcal{B}_\varepsilon(A_W)$. We have for all $t \in [0,\tau]$, $h(x(t)) = h(\chi(t, x_0, u, w)) \in h(\mathcal{R}_t(q_0, u, \mathcal{B}_\varepsilon(\mathcal{A}_\mathcal{W}))) \subseteq h(\mathcal{R}_{[0,\tau]}(q_0, u, \mathcal{B}_\varepsilon(\mathcal{A}_\mathcal{W}))) \subseteq G_Y$, where the second inclusion comes from the second condition

of the definition of the transition relation. Hence, we can conclude that $\Sigma \models_s \mathcal{C}$. ■

Proof of Theorem 3

Proof: Let us remark that (9) and (7) imply that g satisfies the condition (6). Then, $\Sigma \models_s \mathcal{C}$. To prove the second part of the theorem, we show that condition (4) in Proposition 2 holds. Let $x_0 \in \text{dom}(g)$, $u \in g(x_0)$, $w \in C([0,\tau], W)$, and $x = \chi(., x_0, u, w)$. By (9), $u \in \Theta(q_0)$ where $q_0 = Q_{X_d}(x_0)$. By (7), $u \in \text{enab}_\Delta(q_0)$ and by Lemma 1, there exists $q' \in \Delta(q, u)$ such that $x(\tau) \in q'$. Then, (8) gives that $q' \in \text{dom}(\Theta)$, which in turn implies by (9) that $x(\tau) \in \text{dom}(g)$. ■