

# Design of Symbolic Controllers for Networked Control Systems

Alessandro Borri, Giordano Pola and Maria Domenica Di Benedetto <sup>\*†‡</sup>

## Abstract

Networked Control Systems (NCS) are distributed systems where plants, sensors, actuators and controllers communicate over shared networks. Non-ideal behaviors of the communication network include variable sampling/transmission intervals and communication delays, packet losses, communication constraints and quantization errors. NCS have been the object of intensive study in the last few years. However, due to the inherent complexity of NCS, current literature focuses on a subset of these non-idealities and mostly considers stability and stabilizability problems. Recent technology advances need different and more complex control objectives to be considered. In this paper we present first a general model of NCS, including most relevant non-idealities of the communication network; then, we propose a symbolic model approach to the control design with objectives expressed in terms of non-deterministic transition systems. The presented results are based on recent advances in symbolic control design of continuous and hybrid systems. An example in the context of robot motion planning with remote control is included, showing the effectiveness of the proposed approach.

## 1 Introduction

Networked Control Systems (NCS) are complex, heterogeneous, spatially distributed systems where physical processes interact with distributed computing units through non-ideal communication networks. In the past, NCS were limited in the number of computing units and in the complexity of the interconnection

---

<sup>\*</sup>The research leading to these results has been partially supported by the Center of Excellence DEWS and received funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement n. 257462 HYCON2 NoE.

<sup>†</sup>Alessandro Borri is with the Istituto di Analisi dei Sistemi ed Informatica "A. Ruberti", Consiglio Nazionale delle Ricerche (IASI-CNR), 00185 Rome, Italy, alessandro.borri@iasi.cnr.it.

<sup>‡</sup>Giordano Pola and Maria Domenica Di Benedetto are with the Department of Information Engineering, Computer Science and Mathematics, Center of Excellence for Research DEWS, University of L'Aquila, 67100, L'Aquila, Italy, {giordano.pola,mariadomenica.dibenedetto@univaq.it.}

network so that it was possible to obtain reasonable performance by aggregating subsystems that were locally designed and optimized. However the growth of complexity of the physical systems to control, together with the continuous increase in functions that these systems must perform, requires today to adopt a unified design approach where different disciplines (e.g. control systems engineering, computer science, software engineering and communication engineering) should contribute to reach new levels of performance. The heterogeneity of the subsystems that are to be connected in an NCS make the control of these systems a hard but challenging task. NCS have been the focus of much recent research in the control community: Murray et al. in [1] presented control over networks as one of the important future directions for control. Following [2], the most important non-idealities in the analysis of NCS are: (i) variable sampling/transmission intervals; (ii) variable communication delays; (iii) packet dropouts caused by the unreliability of the network; (iv) communication constraints (scheduling protocols) managing the possibly simultaneous transmissions over the shared channel; (v) quantization errors in the digital transmission with finite bandwidth. There are two approaches to deal with such non-idealities: the *deterministic* approach, which assumes worst-case (deterministic) bounds on the aforementioned imperfections, and the *stochastic* approach, which provides a stochastic description of the non-ideal communication network. We focus on the deterministic methods, which can be further distinguished according to the modeling assumptions and the controller synthesis: a) the discrete-time approach (see e.g. [3], [4]) considers discrete-time controllers and plants; b) the sampled-data approach (see e.g. [5], [6]) assumes discrete-time controllers and continuous-time (sampled-data) plants; c) the continuous-time (emulation) approach (see e.g. [7], [8]) focuses on continuous-time controllers and continuous-time (sampled-data) plants. Results obtained in the deterministic approach during the past few years are mostly about stability and stabilizability problems, see e.g. [9, 2, 10], and depend on the method considered and the assumptions on the non-ideal communication infrastructure. In addition, current approaches in the literature take into account only a subset of these non-idealities. As reviewed in [2], for example, [11] studies imperfections of type (i), (iv), (v), [3], [12], [6] consider simultaneously (i), (ii), (iii), [8] focuses on (i), (iii), (iv), while [5] manages (ii), (iii) and (v). Three types of non-idealities, namely (i), (ii), (iv), are considered for example in [13], [14], [7]. In [15], the five non-idealities are dealt with but small delay and other restrictive assumptions are considered. Finally, novel results in the stability analysis of NCS can be found in [16], [17], [18], [19]. However, existing results do not address control design of NCS with complex specifications, as for example safety properties, obstacle avoidance, language and logic specifications. This paper follows the deterministic approach and provides a framework for NCS control design where the aforementioned non-idealities from (i) to (v) can be taken into account. The proposed approach is based on the use of discrete abstractions of continuous and hybrid systems [20, 21], and follows the work in [22, 23, 24] based on the construction of *symbolic models* for nonlinear and switched control systems. As such, it offers a sound paradigm to solve con-

trol problems where software and hardware interact with the physical world, and to address a wealth of novel specifications that are difficult to enforce by means of conventional control design methods. Symbolic models are abstract descriptions of complex systems where a symbol corresponds to an “aggregate” of continuous states and a symbolic control label to an “aggregate” of continuous control inputs. Several classes of dynamical and control systems that admit equivalent symbolic models have been identified in the literature. Within the class of hybrid automata we recall timed automata [25], rectangular hybrid automata [26], and o-minimal hybrid systems [27, 28]. Early results for classes of control systems were based on dynamical consistency properties [29], natural invariants of the control system [30],  $l$ -complete approximations [31], and quantized inputs and states [32, 33]. Further works include results on controllable discrete-time linear systems [34], piecewise-affine and multi-affine systems [35], [36, 37], set-oriented discretization approach for discrete-time nonlinear optimal control problems [38], abstractions based on convexity of reachable sets [39], incrementally stable and incrementally forward complete nonlinear control systems with and without disturbances [22, 23, 40, 41], switched systems [42] and time-delay systems [43, 44]. The interested reader is referred to [45, 21] for an overview on recent advances in this domain.

This paper addresses the control design of a fairly general model of NCS with complex specifications, and provides an extended version of the preliminary results published in [46, 47]. In particular, while in [46, 47] controllers are assumed to be static, we consider here general dynamic controllers.

The main contributions are:

- *A general model of NCS.* We propose a general model of NCS, where the plant is a continuous-time nonlinear control system, the computing units are modelled by Moore machines, and the non-idealities introduced by the communication network include quantization errors, time-varying delay in accessing the network, time-varying delay in delivering messages through the network, limited bandwidth and packet dropouts.

- *Symbolic models for NCS.* We propose symbolic models that approximate NCS with arbitrarily good accuracy, by using a novel notion, introduced in this paper, called *strong alternating approximate simulation*. More specifically, under the assumption of existence of an incremental forward complete Lyapunov function for the plant of the NCS, we derive symbolic models approximating the NCS in the sense of strong alternating approximate simulation. Stability of the open-loop NCS is not required. In some recent work [48], symbolic models for NCS are proposed, which, differently from our approach, are constructed on the basis of a symbolic model of the plant.

- *Symbolic control design of NCS.* Building upon the obtained symbolic models, we address the NCS control design problem, where specifications are expressed in terms of transition systems. Given a NCS and a specification, a symbolic controller is derived such that the controlled system meets the specification *in the presence of the considered non-idealities in the communication network*.

The paper is organized as follows. In Section 2 notation is introduced. In

Section 3 a model is proposed for a general class of nonlinear NCS. In Section 4 symbolic models approximating NCS are derived. In Section 5 symbolic control design is addressed. An example of application of the proposed results is included in Section 6. Finally, Section 7 offers some concluding remarks. The Appendix recalls some technical notions that are instrumental in the paper.

## 2 Notation and preliminary definitions

*Notation.* The symbols  $\mathbb{N}$ ,  $\mathbb{N}_0$ ,  $\mathbb{Z}$ ,  $\mathbb{R}$ ,  $\mathbb{R}^-$ ,  $\mathbb{R}^+$  and  $\mathbb{R}_0^+$  denote the set of natural, nonnegative integer, integer, real, negative real, positive real, and nonnegative real numbers, respectively. The cardinality of a set  $A$  is denoted by  $|A|$ . Given a set  $A$  we denote  $A^2 = A \times A$  and  $A^{n+1} = A \times A^n$  for any  $n \in \mathbb{N}$ . Given a pair of sets  $A$  and  $B$  and a relation  $\mathcal{R} \subseteq A \times B$ , the symbol  $\mathcal{R}^{-1}$  denotes the inverse relation of  $\mathcal{R}$ , i.e.  $\mathcal{R}^{-1} = \{(b, a) \in B \times A : (a, b) \in \mathcal{R}\}$ ; for  $A' \subseteq A$  we define  $\mathcal{R}(A') = \{b \in B | \exists a \in A' \text{ s.t. } (a, b) \in \mathcal{R}\}$  and for  $B' \subseteq B$ ,  $\mathcal{R}^{-1}(B') = \{a \in A | \exists b \in B' \text{ s.t. } (a, b) \in \mathcal{R}\}$ . Given sets  $A$ ,  $B$  and  $C$  and relations  $\mathcal{R}_{ab} \subseteq A \times B$  and  $\mathcal{R}_{bc} \subseteq B \times C$  we recall that the composition relation  $\mathcal{R} = \mathcal{R}_{ab} \circ \mathcal{R}_{bc} \subseteq A \times C$  is defined as  $\mathcal{R}_{ab} \circ \mathcal{R}_{bc} := \{(a, c) \in A \times C | \exists b \in B \text{ s.t. } (a, b) \in \mathcal{R}_{ab} \wedge (b, c) \in \mathcal{R}_{bc}\}$ . Note that, for any  $A' \subseteq A$ ,  $\mathcal{R}(A') = \mathcal{R}_{bc}(\mathcal{R}_{ab}(A'))$  and for any  $C' \subseteq C$ ,  $\mathcal{R}^{-1}(C') = \mathcal{R}_{ab}^{-1}(\mathcal{R}_{bc}^{-1}(C'))$ . Given an interval  $[a, b] \subseteq \mathbb{R}_0^+$ , we denote by  $[a; b]$  (resp.  $[a; b[$ ) the set  $[a, b] \cap \mathbb{N}_0$  (resp.  $[a, b[ \cap \mathbb{N}_0$ ), if  $a \leq b$ , and the empty set  $\emptyset$  otherwise. We denote the ceiling of a real number  $x$  by  $\lceil x \rceil = \min\{n \in \mathbb{Z} | n \geq x\}$ . Given a vector  $x \in \mathbb{R}^n$  we denote by  $\|x\|$  the infinity norm and by  $\|x\|_2$  the Euclidean norm of  $x$ . Given any function  $f : D \rightarrow Y$  and any set  $A \subseteq D$ , we denote by  $f(A)$  the image of the set  $A$  through  $f$ , namely  $f(A) = \{y \in Y : y = f(x), x \in A\}$ .

*Preliminary definitions.* A continuous function  $\gamma : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$  is said to belong to class  $\mathcal{K}$  if it is strictly increasing and  $\gamma(0) = 0$ ; a function  $\gamma$  is said to belong to class  $\mathcal{K}_\infty$  if  $\gamma \in \mathcal{K}$  and  $\gamma(r) \rightarrow \infty$  as  $r \rightarrow \infty$ . Given  $\varepsilon \in \mathbb{R}^+$  and  $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ , the symbol  $\mathcal{B}_\varepsilon(x)$  denotes the closed ball of radius  $\varepsilon$  (in infinity norm) centered at  $x$ , i.e.  $\mathcal{B}_\varepsilon(x) = [-\varepsilon + x_1, x_1 + \varepsilon] \times [-\varepsilon + x_2, x_2 + \varepsilon] \times \dots \times [-\varepsilon + x_n, x_n + \varepsilon]$ , while the symbol  $\mathcal{B}_{[\varepsilon]}(x)$  denotes the set  $[x_1, x_1 + \varepsilon[ \times [x_2, x_2 + \varepsilon[ \times \dots \times [x_n, x_n + \varepsilon[$ . Following [49], given any  $\mu \in \mathbb{R}^+$  and any  $x \in \mathbb{R}^n$ , the symbol  $[x]_\mu$  denotes the unique vector in  $\mu\mathbb{Z}^n$  such that  $x \in \mathcal{B}_{[\mu]}([x]_\mu)$ . As a consequence,  $\|x - [x]_\mu\| \leq \mu$ . Given  $\mu \in \mathbb{R}^+$  and  $A \subseteq \mathbb{R}^n$ , we set  $[A]_\mu := \{b \in \mu\mathbb{Z}^n : b = [a]_\mu, a \in A\}$  and  $\mathcal{B}_{[\mu]}(A) = \bigcup_{a \in A} \mathcal{B}_{[\mu]}(a)$ ; if  $B = \bigcup_{i \in [1; N]} A^i$  we set  $[B]_\mu = \bigcup_{i \in [1; N]} ([A]_\mu)^i$ . Consider a set  $A$  given as a finite union of hyperrectangles, i.e.  $A = \bigcup_{j \in [1; J]} A_j$ , for some  $J \in \mathbb{N}$ , where  $A_j = \times_{k \in [1; n]} [\underline{a}_{j,k}, \bar{a}_{j,k}[ \subseteq \mathbb{R}^n$  with  $\underline{a}_{j,k} < \bar{a}_{j,k}$ ,  $\underline{a}_{j,k}, \bar{a}_{j,k} \in \hat{\mu}_A \mathbb{Z}$  for some  $\hat{\mu}_A \in \mathbb{R}^+$ . By construction, for any integer  $n_A \in \mathbb{N}$ , by setting  $\mu = \hat{\mu}_A / n_A$ , we get that for any  $a \in A$ ,  $\|a - [a]_\mu\| \leq \mu$  and  $[a]_\mu \in A$ , implying  $[A]_\mu \subseteq A$ .

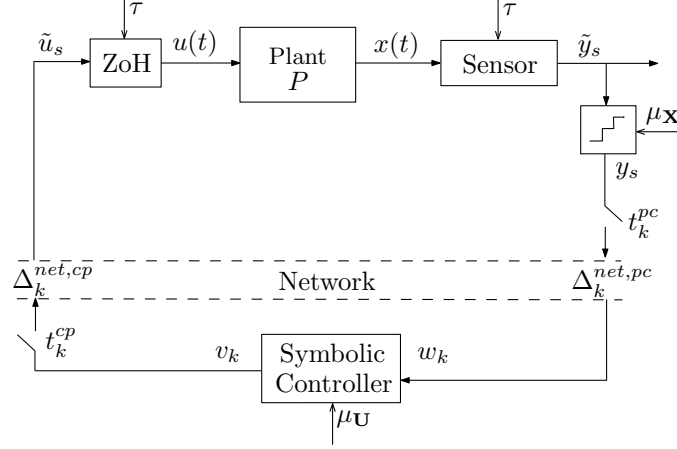


Figure 1: Networked Control System. A detailed description of the sub-systems depicted in this figure is reported in Section III.

### 3 Networked Control Systems and Control Problem

The class of NCS that we consider is depicted in Fig. 1 and is inspired by the models reviewed in [2]. The sub-systems composing the NCS are described hereafter.

**Plant.** The direct branch of the network includes the plant  $P$  that is a nonlinear control system of the form:

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)), \\ x(t) \in \mathbb{R}^n, \quad u(\cdot) \in \mathcal{U}, \quad t \in \mathbb{R}_0^+, \end{cases} \quad (1)$$

where  $x(t)$  and  $u(t)$  are the state and the control input at time  $t$ , and  $\mathcal{U}$  is the set of control inputs, defined as functions from  $\mathbb{R}_0^+$  to a finite non-empty set  $\mathbf{U} \subset [\mathbb{R}^m]_{\mu_U}$ , for some  $\mu_U \in \mathbb{R}^+$ , and constant in any interval  $[s\tau, (s+1)\tau[$  with  $s \in \mathbb{N}_0$  and for some given  $\tau \in \mathbb{R}^+$ , where  $s$  is the index identifying the sampling interval (starting from 0). In the sequel we abuse notation by denoting the constant control input  $u(t) = u$  in the domain  $[s\tau, (s+1)\tau[$  for all  $s \in \mathbb{N}_0$  and for some  $\tau \in \mathbb{R}^+$  by  $u$ . The function  $f : \mathbb{R}^n \times \mathbf{U} \rightarrow \mathbb{R}^n$  is assumed to be Lipschitz on compact sets with respect to the first argument. In the sequel we denote by  $\mathbf{x}(t, x_0, u)$  the state reached by (1) at time  $t$  under the control input  $u$  from the state  $x_0$ . We assume that the control system  $P$  is forward complete in  $\mathbb{R}^n$ , namely that every trajectory  $\mathbf{x}(\cdot, x(0), u)$  of  $P$  is defined on  $[0, \infty[$ . Sufficient and necessary conditions for a control system to be forward complete can be found in [50].

**Sensor.** On the right-hand side of the plant  $P$  in Fig. 1, a sensor is placed. Since the sensor is physically connected to the plant, we assume that:

(A.1) The sensor acts in time-driven fashion, it is synchronized with the plant and updates its output value at times that are integer multiples of  $\tau \in \mathbb{R}^+$ , i.e.  $\tilde{y}_s = \mathbf{x}(s\tau, x(0), u)$ .

**Quantizer.** A quantizer follows the sensor. For simplicity, we assume that the quantizer is *uniform*, with accuracy  $\mu_{\mathbf{x}} \in \mathbb{R}^+$ . The role of the quantizer is: i) to discretize the continuous-valued sensor measurement sequence  $\{\tilde{y}_s\}_{s \in \mathbb{N}_0}$  to get the quantized sequence  $\{y_s\}_{s \in \mathbb{N}_0}$ , with  $y_s = [\tilde{y}_s]_{\mu_{\mathbf{x}}}$ ; ii) to encode the signals into digital messages and to add overhead bits, resulting in the sequence of digital messages  $\{\bar{y}_s\}_{s \in \mathbb{N}_0}$ . The transmission overhead takes into account the communication protocol, the packet headers, source and channel coding as well as data compression and encryption. We assume a fixed average relative overhead  $N_{\text{pc}}^+ \in ]-1, +\infty[$  on each data bit ( $N_{\text{pc}}^+$  may be negative to include the case of data compression). More precisely:

(A.2)  $N_{\text{pc}}^+$  bits are added per each bit of the digital signal encoding  $y_s$ , for all  $s \in \mathbb{N}_0$ .

**Network.** In the following, the index  $k \in \mathbb{N}$  denotes the current iteration in the feedback loop. Due to the non-idealities of the network, not all the output samples can be transmitted through the network. We assume that only one output sample per iteration is sent. In particular,  $\{M_k\}_{k \in \mathbb{N}} \subseteq \mathbb{N}_0$  denotes the subsequence of the sampling intervals when the output samples are sent through the network, i.e. at time  $M_k\tau$  the digital message  $\bar{y}_{M_k}$  encodes the output sample  $y_{M_k} = [x(M_k\tau)]_{\mu_{\mathbf{x}}}$  and is sent (iteration  $k$ ). We set  $M_1 = 0$ . The communication network is characterized by the following features:

*Time-varying access to the network.* The digital message  $\bar{y}_{M_k}$  cannot be sent instantaneously to the network, because the communication channel is assumed to be a resource which is shared with other nodes or processes in the network. The policy by which a signal of a node is sent before or after a message of another node is managed by the network scheduling protocol selected. We assume that:

(A.3) The network waiting times  $\Delta_k^{\text{req,pc}}$  in the plant-to-controller branch of the feedback loop are bounded, i.e.  $\Delta_k^{\text{req,pc}} \in [\Delta_{\min}^{\text{req}}, \Delta_{\max}^{\text{req}}]$ , for some  $\Delta_{\min}^{\text{req}}, \Delta_{\max}^{\text{req}} \in \mathbb{R}_0^+$ .

At time  $t_k^{\text{pc}} := M_k\tau + \Delta_k^{\text{req,pc}}$ , the message  $\bar{w}_k := \bar{y}_{M_k}$  is sent through the network.

*Limited bandwidth.* In real applications, the capacity of the digital communication channel is limited and time-varying. We denote by  $B_{\min}, B_{\max} \in \mathbb{R}^+$ ,

with  $B_{\min} \leq B_{\max}$ , the minimum and maximum capacities of the channel (expressed in bits per second, bps). In view of the binary coding and the transmission overhead (see Assumption (A.2)), we assume that:

(A.4) A delay  $\Delta_k^{B,pc} \in \mathbb{R}^+$ , due to the limited bandwidth, is introduced in the plant-to-controller branch of the feedback loop, for all  $k \in \mathbb{N}$ .

*Time-varying delivery of messages.* The delivery of message  $\bar{w}_k$  may be subject to further delays, due to congestion phenomena in the network, etc. We assume that:

(A.5) Network communication delays  $\Delta_k^{\text{net},pc}$  in the plant-to-controller branch of the feedback loop are bounded, i.e.  $\Delta_k^{\text{net},pc} \in [\Delta_{\min}^{\text{net}}, \Delta_{\max}^{\text{net}}]$ , for some  $\Delta_{\min}^{\text{net}}, \Delta_{\max}^{\text{net}} \in \mathbb{R}_0^+$ .

*Packet dropout.* In real applications, one or more messages can be lost during the transmission, because of the unreliability of the communication channel. We assume that:

(A.6) The maximum number of successive packet dropouts is  $N_{pd}$ .

**Symbolic Controller.** After a finite number of possible retransmissions (see Assumption (A.6)), message  $\bar{w}_k$  is decoded into the quantized sensor measurement  $w_k$  and reaches the controller. The symbolic controller  $C$  is dynamic, non-deterministic, remote and asynchronous with respect to the plant and is expressed as a Moore machine:

$$C : \begin{cases} \xi_k \in f_C(\xi_{k-1}, w_k), & \xi_k \in \Xi_C, k \in \mathbb{N} \setminus \{1\}, \\ v_k = h_C(\xi_k), & v_k \in \mathbf{U}, k \in \mathbb{N}, \\ \xi_1 \in \Xi_C^0, \end{cases} \quad (2)$$

where  $\Xi_C$  is the finite set of states of the controller,  $\Xi_C^0 \subseteq \Xi_C$  is the set of initial states of the controller,  $f_C$  is a possibly partial function  $f_C : \Xi_C \times [\mathbb{R}^n]_{\mu_{\mathbf{x}}} \rightarrow 2^{\Xi_C}$  and  $h_C : \Xi_C \rightarrow \mathbf{U}$ . At each iteration  $k$ , the controller takes as input the measurement sample  $w_k \in [\mathbb{R}^n]_{\mu_{\mathbf{x}}}$ , updates its internal state to  $\xi_k$  and returns the control sample  $v_k = h_C(\xi_k) \in \mathbf{U}$  as output, which is synthesized by a computing unit that may be employed to execute several tasks. Note that, when  $\Xi_C$  is a singleton set,  $C$  becomes static. The policy by which a computation is executed before or after another computation depends on the scheduling protocol adopted. We assume that:

(A.7) The computation time  $\Delta_k^{\text{ctrl}}$  for the symbolic controller to return its output value  $v_k$  is bounded, i.e.  $\Delta_k^{\text{ctrl}} \in [\Delta_{\min}^{\text{ctrl}}, \Delta_{\max}^{\text{ctrl}}]$ , for some  $\Delta_{\min}^{\text{ctrl}}, \Delta_{\max}^{\text{ctrl}} \in \mathbb{R}_0^+$ .

The control sample  $v_k$  is encoded into a digital signal and some overhead information is added to take into account the communication protocol, the packet

headers, source and channel coding as well as data compression and encryption. The resulting message is denoted by  $\bar{v}_k$ . We assume a fixed average relative overhead  $N_{\text{cp}}^+$  on each data bit, which may also be negative due to possible data compression. The following Assumptions (A.8) to (A.11), describing the non-idealities in the controller-to-plant branch of the network, correspond exactly to Assumptions (A.2) to (A.5), previously given for the plant-to-controller branch:

(A.8)  $N_{\text{cp}}^+ \in ]-1, +\infty[$  bits are added per each bit of  $v_k$ .

(A.9) Network waiting times  $\Delta_k^{\text{req},\text{cp}}$  in the controller-to-plant branch of the feedback loop are bounded, i.e.  $\Delta_k^{\text{req},\text{pc}} \in [\Delta_{\min}^{\text{req}}, \Delta_{\max}^{\text{req}}]$ .

At time  $t_k^{\text{cp}} := M_k\tau + \Delta_k^{\text{req},\text{pc}} + \Delta_k^{B,\text{pc}} + \Delta_k^{\text{net},\text{pc}} + \Delta_k^{\text{ctrl}} + \Delta_k^{\text{req},\text{cp}}$ , the message  $\bar{v}_k$  is sent.

(A.10) A delay  $\Delta_k^{B,\text{cp}} \in \mathbb{R}^+$ , due to the limited bandwidth, is introduced in the controller-to-plant branch of the feedback loop.

(A.11) Network communication delays  $\Delta_k^{\text{net},\text{cp}}$  in the controller-to-plant branch of the feedback loop are bounded, i.e.  $\Delta_k^{\text{net},\text{cp}} \in [\Delta_{\min}^{\text{net}}, \Delta_{\max}^{\text{net}}]$ .

We denote by

$$\Delta_k := \Delta_k^{\text{req},\text{pc}} + \Delta_k^{B,\text{pc}} + \Delta_k^{\text{net},\text{pc}} + \Delta_k^{\text{ctrl}} + \Delta_k^{\text{req},\text{cp}} + \Delta_k^{B,\text{cp}} + \Delta_k^{\text{net},\text{cp}}$$

the total delay induced by network and computing unit at iteration  $k$ , as a result of the assumptions above. We can finally define

$$N_k := \lceil \Delta_k / \tau \rceil \in \mathbb{N} \quad (3)$$

as the *discrete delay* induced by iteration  $k$ , expressed in terms of number of sampling intervals of duration  $\tau$ . From the definitions of  $M_k$  and  $N_k$ , we get  $M_{k+1} = M_k + N_k$ .

**ZoH.** After a finite number of possible retransmissions (see Assumption (A.6)), message  $\bar{v}_k$  is decoded into the control input  $v_k$  and reaches the Zero-order-Holder (ZoH), placed on the left-hand side of the plant  $P$  in Fig. 1. We assume that:

(A.12) The ZoH is updated at time  $M_{k+1}\tau$  to the new value  $v_k$ , which is held exactly for one iteration, until a new control sample shows up, i.e.  $u(t) = v_{k-1}$ ,  $t \in [M_k\tau, M_{k+1}\tau[$ . At time  $t = 0$  a reference control input  $v_0 := \bar{u}_0 \in \mathbf{U}$  is held by the ZoH.

In the sequel we refer to the NCS model as  $\Sigma$ , which is also formally described in (4). A trajectory of  $\Sigma$  is a function  $x : \mathbb{R}_0^+ \rightarrow \mathbb{R}^n$  satisfying (4). Due to possible different realizations of the non-idealities and the non-deterministic



$$\Sigma : \left\{ \begin{array}{ll} \text{Iteration delay:} & N_k = \lceil \frac{\Delta_k}{\tau} \rceil, \Delta_k \in \mathbb{R}^+, k \in \mathbb{N}, \\ \text{Sampling/holding time sequence:} & \begin{cases} M_{k+1} = M_k + N_k, k \in \mathbb{N}, \\ M_1 = 0, \end{cases} \\ \text{ZoH:} & \begin{cases} u(t) = \sum_{k=1}^{\infty} v_{k-1} \mathbf{1}_{[M_k \tau, M_{k+1} \tau)}(t), t \in \mathbb{R}_0^+, \\ v_0 = \tilde{u}_0 \text{ given,} \end{cases} \\ \text{Plant:} & \begin{cases} \dot{x}(t) = f(x(t), u(t)), \\ x(t) \in \mathbb{R}^n, \quad u(\cdot) \in \mathcal{U}, \quad t \in \mathbb{R}_0^+, \end{cases} \\ \text{Sensor:} & \tilde{y}_s = \mathbf{x}(s\tau, x(0), u) \in \mathbb{R}^n, s \in \mathbb{N}_0, \\ \text{Quantizer:} & y_s = [\tilde{y}_s]_{\mu_{\mathbf{x}}}, s \in \mathbb{N}_0, \\ \text{Switch:} & w_k = y_s, s = M_k, k \in \mathbb{N}, \\ \text{Controller:} & \begin{cases} \xi_k \in f_C(\xi_{k-1}, w_k), & \xi_k \in \Xi_C, k \in \mathbb{N} \setminus \{1\}, \\ v_k = h_C(\xi_k), & v_k \in \mathbf{U}, k \in \mathbb{N}, \\ \xi_1 \in \Xi_C^0. \end{cases} \end{array} \right. \quad (4)$$

controller, the NCS  $\Sigma$  is non-deterministic. Note that the definition of NCS given in this section allows taking into account different scheduling protocols and communication constraints: any protocol or set of protocols satisfying Assumptions (A.2–A.5), (A.6) and (A.8–A.11), such as Controller Area Network (CAN) [51] and Time Triggered Protocol (TTP) [52] used in vehicular and industrial applications, can be used.

We conclude this section by introducing the control problem that we address in this paper. We consider a control design problem where the NCS  $\Sigma$  has to satisfy a specification  $Q$ , given in terms of a non-deterministic transition system, up to a desired accuracy  $\varepsilon$ , while being robust with respect to the non-idealities of the communication network. More formally:

**Problem 1** *Consider a specification  $Q$  expressed in terms of a finite collection of transitions  $T_Q \subseteq X_Q \times X_Q$ , with  $X_Q \subseteq \mathbb{R}^n$ , and let  $X_Q^0 \subseteq X_Q$  be a set of initial states. For any desired accuracy  $\varepsilon \in \mathbb{R}^+$ , find a quantization parameter  $\mu_{\mathbf{x}} \in \mathbb{R}^+$ , a set of initial states  $\mathbf{X}_0$  of the plant and a symbolic controller  $C$  in the form of (2) such that, for any sequence  $\{\tilde{y}_s\}_{s \in \mathbb{N}_0}$  generated by the NCS  $\Sigma$  in (4) with  $\tilde{y}_0 \in \mathbf{X}_0$ , there exists a sequence  $\{x_Q^s\}_{s \in \mathbb{N}_0}$  with  $x_Q^0 \in X_Q^0$  such that, for any discrete-time  $s \in \mathbb{N}_0$ , the following conditions hold:*

- 1)  $(x_Q^s, x_Q^{s+1}) \in T_Q$ ;
- 2)  $\|\tilde{y}_s - x_Q^s\| \leq \varepsilon$ .

## 4 Symbolic Models for NCS

In this section we propose symbolic models that approximate NCS with arbitrarily good accuracy, which is instrumental to give in Section 5 the solution to Problem 1.

We start by providing tighter bounds on the delay defined in Section 3, depending on the particular specification considered. Consider a set  $\mathbf{X}$ , with  $\mathcal{B}_\varepsilon(X_Q) \subseteq \mathbf{X} \subseteq \mathbb{R}^n$ , given as a finite union of hyperrectangles  $\mathbf{X} = \bigcup_{j \in [1;J]} \mathbf{X}_j$ , for some  $J \in \mathbb{N}$ , each in the form  $\mathbf{X}_j = \times_{k \in [1;n]} [\underline{x}_{j,k}, \bar{x}_{j,k}[$ , with  $\underline{x}_{j,k} < \bar{x}_{j,k}$ ,  $\underline{x}_{j,k}, \bar{x}_{j,k} \in \hat{\mu}_{\mathbf{X}} \mathbb{Z}$  for some  $\hat{\mu}_{\mathbf{X}} \in \mathbb{R}^+$ . The property  $\mathcal{B}_\varepsilon(X_Q) \subseteq \mathbf{X}$  and condition 2) in Problem 1 imply that, if a controller  $C$  in the form (2) solves Problem 1, then the corresponding sensor measurements  $\tilde{y}_s$  belong to the bounded set  $\mathbf{X}$  for all  $s \in \mathbb{N}_0$ . As a consequence, it is possible to provide an upper-bound on the length of the digital messages encoding sensor measurements and, in turn, some uniform bounds on the delay  $\Delta_k$  induced by each network iteration. In particular:

- Assumption A.2) implies that the number of bits of message  $\tilde{y}_s$  is bounded by  $\lceil (1 + N_{\text{pc}}^+) \lceil \log_2 \|\mathbf{X}\|_{\mu_{\mathbf{X}}} \rceil \rceil$ , for all  $s \in \mathbb{N}_0$ ;
- from Assumption A.4), one has  $\Delta_k^{B,\text{pc}} \in [\Delta_{\min}^{B,\text{pc}}, \Delta_{\max}^{B,\text{pc}}]$ , with  $\Delta_{\min}^{B,\text{pc}} = \lceil (1 + N_{\text{pc}}^+) \lceil \log_2 \|\mathbf{X}\|_{\mu_{\mathbf{X}}} \rceil \rceil / B_{\max}$  and  $\Delta_{\max}^{B,\text{pc}} = \lceil (1 + N_{\text{pc}}^+) \lceil \log_2 \|\mathbf{X}\|_{\mu_{\mathbf{X}}} \rceil \rceil / B_{\min}$ ;
- Assumption (A.8) implies that the number of bits of  $\tilde{v}_k$  is bounded by  $\lceil (1 + N_{\text{cp}}^+) \lceil \log_2 \|\mathbf{U}\| \rceil \rceil$ ;
- from Assumption (A.10), one has  $\Delta_k^{B,\text{cp}} \in [\Delta_{\min}^{B,\text{cp}}, \Delta_{\max}^{B,\text{cp}}]$ , with  $\Delta_{\min}^{B,\text{cp}} = \lceil (1 + N_{\text{cp}}^+) \lceil \log_2 \|\mathbf{U}\| \rceil \rceil / B_{\max}$  and  $\Delta_{\max}^{B,\text{cp}} = \lceil (1 + N_{\text{cp}}^+) \lceil \log_2 \|\mathbf{U}\| \rceil \rceil / B_{\min}$ .

In the absence of packet dropouts, one has  $\Delta_k \in [\bar{\Delta}_{\min}, \bar{\Delta}_{\max}]$ , where  $\bar{\Delta}_{\min}, \bar{\Delta}_{\max} \in \mathbb{R}^+$  are the minimum and maximum delays computed according to the given assumptions (excluding (A.6)), as

$$\begin{aligned} \bar{\Delta}_{\min} &:= \Delta_{\min}^{B,\text{pc}} + \Delta_{\min}^{\text{ctrl}} + \Delta_{\min}^{B,\text{cp}} + 2\Delta_{\min}^{\text{req}} + 2\Delta_{\min}^{\text{net}}, \\ \bar{\Delta}_{\max} &:= \Delta_{\max}^{B,\text{pc}} + \Delta_{\max}^{\text{ctrl}} + \Delta_{\max}^{B,\text{cp}} + 2\Delta_{\max}^{\text{req}} + 2\Delta_{\max}^{\text{net}}. \end{aligned}$$

In presence of packet dropouts, under Assumption (A.6) and following the so-called *emulation approach*, reformulating them in terms of additional delays, see e.g. [2], it is readily seen that iteration  $k$  introduces a time-varying delay  $\Delta_k \in [\Delta_{\min}, \Delta_{\max}]$  in (4), with  $\Delta_{\min} = \bar{\Delta}_{\min}$  and  $\Delta_{\max} = (1 + N_{\text{pd}}) \bar{\Delta}_{\max}$ , where  $N_{\text{pd}}$  is the maximum number of subsequent packet dropouts. Consequently, discrete delays  $N_k$  in (3) will be bounded as follows:

$$N_k \in [N_{\min}; N_{\max}] \quad \forall k \in \mathbb{N}, \quad (5)$$

with bounds given by:

$$N_{\min} = \lceil \Delta_{\min} / \tau \rceil \in \mathbb{N}, \quad N_{\max} = \lceil \Delta_{\max} / \tau \rceil \in \mathbb{N}. \quad (6)$$

We are now ready to use the notion of system as a unified mathematical framework to describe NCS.

$$\Sigma_d : \left\{ \begin{array}{l} \bar{\Sigma}_d : \left\{ \begin{array}{l} \text{Iteration delay:} \quad N_k \in \mathbb{N}, k \in \mathbb{N}, \\ \text{Sampling/holding time sequence:} \quad \begin{cases} M_{k+1} = M_k + N_k, k \in \mathbb{N}, \\ M_1 = 0, \\ z_{s+1} = \bar{f}(z_s, v_{k-1}) = \mathbf{x}(\tau, z_s, v_{k-1}) \in \mathbb{R}^n, s \in [M_k; M_{k+1}[, k \in \mathbb{N}, \\ \tilde{y}_s = z_s, s \in \mathbb{N}_0, \\ z_0 = x(0), \quad v_0 = \tilde{u}_0 \quad \text{given,} \end{cases} \\ \text{Sampled-data control system } P_d: \end{array} \right. \\ \text{Quantizer:} \quad y_s = [\tilde{y}_s]_{\mu_{\mathbf{x}}}, s \in \mathbb{N}_0, \\ \text{Switch:} \quad w_k = y_s, s = M_k, k \in \mathbb{N}, \\ \text{Controller:} \quad \begin{cases} \xi_k \in f_C(\xi_{k-1}, w_k), & \xi_k \in \Xi_C, k \in \mathbb{N} \setminus \{1\}, \\ v_k = h_C(\xi_k), & v_k \in \mathbf{U}, k \in \mathbb{N}, \\ \xi_1 \in \Xi_C^0. \end{cases} \end{array} \right. \quad (7)$$


---

**Definition 1** [21] *A system is a sextuple*

$$S = (X, X_0, U, \longrightarrow, Y, H)$$

consisting of a set of states  $X$ , a set of initial states  $X_0 \subseteq X$ , a set of inputs  $U$ , a transition relation  $\longrightarrow \subseteq X \times U \times X$ , a set of outputs  $Y$  and an output function  $H : X \rightarrow Y$ . A transition  $(x, u, x') \in \longrightarrow$  of  $S$  is denoted by  $x \xrightarrow{u} x'$ . For such a transition, state  $x'$  is called a  $u$ -successor or simply a successor of state  $x$ . We denote by  $\text{Post}_u(x)$  the set of  $u$ -successors of a state  $x$  and by  $U(x)$  the set of inputs  $u \in U$  for which  $\text{Post}_u(x)$  is nonempty.

System  $S$  is said to be *symbolic* (or *finite*), if  $X$  and  $U$  are finite sets, *(pseudo)metric*, if the output set  $Y$  is equipped with a (pseudo)metric  $d : Y \times Y \rightarrow \mathbb{R}_0^+$ , *deterministic*, if for any  $x \in X$  and  $u \in U$  there exists at most one state  $x' \in X$  such that  $x \xrightarrow{u} x'$ , *non-blocking*, if  $U(x) \neq \emptyset$  for any  $x \in X$ . The evolution of systems is captured by the notions of state and output runs. A state run of  $S$  is a possibly infinite sequence  $\{x_i\}$  such that  $x_0 \in X_0$  and, for any  $i$ , there exists  $u_i \in U$  for which  $x_i \xrightarrow{u_i} x_{i+1}$ . An output run is a possibly infinite sequence  $\{y_i\}$  such that there exists a state run  $\{x_i\}$  with  $y_i = H(x_i)$  for any  $i$ . In order to give a representation of NCS in terms of systems, we first need to provide an equivalent formulation of NCS. Given the NCS  $\Sigma$ , consider the NCS  $\Sigma_d$  depicted in Fig. 2 and with evolution formally specified by equations (7). In equations (7), we replace the interconnected blocks ZoH, Plant and Sensor of (4) by the nonlinear *sampled-data control system*  $P_d$ , where

$$\bar{f}(x, u) := \mathbf{x}(\tau, x, u),$$

for any  $x \in \mathbb{R}^n$  and  $u \in \mathbf{U}$ , which is the time discretization of the plant  $P$  with sampling time  $\tau$ . A sequence  $\{z_s\}_{s \in \mathbb{N}_0}$  satisfying (7) for some sequence  $\{v_k\}_{k \in \mathbb{N}_0}$  is called a *trajectory* of  $\Sigma_d$ . We stress that control sample  $v_{k-1}$ , designed at



- $x^1 = (x_1^1, \dots, x_{N_1}^1, \bar{u}^1) \xrightarrow[\tau]{u} x^2 = (x_1^2, \dots, x_{N_2}^2, \bar{u}^2)$ , if  $\bar{u}^2 = u$ ,  $x_1^2 = \bar{f}(x_{N_1}^1, \bar{u}^1)$  and  $x_{i+1}^2 = \bar{f}(x_i^2, \bar{u}^1)$  for  $i \in [1; N_2 - 1]$ ,  $N_1, N_2 \in [N_{\min}; N_{\max}]$ ;
- $Y_\tau = \mathbb{R}^n \cup (\bigcup_{N \in [N_{\min}; N_{\max}]} \mathbb{R}^{nN})$ ;
- $H_\tau(x_0, \tilde{u}_0) = x_0$  for all  $x_0 \in \mathbb{R}^n$ ;
- $H_\tau(x_1, x_2, \dots, x_N, \bar{u}) = (x_1, x_2, \dots, x_N)$ , for all  $(x_1, x_2, \dots, x_N, \bar{u}) \in X_\tau$ ,  $N \in [N_{\min}; N_{\max}]$ .

Note that  $S(\bar{\Sigma}_d)$  is non-deterministic because, depending on the values of  $N_2$  in the transition relation, multiple  $u$ -successors of  $x^1$  exist. System  $S(\bar{\Sigma}_d)$  can be regarded as a pseudometric system with the pseudometric  $d_{Y_\tau}$  on  $Y_\tau$  naturally induced by the metric  $d(x_1, x_2) = \|x_1 - x_2\|$  on  $\mathbb{R}^n$ , as follows. Given any  $x^i = (x_1^i, x_2^i, \dots, x_{N_i}^i, \bar{u}^i)$ ,  $i = 1, 2$ , we set

$$d_{Y_\tau}(H_\tau(x^1), H_\tau(x^2)) = \begin{cases} \max_{i \in [1; N_1]} \|x_i^1 - x_i^2\|, & \text{if } N_1 = N_2; \\ +\infty, & \text{otherwise.} \end{cases}$$

Since the state vectors of  $S(\bar{\Sigma}_d)$  are built from the trajectories of  $P_d$  in  $\bar{\Sigma}_d$ , it is readily seen that:

**Proposition 2** *For any trajectory  $\{z_s\}_{s \in \mathbb{N}_0}$  of  $\Sigma_d$ , with  $N_k$  satisfying (5), there exists a state run*

$$\underbrace{(x(0), \tilde{u}_0)}_{x^0} \xrightarrow{\tilde{u}_1} \underbrace{(\bar{x}^1, \tilde{u}_1)}_{x^1} \xrightarrow{\tilde{u}_2} \underbrace{(\bar{x}^2, \tilde{u}_2)}_{x^2} \xrightarrow{\tilde{u}_3} \dots \quad (8)$$

of  $S(\bar{\Sigma}_d)$  such that:

$$\{x(0) \quad , \quad \underbrace{\bar{x}_1^1, \dots, \bar{x}_{N_1}^1}_{\bar{x}^1} \quad , \quad \underbrace{\bar{x}_1^2, \dots, \bar{x}_{N_2}^2}_{\bar{x}^2} \quad , \quad \dots\} = \{z_s\}_{s \in \mathbb{N}_0}. \quad (9)$$

Conversely, for any state run (8) of  $S(\bar{\Sigma}_d)$ , there exists a trajectory  $\{z_s\}_{s \in \mathbb{N}_0}$  of  $\Sigma_d$  such that (9) holds.

Although system  $S(\bar{\Sigma}_d)$  contains all the information of the NCS available at the sensor, it is not a finite model. Hereafter, we illustrate the construction of symbolic models that approximate possibly unstable NCS in the sense of strong alternating approximate simulation, whose definition is formally introduced in the Appendix. Our results rely on the assumption of existence of an incremental forward complete ( $\delta$ -FC) Lyapunov function for the plant of the NCS. More formally:

**Definition 3** [23] *A continuously differentiable function  $V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+$  is a  $\delta$ -FC Lyapunov function for the plant control system of the NCS if there exist a real number  $\lambda \in \mathbb{R}$  and  $\mathcal{K}_\infty$  functions  $\underline{\alpha}$  and  $\bar{\alpha}$  such that, for any  $x_1, x_2 \in \mathbb{R}^n$  and any  $u \in \mathbf{U}$ , the following conditions hold:*

- (i)  $\underline{\alpha}(\|x_1 - x_2\|) \leq V(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|)$ ,
- (ii)  $\frac{\partial V}{\partial x_1}(x_1, x_2) f(x_1, u) + \frac{\partial V}{\partial x_2}(x_1, x_2) f(x_2, u) \leq \lambda V(x_1, x_2)$ .

We refer the interested reader to [23] for further details on this notion. In the following, we suppose the existence of a  $\delta$ -FC Lyapunov function  $V$  for the control system  $P$  in the NCS  $\Sigma$  and of a  $\mathcal{K}_\infty$  function  $\gamma$  such that  $V(x, x') - V(x, x'') \leq \gamma(\|x' - x''\|)$ , for every  $x, x', x'' \in \mathbb{R}^n$ . We assume without loss of generality that  $V$  is symmetric, i.e.  $V(x_1, x_2) = V(x_2, x_1)$  for all  $x_1, x_2 \in \mathbb{R}^n$ .

**Definition 4** Given  $\bar{\Sigma}_d$  in (7), with  $N_k$  satisfying (5), define the system

$$S_*(\bar{\Sigma}_d) := (X_*, X_{0,*}, \mathbf{U}, \xrightarrow{*}, Y_*, H_*),$$

where

- $X_* = ([\mathbb{R}^n]_{\mu_{\mathbf{X}}} \times \{\tilde{u}_0\}) \cup \{(x_1^*, x_2^*, \dots, x_N^*, \bar{u}_*) \in [\mathbb{R}^{nN}]_{\mu_{\mathbf{X}}} \times \mathbf{U} : \exists \underline{u}_* \in \mathbf{U} \text{ s.t. } V([\bar{f}(x_i^*, \underline{u}_*)]_{\mu_{\mathbf{X}}}, x_{i+1}^*) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}), \forall i \in [1; N-1], N \in [N_{\min}; N_{\max}]\}$ ;
- $X_{0,*} = [\mathbb{R}^n]_{\mu_{\mathbf{X}}} \times \{\tilde{u}_0\}$ ,
- $x^1 = (x_0, \tilde{u}_0) \xrightarrow{*} x^2 = (x_1^2, \dots, x_{N_2}^2, \bar{u}_*^2)$ , if  $x^1 \in X_{0,*}$ ,  $\bar{u}_*^2 = u_*$ ,  $N_2 \in [N_{\min}; N_{\max}]$ , and

$$\begin{cases} V([\bar{f}(x_0, \tilde{u}_0)]_{\mu_{\mathbf{X}}}, x_1^2) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}), \\ V([\bar{f}(x_i^2, \tilde{u}_0)]_{\mu_{\mathbf{X}}}, x_{i+1}^2) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}), i \in [1; N_2 - 1]; \end{cases} \quad (10)$$

- $x^1 = (x_1^1, \dots, x_{N_1}^1, \bar{u}_*^1) \xrightarrow{*} x^2 = (x_1^2, \dots, x_{N_2}^2, \bar{u}_*^2)$ , if  $\bar{u}_*^2 = u_*$ ,  $N_1, N_2 \in [N_{\min}; N_{\max}]$ , and

$$\begin{cases} V([\bar{f}(x_{N_1}^1, \bar{u}_*^1)]_{\mu_{\mathbf{X}}}, x_1^2) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}), \\ V([\bar{f}(x_i^2, \bar{u}_*^1)]_{\mu_{\mathbf{X}}}, x_{i+1}^2) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}), i \in [1; N_2 - 1]; \end{cases} \quad (11)$$

- $Y_* = Y_\tau$ ;
- $H_*(x_0, \tilde{u}_0) = x_0$  for all  $x_0 \in [\mathbb{R}^n]_{\mu_{\mathbf{X}}}$ ;
- $H_*(x_1^*, x_2^*, \dots, x_N^*, \bar{u}_*) = (x_1^*, x_2^*, \dots, x_N^*)$ , for all  $(x_1^*, x_2^*, \dots, x_N^*, \bar{u}_*) \in X_*$ ,  $N \in [N_{\min}; N_{\max}]$ .

System  $S_*(\bar{\Sigma}_d)$  is pseudometric when  $Y_*$  is equipped with the pseudometric  $d_{Y_\tau}$ . We can now present the following result.

**Theorem 1** Consider  $\bar{\Sigma}_d$  in (7), with  $N_k$  satisfying (5), and suppose that there exists a  $\delta$ -FC Lyapunov function  $V$  for the control system  $P$  in the NCS  $\Sigma$ . Then,  $S_*(\bar{\Sigma}_d) \preceq_\varepsilon^{s, \text{alt}} S(\bar{\Sigma}_d)$  for any desired accuracy  $\varepsilon \in \mathbb{R}^+$  and any state quantization  $\mu_{\mathbf{X}} \in \mathbb{R}^+$  satisfying

$$\mu_{\mathbf{X}} = \hat{\mu}_{\mathbf{X}}/n_{\mathbf{X}} \leq \varepsilon, \quad (12)$$

for some integer  $n_{\mathbf{X}}$ .

**Proof 1** Consider the relation  $\mathcal{R} \subseteq X_* \times X_\tau$  defined by  $(x^*, x) \in \mathcal{R}$  if and only if  $x^* = (x_1^*, x_2^*, \dots, x_N^*, \bar{u}_*)$ ,  $x = (x_1, x_2, \dots, x_N, \bar{u})$ , for some  $N$ ,  $x_i^* = [x_i]_{\mu_{\mathbf{X}}}$ , for all  $i \in [1; N]$ , and  $\bar{u}_* = \bar{u}$ . We first prove condition (i) of Definition 6 in the Appendix. By definition of  $[\mathbb{R}^n]_{\mu_{\mathbf{X}}}$ , for any  $x^* = (x_0^*, \tilde{u}_0) \in X_{0,*}$ , there exists  $x = (x_0, \tilde{u}_0) \in X_{0,\tau}$  with  $x_0^* = [x_0]_{\mu_{\mathbf{X}}}$ . We now consider condition (ii) of Definition 6. For any  $(x^*, x) \in \mathcal{R}$ , from the definition of the pseudometric  $d_{Y_\tau}$ , the definition of  $\mathcal{R}$  and condition (12) we get  $d_{Y_\tau}(H_*(x^*), H_\tau(x)) = \max_i \|x_i^* - x_i\| \leq \mu_{\mathbf{X}} \leq \varepsilon$ . We now show condition (iii''). Consider any  $(x^*, x) \in \mathcal{R}$ , with  $x^* = (x_1^*, x_2^*, \dots, x_N^*, \bar{u}_*)$  and  $x = (x_1, x_2, \dots, x_N, \bar{u})$ ; then pick any  $u = u_* \in \mathbf{U}$  and consider any transition  $x \xrightarrow[\tau]{u} \bar{x}$ , with  $\bar{x} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{\bar{N}}, u)$ , for some  $\bar{N}$ . Pick  $\bar{x}^* = (\bar{x}_1^*, \bar{x}_2^*, \dots, \bar{x}_{\bar{N}}^*, u_*)$  defined by  $\bar{x}_i^* = [\bar{x}_i]_{\mu_{\mathbf{X}}}$  for all  $i \in [1; \bar{N}]$ . By definition of  $\bar{x}^*$  we get  $(\bar{x}^*, \bar{x}) \in \mathcal{R}$ . We conclude the proof by showing that  $x^* \xrightarrow[\ast]{u_*} \bar{x}^*$ , i.e. it is a transition of  $S_*(\bar{\Sigma}_d)$ . By using condition (ii) in Definition 3, one has  $\frac{\partial V}{\partial x_N^*}(x_N^*, x_N)f(x_N^*, \bar{u}_*) + \frac{\partial V}{\partial x_N}(x_N^*, x_N)f(x_N, \bar{u}) \leq \lambda V(x_N^*, x_N)$ . By the definitions of  $\gamma$ ,  $\mathcal{R}$  and  $S(\bar{\Sigma}_d)$ , and by integrating the previous inequality, the following holds:

$$\begin{aligned}
V([\bar{f}(x_N^*, \bar{u}_*)]_{\mu_{\mathbf{X}}}, \bar{x}_1^*) &\leq V(\bar{f}(x_N^*, \bar{u}_*), \bar{x}_1^*) + \gamma(\mu_{\mathbf{X}}) \\
&\leq V(\bar{f}(x_N^*, \bar{u}_*), \bar{x}_1) + 2\gamma(\mu_{\mathbf{X}}) \\
&\leq e^{\lambda\tau} V(x_N^*, x_N) + 2\gamma(\mu_{\mathbf{X}}) \\
&\leq e^{\lambda\tau} (V(x_N^*, [x_N]_{\mu_{\mathbf{X}}}) + \gamma(\mu_{\mathbf{X}})) + 2\gamma(\mu_{\mathbf{X}}) \\
&= (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}}),
\end{aligned} \tag{13}$$

where the last equality holds by condition (i) of Definition 3. By similar computations, it is possible to prove that  $V([\bar{f}(\bar{x}_i^*, \bar{u}_*)]_{\mu_{\mathbf{X}}}, \bar{x}_{i+1}^*) \leq (e^{\lambda\tau} + 2)\gamma(\mu_{\mathbf{X}})$ ,  $i \in [1; \bar{N} - 1]$ . Hence, from the inequality above, from (13) and from the definition of the transition relation of  $S_*(\bar{\Sigma}_d)$  in (11), we get  $x^* \xrightarrow[\ast]{u_*} \bar{x}^*$ .

## 5 NCS Symbolic Control Design

In this section we provide the solution to Problem 1, which is based on the use of the symbolic models proposed in the previous section. We first design a symbolic controller system  $S_{C^*}$  that solves an appropriate approximate similarity game associated with Problem 1. We then refine the controller system  $S_{C^*}$  to a controller  $C^*$  in the form of (2) which solves Problem 1.

We start by reformulating the specification  $Q$  in Problem 1 in terms of the following system:

$$S(Q) = (X_q, X_Q^0, U_q, \xrightarrow{q}, Y_q, H_q), \tag{14}$$

where

- $X_q = X_Q^0 \cup \{x = (x_1, x_2, \dots, x_N) \in X_Q^N, N \in [N_{\min}; N_{\max}] | (x_i, x_{i+1}) \in T_Q, i \in [1; N - 1]\}$ ;

- $U_q = \{u_q\}$ , where  $u_q$  is a dummy symbol;
- $x^1 \xrightarrow[q]{u_q} x^2$ , if  $x^1 = (x_1^1, \dots, x_{N_1}^1)$ ,  $x^2 = (x_1^2, \dots, x_{N_2}^2)$  and  $x_{N_1}^1 \xrightarrow{Q} x_1^2$ ;
- $Y_q = Y_\tau$ ;
- $H_q(x) = x$ , for all  $x \in X_q$ .

We now consider the following symbolic control problem:

**Problem 2** Consider the specification  $S(Q)$  in (14), the system  $S(\bar{\Sigma}_d)$ , and a desired accuracy  $\varepsilon \in \mathbb{R}^+$ . Find a symbolic controller system  $S_C$ , some parameters  $\theta, \mu_{\mathbf{X}} \in \mathbb{R}^+$  and a strong A $\theta$ A simulation relation  $\mathcal{R}$  from  $S_C$  to  $S(\bar{\Sigma}_d)$  such that:

- 1) the  $\theta$ -approximate feedback composition of  $S(\bar{\Sigma}_d)$  and  $S_C$ , denoted  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_C$ , is approximately simulated<sup>1</sup> by  $S(Q)$  with accuracy  $\varepsilon$ , i.e.  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_C \preceq_{\varepsilon} S(Q)$ ;
- 2) the system  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_C$  is non-blocking;
- 3) for any pair of states  $x = (x_1, x_2, \dots, x_N, u)$  and  $x' = (x'_1, x'_2, \dots, x'_N, u')$  of  $S(\bar{\Sigma}_d)$  if  $[x_i]_{\mu_{\mathbf{X}}} = [x'_i]_{\mu_{\mathbf{X}}}$  for all  $i \in [1; N]$ , then  $\mathcal{R}^{-1}(\{x\}) = \mathcal{R}^{-1}(\{x'\})$ .

The control design problem above, except for condition 3), is known in the literature as an approximate similarity game (see e.g. [21]). Condition 1) requires the state trajectories of the NCS to be close to the state run of the specification  $S(Q)$  up to the accuracy  $\varepsilon$  irrespective of the particular realization of the network non-idealities, and condition 2) prevents deadlocks in the interaction between the plant and the controller. Condition 3) requires that aggregate states of  $S(\bar{\Sigma}_d)$  with the same quantization are indistinguishable for the controller. By adding condition 3) and by using the notion of strong alternating simulation relation (embedded in the notion of approximate feedback composition), we are able to deal with approximate similarity games where state measurements are only available through their quantizations. Symbolic control problems for control systems with quantized state measurements and safety and reachability specifications have been studied in [24]. We also recall the recent work [53] that extends [24] to general specifications for the class of nonlinear systems. The present control problem extends those considered in [24] to NCS and specifications expressed as non-deterministic transition systems.

In order to solve Problem 2, some preliminary definitions and results are needed. Given two systems  $S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i)$  ( $i = 1, 2$ ),  $S_1$  is a *sub-system* of  $S_2$  if  $X_1 \subseteq X_2$ ,  $X_{0,1} \subseteq X_{0,2}$ ,  $U_1 \subseteq U_2$ ,  $\xrightarrow{1} \subseteq \xrightarrow{2}$ ,  $Y_1 \subseteq Y_2$  and  $H_1(x) = H_2(x)$  for any  $x \in X_1$ . Moreover, given two sub-systems  $S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i)$  ( $i = 1, 2$ ) of a system  $S$ , define the union

---

<sup>1</sup>The notions of approximate feedback composition and of approximate simulation are formally recalled in the Appendix.



system  $S_1 \sqcup S_2$  as  $(X_1 \cup X_2, X_{0,1} \cup X_{0,2}, U_1 \cup U_2, \xrightarrow{1} \cup \xrightarrow{2}, Y_1 \cup Y_2, H)$ , where  $H(x) = H_1(x)$  if  $x \in X_1$  and  $H(x) = H_2(x)$  otherwise. Note that  $S_1 \sqcup S_2$  is a sub-system of  $S$ . It is easy to see that the union operator enjoys the associative property. We now have all the ingredients to introduce the controller  $S_{C^*}$  that will solve Problem 2.

**Definition 5** *The symbolic controller  $S_{C^*}$  is the maximal non-blocking sub-system<sup>2</sup>  $S_C$  of  $S_*(\bar{\Sigma}_d)$  such that:*

- 1)  $S_C$  is approximately simulated by  $S(Q)$  with accuracy  $\mu_{\mathbf{X}}$ , i.e.  $S_C \preceq_{\mu_{\mathbf{X}}} S(Q)$ ;
- 2)  $S_C$  is strongly alternatingly 0-simulated by  $S_*(\bar{\Sigma}_d)$ , i.e.  $S_C \preceq_0^{s, \text{alt}} S_*(\bar{\Sigma}_d)$ .

Condition 1) of the definition above requires that for any state run  $r_c$  of  $S_C$  there exists a state run  $r_q$  in  $S(Q)$  such that  $r_c$  approximates  $r_q$  within the accuracy  $\mu_{\mathbf{X}}$ . Condition 2) ensures that the controller enforces the specification irrespective of the time-delay realization induced by the communication network. The following result holds.

**Proposition 3** *The symbolic controller  $S_{C^*}$  is the union of all non-blocking sub-systems  $S_C$  of  $S_*(\bar{\Sigma}_d)$  satisfying conditions 1) and 2) of Definition 5.*

**Proof 2** Let  $S_C$  and  $S'_C$  be a pair of non-blocking sub-systems of  $S_*(\bar{\Sigma}_d)$  satisfying both conditions 1) and 2) of Definition 5. Let  $\mathcal{R}_a$  (resp.  $\mathcal{R}'_a$ ) be a  $\mu_{\mathbf{X}}$ -approximate simulation relation from  $S_C$  (resp.  $S'_C$ ) to  $S(Q)$ . Let  $\mathcal{R}_b$  (resp.  $\mathcal{R}'_b$ ) be a strong alternating 0-approximate simulation relation from  $S_C$  (resp.  $S'_C$ ) to  $S_*(\bar{\Sigma}_d)$ . Consider the system  $S_C \sqcup S'_C$ . By definition of operator  $\sqcup$ , relation  $\mathcal{R}_a \cup \mathcal{R}'_a$  is a  $\mu_{\mathbf{X}}$ -approximate simulation from  $S_C \sqcup S'_C$  to  $S(Q)$ , and relation  $\mathcal{R}_b \cup \mathcal{R}'_b$  is a strong alternating 0-approximate simulation from  $S_C \sqcup S'_C$  to  $S_*(\bar{\Sigma}_d)$ . Hence,  $S_C \sqcup S'_C$  satisfies condition 1) and 2) of Definition 5. Moreover, since  $S_C$  and  $S'_C$  are non-blocking, again by definition of operator  $\sqcup$ , system  $S_C \sqcup S'_C$  is non-blocking as well. Finally, since  $S_{C^*}$  is the union of all non-blocking sub-systems  $S_C$  of  $S_*(\bar{\Sigma}_d)$  satisfying conditions 1) and 2) of Definition 5, it is the maximal non-blocking sub-system  $S_C$  of  $S_*(\bar{\Sigma}_d)$  satisfying conditions 1) and 2) of Definition 5.

Although  $S_*(\bar{\Sigma}_d)$  is countable, since the set  $\mathbf{X}$  is bounded and  $S(Q)$  is symbolic, the controller system  $S_{C^*}$  is symbolic and can be computed in a finite number of steps by adapting standard fixed point characterizations of simulation [54, 21]. We now provide the solution to Problem 2.

**Theorem 2** *Consider the NCS  $\Sigma$  and the specification  $S(Q)$ . Suppose that there exists a  $\delta$ -FC Lyapunov function  $V$  for the control system  $P$  in the NCS*

<sup>2</sup>Here maximality is defined with respect to the preorder induced by the notion of sub-system.

$\Sigma$ . For any desired accuracy  $\varepsilon \in \mathbb{R}^+$ , choose the parameters  $\theta, \mu_{\mathbf{X}} \in \mathbb{R}^+$  such that:

$$\mu_{\mathbf{X}} + \theta \leq \varepsilon \quad (15)$$

with  $\mu_{\mathbf{X}} = \hat{\mu}_{\mathbf{X}}/n_{\mathbf{X}}$ , for some integer  $n_{\mathbf{X}}$ . Then a strong A $\theta$ A simulation relation  $\mathcal{R}$  from  $S_{C^*}$  to  $S(\bar{\Sigma}_d)$  exists solving Problem 2 with  $S_C = S_{C^*}$ .

**Proof 3** By condition 2) in Definition 5, a (non-empty) strong A $\theta$ A simulation relation  $\mathcal{R}_1$  from  $S_{C^*}$  to  $S_*(\bar{\Sigma}_d)$  exists. Let  $\mathcal{R}_2$  be the relation defined in the proof of Theorem 1. Since there exists a  $\delta$ -FC Lyapunov function for the plant  $P$  and condition (15) holds, by Theorem 1,  $\mathcal{R}_2$  is a strong A $\theta$ A simulation relation from  $S_*(\bar{\Sigma}_d)$  to  $S(\bar{\Sigma}_d)$ . Define the relation  $\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2$ . By Lemma 1 (ii),  $\mathcal{R}$  is a strong A $\theta$ A simulation relation from  $S_{C^*}$  to  $S(\bar{\Sigma}_d)$ . We start by showing condition 1) of Problem 2. The existence of  $\mathcal{R}_1$  and  $\mathcal{R}_2$  implies by Definition 6 that  $S_{C^*} \preceq_0^{s, \text{alt}} S_*(\bar{\Sigma}_d)$  and  $S_*(\bar{\Sigma}_d) \preceq_{\theta}^{s, \text{alt}} S(\bar{\Sigma}_d)$ . Hence, from Lemma 1 (ii) in the Appendix, by combining the previous implications, one gets  $S_{C^*} \preceq_{\theta}^{s, \text{alt}} S(\bar{\Sigma}_d)$  which, by Lemma 1 (iii), leads to  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*} \preceq_{\theta} S_{C^*}$ . Since  $S_{C^*} \preceq_{\mu_{\mathbf{X}}} S(Q)$  by condition 1) in Definition 5, Lemma 1 (ii) and condition (15) imply  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*} \preceq_{\varepsilon} S(Q)$ . We now show that condition 2) holds. Consider any state  $(x, x_c)$  of  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$ . Pick any  $u_c \in U_c(x_c)$ , which is a non-empty set because  $S_{C^*}$  is non-blocking. Since  $(x_c, x) \in \mathcal{R}$ , for any  $x \xrightarrow[\tau]{u} x'$  in  $S(\bar{\Sigma}_d)$  there exists  $x_c \xrightarrow[c]{u} x'_c$  in  $S_{C^*}$  with  $(x'_c, x') \in \mathcal{R}$ .

Hence, from Definition 7, the transition  $(x, x_c) \xrightarrow{u} (x', x'_c)$  is in  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$ , implying that  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$  is non-blocking. We conclude by showing condition 3). Consider a pair of states  $x = (x_1, x_2, \dots, x_N, u)$  and  $x' = (x'_1, x'_2, \dots, x'_N, u')$  of  $S(\bar{\Sigma}_d)$  such that  $[x_i]_{\mu_{\mathbf{X}}} = [x'_i]_{\mu_{\mathbf{X}}}$  for all  $i \in [1; N]$ . Since  $\mathcal{R}_2^{-1}(\{x\}) = \{[x]_{\mu_{\mathbf{X}}}\}$ ,  $\mathcal{R}_2^{-1}(\{x'\}) = \{[x']_{\mu_{\mathbf{X}}}\} = \{[x]_{\mu_{\mathbf{X}}}\}$ , by recalling that  $\mathcal{R}^{-1}(\{x\}) = \mathcal{R}_1^{-1}(\mathcal{R}_2^{-1}(\{x\}))$  and  $\mathcal{R}^{-1}(\{x'\}) = \mathcal{R}_1^{-1}(\mathcal{R}_2^{-1}(\{x'\}))$ , we get condition 3).

We now proceed with a further step by refining the controller  $S_{C^*}$  solving Problem 2 to a controller  $C^*$  in form of (2) which can be applied to the original NCS and solves Problem 1. Let  $U_{C^*}(\cdot)$  and  $\text{Post}(\cdot)$  be the operators defined in Definition 1 but applied to system  $S_{C^*}$ . Let  $S_{C^*} = (X_{C^*}, X_{0, C^*}, U_{C^*}, \xrightarrow{C^*}, Y_{C^*}, H_{C^*})$ . Define  $\Xi_C = X_{C^*}$ ,  $\Xi_C^0 = X_{0, C^*}$  and

$$\begin{cases} h_C(\xi) \in U_{C^*}(\xi), \\ f_C(\xi, w) = \{\xi' = (\xi'_1, \dots, \xi'_{N'}, \bar{u}) \in \text{Post}_{h_C(\xi)}(\xi) : \xi'_{N'} = w\}, \end{cases} \quad (16)$$

for any  $(\xi, w) \in \Xi_C \times [\mathbf{X}]_{\mu_{\mathbf{X}}}$ . Note from the first line in (16) that the controller  $C$ , as in (2), derived from a non-blocking non-deterministic system  $S_{C^*}$  is not uniquely determined, since  $U_{C^*}(\xi) \neq \emptyset$  may not be a singleton. Moreover, the second line in (16) takes into account that  $\xi'_{N'}$  is the state of the aggregate vector  $x^*$  in  $\xi'$  which is required to match the output sample  $w$ , sent through the plant-to-controller branch of the network and reaching the controller (as illustrated in Section 3). We conclude this section by proving the formal correctness of the controller  $C^*$  as defined above.

**Theorem 3** Assume that the conditions of Theorem 2 hold, implying the existence of some parameters  $\theta, \mu_{\mathbf{X}} \in \mathbb{R}^+$  satisfying the inequality in (15), with  $\mu_{\mathbf{X}} = \hat{\mu}_{\mathbf{X}}/n_{\mathbf{X}}$  for some integer  $n_{\mathbf{X}}$ , of a symbolic controller system  $S_C = S_{C^*}$  and of a strong A $\theta$ A simulation relation  $\mathcal{R}$  from  $S_C$  to  $S(\bar{\Sigma}_d)$  solving Problem 2. Set  $\mathbf{X}_0$  such that  $\mathcal{R}(X_{0,C^*}) = \mathbf{X}_0 \times \{\tilde{u}_0\}$ . Then the controller  $C^*$  solves Problem 1.

**Proof 4** Consider the strong A $\theta$ A simulation relation  $\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2$  from  $S_{C^*}$  to  $S(\bar{\Sigma}_d)$  defined in the proof of Theorem 2. Now consider any  $\tilde{y}_0 = x(0) \in \mathbf{X}_0$ , implying that  $x^0 = (x(0), \tilde{u}_0) \in \mathcal{R}(X_{0,C^*})$  by definition of  $\mathbf{X}_0$ . Then consider the state  $\xi_1 := ([x(0)]_{\mu_{\mathbf{X}}}, \tilde{u}_0)$ ; by definition of  $\mathcal{R}$  we get  $\xi_1 \in \mathcal{R}^{-1}(x^0)$ , implying that  $\xi_1 \in X_{0,C^*}$ . From the first line in the refinement equation (16), the control input  $v_1 = h_C(\xi_1) \in U_{C^*}(\xi_1)$  is uniquely determined. Furthermore, since  $(\xi_1, x^0) \in \mathcal{R}$ , which is a strong A $\theta$ A simulation relation from  $S_{C^*}$  to  $S(\bar{\Sigma}_d)$ , then  $v_1 \in \mathbf{U}(x^0)$  in  $S(\bar{\Sigma}_d)$  and, for any transition  $x^0 \xrightarrow{v_1} x^1 = (\bar{x}^1, v_1) = ((\bar{x}_1^1, \dots, \bar{x}_{N_1}^1), v_1)$  in  $S(\bar{\Sigma}_d)$ , there exists a transition  $\xi_1 \xrightarrow{v_1} \xi_2 = ((\xi_{2,1}, \dots, \xi_{2,N_1}), v_1)$  in  $S_{C^*}$  such that  $(\xi_2, x^1) \in \mathcal{R}$ , implying  $\xi_{2,N_1} = [x_{N_1}^1]_{\mu_{\mathbf{X}}}$  from the definition of  $\mathcal{R}$ . By induction, assume now  $(\xi_k, x^{k-1}) \in \mathcal{R}$  for some  $k \in \mathbb{N}$ , with  $x^{k-1}$  in the form  $x^{k-1} = (\bar{x}^{k-1}, v_{k-1})$ , and again by exploiting the non-blocking property of  $S_{C^*}$ , the definition of  $\mathcal{R}$  and the refinement equation (16), it is readily seen that by choosing  $v_k = h_C(\xi_k) \in U_{C^*}(\xi_k)$ , then one has  $v_k \in \mathbf{U}(x^{k-1})$  in  $S(\bar{\Sigma}_d)$  and, for any transition  $x^{k-1} \xrightarrow{v_k} x^k = (\bar{x}^k, v_k) = ((\bar{x}_1^k, \dots, \bar{x}_{N_k}^k), v_k)$  in  $S(\bar{\Sigma}_d)$ , there exists a transition  $\xi_k \xrightarrow{v_k} \xi_{k+1} = ((\xi_{k+1,1}, \dots, \xi_{k+1,N_k}), v_k)$  in  $S_{C^*}$  such that  $(\xi_{k+1}, x^k) \in \mathcal{R}$ , implying  $\xi_{k+1,N_k} = [x_{N_k}^k]_{\mu_{\mathbf{X}}}$  from the definition of  $\mathcal{R}$ . As a result of the procedure above, we built an infinite sequence  $\{(\xi_k, x^{k-1})\}_{k \in \mathbb{N}} \subseteq \mathcal{R}$  and two infinite state runs  $\xi_1 \xrightarrow{v_1} \xi_2 \xrightarrow{v_2} \xi_3 \xrightarrow{v_3} \dots$  and  $x^0 \xrightarrow{v_1} x^1 \xrightarrow{v_2} x^2 \xrightarrow{v_3} \dots$  in  $S_{C^*}$  and  $S(\bar{\Sigma}_d)$ , respectively. By Definition 7 of approximate feedback composition, this implies that

$$(x^0, \xi_1) \xrightarrow{v_1} (x^1, \xi_2) \xrightarrow{v_2} (x^2, \xi_3) \xrightarrow{v_3} \dots \quad (17)$$

is an infinite state run of  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$ . From Proposition 2, the existence of an infinite state run  $x^0 \xrightarrow{v_1} x^1 \xrightarrow{v_2} x^2 \xrightarrow{v_3} \dots$  in  $S(\bar{\Sigma}_d)$  implies the existence of an infinite trajectory  $\{\tilde{y}_s\}_{s \in \mathbb{N}_0} = \{z_s\}_{s \in \mathbb{N}_0}$  of  $\Sigma_d$  such that

$$\{x(0), \underbrace{\bar{x}_1^1, \dots, \bar{x}_{N_1}^1}_{\bar{x}^1}, \underbrace{\bar{x}_1^2, \dots, \bar{x}_{N_2}^2}_{\bar{x}^2}, \dots\} = \{z_s\}_{s \in \mathbb{N}_0} = \{\tilde{y}_s\}_{s \in \mathbb{N}_0}. \quad (18)$$

From the definition of quantizer and switch in (7), one can write, for any  $k \in \mathbb{N} \setminus \{1\}$ ,  $w_k = y_{M_k} = [\tilde{y}_{M_k}]_{\mu_{\mathbf{X}}} = [x_{N_{k-1}}^{k-1}]_{\mu_{\mathbf{X}}} = \xi_{k,N_{k-1}}$ . This implies, from the second line in (16), that  $\xi_k \in f_C(\xi_{k-1}, w_k)$ , so the evolution of the controller in (2) is well defined at all iterations  $k$ . Finally, from Proposition 1, the existence of the trajectory  $\{z_s\}_{s \in \mathbb{N}_0}$  of  $\Sigma_d$  in (18) implies that there exists a trajectory  $x : [0, +\infty[ \rightarrow \mathbb{R}^n$  of the NCS  $\Sigma$  such that  $\tilde{y}_s = z_s = x(\tau s)$  for all  $s \in \mathbb{N}_0$ . This

concludes the proof that any sequence  $\{\tilde{y}_s\}$  generated by the NCS is defined for all  $s \in \mathbb{N}_0$ . Since the assumptions of Theorem 2 hold, condition 1) of Problem 2 is fulfilled by the controller  $S_{C^*}$ , i.e.  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*} \preceq_{\varepsilon} S(Q)$ . Hence, Definition 6 (approximate simulation) implies that, for any initial state  $(x^0, \xi_1)$  of  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$ , there exists  $x_q^0 \in X_Q^0$  such that  $d_{Y_{\tau}}(H_{\tau}(x^0), H_q(x_q^0)) = \|x(0) - x_q^0\| \leq \varepsilon$ , and the existence of a state run (17) in  $S(\bar{\Sigma}_d) \times_{\theta}^{\mathcal{R}} S_{C^*}$  implies the existence of a state run

$$x_q^0 \xrightarrow[q]{u_q} x_q^1 \xrightarrow[q]{u_q} x_q^2 \xrightarrow[q]{u_q} \dots \quad (19)$$

in  $S(Q)$ , with  $x_q^k$  in the form  $x_q^k = (x_{q,1}^k, \dots, x_{q,N_k}^k)$ , such that  $d_{Y_{\tau}}(H_{\tau}(x^k), H_q(x_q^k)) = \max_i \|\bar{x}_i^k - x_{q,i}^k\| \leq \varepsilon$ , implying

$$\|\bar{x}_i^k - x_{q,i}^k\| \leq \varepsilon, \quad \forall k \in \mathbb{N} \text{ and } \forall i = 1, \dots, N_k. \quad (20)$$

In turn, from the definition of specification  $Q$ , the existence of a state run in  $S(Q)$  in Eq. (19) implies the existence in  $Q$  of the transitions  $(x_Q^s, x_Q^{s+1}) \in T_Q$ , for all  $s \in \mathbb{N}_0$ , such that:

$$\{x_q^0, \underbrace{x_{q,1}^1, \dots, x_{q,N_1}^1}_{x_q^1}, \underbrace{x_{q,1}^2, \dots, x_{q,N_2}^2}_{x_q^2}, \dots\} = \{x_Q^s\}_{s \in \mathbb{N}_0}. \quad (21)$$

Hence, condition 1) of Problem 1 holds. Finally, by (18), (21), and (20), we get condition 2) of Problem 1.

## 6 Application to Robot Motion Planning with Remote Control

Symbolic techniques for robot motion planning and control have been successfully exploited in the literature, see e.g. [55] and the references therein. However, existing work does not consider the symbolic control of robot motion over non-ideal communication networks. In this section we exploit the remote control of an electric car-like robot, with limited power, sensing, computation and communication capabilities, whose goal is the surveillance of an area. The motion of the robot  $P$  is described by means of the following nonlinear control system:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} u_1 \frac{\cos(x_3 + \delta(u_2))}{\cos(\delta(u_2))} \\ u_1 \frac{\sin(x_3 + \delta(u_2))}{\cos(\delta(u_2))} \\ \frac{u_1}{b} \tan(u_2) \end{bmatrix}, \quad (22)$$

where  $\delta(u_2) = \arctan\left(\frac{a \tan(u_2)}{b}\right)$ ,  $a = 0.5$  is the distance of the center of mass from the rear axle and  $b = 1.5$  is the wheel base, see Fig. 3 (left panel) (modified from Fig. 2.16 in [56]). States  $x_1$  and  $x_2$  are the 2D-coordinates of the center of mass of the vehicle and state  $x_3$  is its heading angle, while the inputs  $u_1$  and  $u_2$  are the velocity of the rear wheel and the steering angle, respectively. Note that

$u_1$  is always nonnegative to guarantee that the vehicle does not move backwards. All the quantities are expressed in units of the International System (SI). We consider an accuracy  $\varepsilon = 0.02$ , and the bounded set including all the specification trajectories up to  $\varepsilon$  is  $\mathbf{X} = [-x_{1,\max}, x_{1,\max}] \times [-x_{2,\max}, x_{2,\max}] \times [-x_{3,\max}, x_{3,\max}]$ , and  $u \in \mathbf{U} \subset [0, u_{1,\max}] \times [-u_{2,\max}, u_{2,\max}]$ , where  $x_{\max} = [x_{1,\max}, x_{2,\max}, x_{3,\max}]' = [50, 50, \pi]'$  and  $u_{\max} = [u_{1,\max}, u_{2,\max}]' = [5, \frac{\pi}{3}]'$ . The model above is known in the literature as *single-track* vehicle model and is widely used because, in spite of its simplicity, it well captures the major features of interest of the vehicle cornering behavior [57]. The robot  $P$  is remotely connected to a controller, implemented on a shared CPU, by means of a non-ideal communication network. The control loop forms a NCS, as the one in Fig. 1, whose network/computation parameters are  $B_{\min} = 0.1 \text{ kbit/s}$ ,  $B_{\max} = 1 \text{ kbit/s}$ ,  $\tau = 1s$ ,  $\Delta_{\min}^{\text{ctrl}} = 0.01s$ ,  $\Delta_{\max}^{\text{ctrl}} = 0.1s$ ,  $\Delta_{\min}^{\text{req}} = 0.05s$ ,  $\Delta_{\max}^{\text{req}} = 0.2s$ ,  $\Delta_{\min}^{\text{net}} = 0.1s$ ,  $\Delta_{\max}^{\text{net}} = 0.25s$ . Given the different nature of the three state variables, the state quantization is assumed to be different (in absolute values) for each component and equal to  $x_{i,\max}/100$  for the state  $x_i$  ( $i = 1, 2, 3$ ), so that we have 200 quantization values for each state component. Similarly, we assume the input quantization to be equal to  $u_{i,\max}/5$  for the input  $u_i$  ( $i = 1, 2$ ) and the network protocols to introduce a relative overhead which is bounded by the 20% of the total number of data bits ( $N_{\text{cp}}^+ = N_{\text{pc}}^+ = 0.2$ ). This implies  $|\mathbf{X}|_{\mu_{\mathbf{X}}} = 200^3$  and  $|\mathbf{U}| = 50$ , hence  $\Delta_{\min}^{B,\text{pc}} = 0.0276s$ ,  $\Delta_{\max}^{B,\text{pc}} = 0.276s$ ,  $\Delta_{\min}^{B,\text{cp}} = 0.0072s$ ,  $\Delta_{\max}^{B,\text{cp}} = 0.072s$ . We assume there may be packet dropouts, with the constraint that two consecutive dropouts are not allowed ( $N_{\text{pd}} = 1$ ). The motion planning problem considered here is described in the following. We require that the robot leaves its support (HOME location) and visits (in the exact order) two buildings, denoted by  $B1$  and  $B2$ , to then reach an outlet where it possibly powers up the battery (CHARGE location). Finally, the vehicle returns HOME. During the whole path, the robot is requested to avoid some obstacles, such as walls and other buildings. We denote the union of the obstacles locations as the UNSAFE location. We now start applying the results in Section 4 regarding the design of a symbolic model for the given NCS. According to the definition of  $\Sigma_d$ , the minimum and maximum delays in a single iteration of the network amount to  $\Delta_{\min} = 0.24s$  and  $\Delta_{\max} = 2.07s$ , respectively. From (6), this results in  $N_{\min} = 1$ ,  $N_{\max} = 3$ . In order to have a uniform quantization in the state space, we apply the results to a normalized plant  $\tilde{P}$ , whose state is the one of  $P$ , but component-wise normalized with respect to  $x_{\max}$ . According to the previous description of the NCS, this results in  $\hat{\mu}_{\mathbf{X}} = 1$ ,  $n_{\mathbf{X}} = 200$  and  $\mu_{\mathbf{X}} = 0.005$ . We assume that the normalized signals are sent through the network and the static block implementing the coordinate change from  $P$  to  $\tilde{P}$  and vice versa (omitted in the general scheme) is physically connected to the sensor. It is possible to show that the quadratic Lyapunov-like function  $V(x, x') = 0.5 \|x - x'\|_2^2$ , is  $\delta$ -FC for control system (22), with  $\lambda = \frac{2u_{1,\max}}{\cos(\delta(u_{2,\max}))}$ ,  $\underline{\alpha}(r) = 0.5r^2$ ,  $\overline{\alpha}(r) = 1.5r^2$  and  $\gamma(r) = 6r$ ; hence Theorem 1 can be applied. In the symbolic control design step, we apply the results illustrated in Section 5. We first construct a finite transition system  $Q$  which encodes a number of randomly generated trajectories

satisfying the given specification. For the choice of  $\theta = 0.0125$ , Theorem 2 holds and the controller  $S_{C^*}$  in Definition 5 solves the control problem. Estimates of the space complexity in constructing  $S_{C^*}$  indicate  $4 \cdot 10^{13}$  32-bit integers. Because of the large computational complexity in building the controller  $S_{C^*}$ , we do not construct the whole symbolic model  $S_*(\bar{\Sigma}_d)$ , from which deriving  $S_{C^*}$ , but only the part of  $S_*(\bar{\Sigma}_d)$  that can implement (part of) the specification  $Q$ ; similar ideas were explored in [47], see also [49]. The total memory occupation and time required to construct  $S_{C^*}$  are respectively 3742 32-bit integers and 2833 s. The computation has been performed on the Matlab suite through an Apple MacBook Pro with 2.5GHz Intel Core i5 CPU and 16 GB RAM. In Fig. 3 (right panel), we show a sample path of the NCS (blue solid line), for a particular realization of the network uncertainties, compared to the trajectory of the system controlled through an ideal network (black dash-dotted line). Each time delay realization  $N_k$  is sampled from a discrete uniform random distribution over  $[N_{\min}; N_{\max}]$ . As a result, the NCS used just 59 control samples, in spite of the 94 control samples (one at each  $\tau$ ) used in the ideal case. Note that, although the behavior of the NCS is not as regular as in the ideal case, the specification is indeed met.

## 7 Conclusions

In this paper we proposed a symbolic approach to the control design of nonlinear NCS, where the most important non-idealities in the communication channel are taken into account. Under the assumption of existence of incremental forward complete Lyapunov functions, we derived symbolic models that approximate NCS in the sense of strong alternating approximate simulation. NCS symbolic control design, where specifications are expressed in terms of transition systems, was then solved and applied to an example of remote robot motion planning.

## Acknowledgements

The authors are grateful to Pierdomenico Pepe for fruitful discussions on the topic of this article.

## References

- [1] R. Murray, K. Astrom, S. Boyd, R. Brockett, and G. Stein, “Control in an information rich world,” *IEEE Control Systems Magazine*, vol. 23, no. 2, pp. 20–33, April 2003.
- [2] W. Heemels and N. van de Wouw, “Stability and stabilization of networked control systems,” in *Networked Control Systems*, ser. Lecture notes in control and information sciences, A. Bemporad, W. Heemels, and M. Johansson, Eds. London: Springer Verlag, 2011, vol. 406, pp. 203–253.

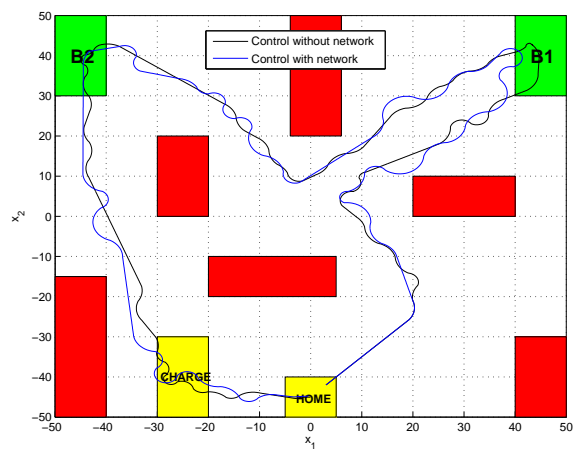
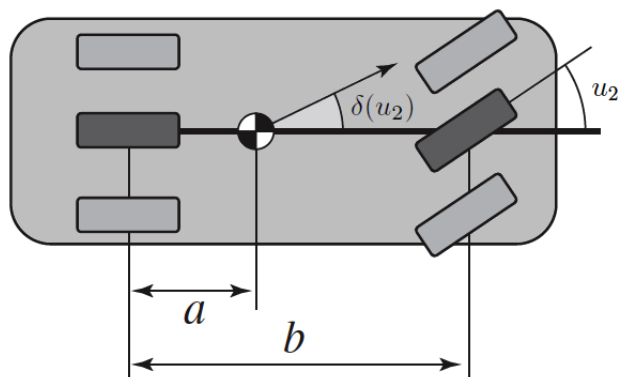


Figure 3: Overhead view of the robot dynamics (top panel). Space trajectory of the vehicle (bottom panel).

- [3] M. B. Cloosterman, L. Hetel, N. Van De Wouw, W. Heemels, J. Daafouz, and H. Nijmeijer, "Controller synthesis for networked control systems," *Automatica*, vol. 46, no. 10, pp. 1584–1594, 2010.
- [4] M. García-Rivera and A. Barreiro, "Analysis of networked control systems with drops and variable delays," *Automatica*, vol. 43, no. 12, pp. 2054–2059, 2007.
- [5] H. Gao, T. Chen, and J. Lam, "A new delay system approach to network-based control," *Automatica*, vol. 44, no. 1, pp. 39–52, 2008.
- [6] P. Naghshtabrizi, J. P. Hespanha, and A. R. Teel, "Stability of delay impulsive systems with application to networked control systems," *Transactions of the Institute of Measurement and Control*, vol. 32, no. 5, pp. 511–528, 2010.
- [7] W. H. Heemels, A. R. Teel, N. van de Wouw, and D. Nesic, "Networked control systems with communication constraints: Tradeoffs between transmission intervals, delays and performance," *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1781–1796, 2010.
- [8] D. Nesic and A. R. Teel, "Input-output stability properties of networked control systems," *IEEE Transactions on Automatic Control*, vol. 49, no. 10, pp. 1650–1667, 2004.
- [9] J. Hespanha, P. Naghshtabrizi, and X. Yonggang, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, January 2007.
- [10] W. Heemels, N. van de Wouw, R. Gielen, M. Donkers, L. Hetel, S. Oлару, M. Lazar, J. Daafouz, and S. Niculescu, "Comparison of overapproximation methods for stability analysis of networked control systems," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, K. Johansson and W. Yi, Eds. Berlin: Springer Verlag, 2010, vol. 6174, pp. 181–191.
- [11] D. Nesic and D. Liberzon, "A unified framework for design and analysis of networked and quantized control systems," *IEEE Transactions on Automatic Control*, vol. 54, no. 4, pp. 732–747, 2009.
- [12] P. Naghshtabrizi and J. P. Hespanha, "Designing an observer-based controller for a network control system," in *44th IEEE Conference on Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC'05*. IEEE, 2005, pp. 848–853.
- [13] A. Chaillet and A. Bicchi, "Delay compensation in packet-switching networked controlled systems," in *47th IEEE Conference on Decision and Control, 2008. CDC 2008*. IEEE, 2008, pp. 3620–3625.



- [14] M. Donkers, W. Heemels, N. Van De Wouw, and L. Hetel, “Stability analysis of networked control systems using a switched linear systems approach,” *IEEE Transactions on Automatic Control*, vol. 56, no. 9, pp. 2101–2115, 2011.
- [15] W. P. M. H. Heemels, D. Nesic, A. Teel, and N. Van de Wouw, “Networked and quantized control systems with communication delays,” in *Proceedings of the 48th IEEE Conference on Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009.*, Dec 2009, pp. 7929–7935.
- [16] R. Alur, A. D’Innocenzo, K. H. Johansson, G. J. Pappas, and G. Weiss, “Compositional modeling and analysis of multi-hop control networks,” *IEEE Transactions on Automatic control*, vol. 56, no. 10, pp. 2345–2357, 2011.
- [17] D. J. Antunes, J. P. Hespanha, and C. J. Silvestre, “Volterra integral approach to impulsive renewal systems: Application to networked control,” *IEEE Transactions on Automatic Control*, vol. 57, no. 3, pp. 607–619, 2012.
- [18] N. W. Bauer, P. J. Maas, and W. Heemels, “Stability analysis of networked control systems: A sum of squares approach,” *Automatica*, vol. 48, no. 8, pp. 1514–1524, 2012.
- [19] N. van de Wouw, D. Nešić, and W. Heemels, “A discrete-time framework for stability analysis of nonlinear networked control systems,” *Automatica*, vol. 48, no. 6, pp. 1144–1153, 2012.
- [20] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas, “Discrete abstractions of hybrid systems,” *Proceedings of the IEEE*, vol. 88, pp. 971–984, 2000.
- [21] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.
- [22] G. Pola, A. Girard, and P. Tabuada, “Approximately bisimilar symbolic models for nonlinear control systems,” *Automatica*, vol. 44, pp. 2508–2516, October 2008.
- [23] M. Zamani, M. Mazo, G. Pola, and P. Tabuada, “Symbolic models for nonlinear control systems without stability assumptions,” *IEEE Transactions of Automatic Control*, vol. 57, no. 7, pp. 1804–1809, July 2012.
- [24] A. Girard, “Low-complexity quantized switching controllers using approximate bisimulation,” *Nonlinear Analysis: Hybrid Systems*, vol. 10, pp. 34–44, 2013.
- [25] R. Alur and D. L. Dill, *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science. Berlin: Springer, April 1990, vol. 443, ch. Automata for modeling real-time systems, pp. 322–335.

- [26] T. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya, “What’s decidable about hybrid automata?” *Journal of Computer and System Sciences*, vol. 57, pp. 94–124, 1998.
- [27] G. Lafferriere, G. J. Pappas, and S. Sastry, “O-minimal hybrid systems,” *Math. Control Signal Systems*, vol. 13, pp. 1–21, 2000.
- [28] T. Brihaye and C. Michaux, “On the expressiveness and decidability of o-minimal hybrid systems,” *Journal of Complexity*, vol. 21, no. 4, pp. 447–478, 2005.
- [29] P. E. Caines and Y. J. Wei, “Hierarchical hybrid control systems: A lattice-theoretic formulation,” *Special Issue on Hybrid Systems, IEEE Transaction on Automatic Control*, vol. 43, no. 4, pp. 501–508, April 1998.
- [30] X. D. Koutsoukos, P. J. Antsaklis, J. A. Stiver, and M. D. Lemmon, “Supervisory control of hybrid systems,” *Proceedings of the IEEE*, vol. 88, no. 7, pp. 1026–1049, July 2000.
- [31] T. Moor, J. Raisch, and S. D. O’Young, “Discrete supervisory control of hybrid systems based on l-complete approximations,” *Journal of Discrete Event Dynamic Systems*, vol. 12, pp. 83–107, 2002.
- [32] D. Forstner, M. Jung, and J. Lunze, “A discrete-event model of asynchronous quantised systems,” *Automatica*, vol. 38, pp. 1277–1286, 2002.
- [33] A. Bicchi, A. Marigo, and B. Piccoli, “On the reachability of quantized control systems,” *IEEE Transactions on Automatic Control*, vol. 47, no. 4, pp. 546–563, 2002.
- [34] P. Tabuada and G. Pappas, “Linear time logic control of discrete-time linear systems,” *IEEE Transactions of Automatic Control*, vol. 51, no. 12, pp. 1862–1877, 2006.
- [35] G. Pola and M.D. Di Benedetto, “Symbolic models and control of discrete-time piecewise affine systems: An approximate simulation approach,” *IEEE Transactions of Automatic Control*, vol. 59, no. 1, pp. 175–180, January 2014.
- [36] L. Habets, P. Collins, and J. V. Schuppen, “Reachability and control synthesis for piecewise-affine hybrid systems on simplices,” *IEEE Transactions on Automatic Control*, vol. 51, no. 6, pp. 938–948, 2006.
- [37] C. Belta and L. Habets, “Controlling a class of nonlinear systems on rectangles,” *IEEE Transactions on Automatic Control*, vol. 51, no. 11, pp. 1749–1759, 2006.
- [38] O. Junge, “A set oriented approach to global optimal control,” *ESAIM: Control, optimisation and calculus of variations*, vol. 10, no. 2, pp. 259–270, 2004.

- [39] G. Reißig, “Computation of discrete abstractions of arbitrary memory span for nonlinear sampled systems,” in *Proc. of 12th Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, vol. 5469, pp. 306–320, April 2009.
- [40] G. Pola and P. Tabuada, “Symbolic models for nonlinear control systems: Alternating approximate bisimulations,” *SIAM Journal on Control and Optimization*, vol. 48, no. 2, pp. 719–733, 2009.
- [41] A. Borri, G. Pola, and M. D. Di Benedetto, “Symbolic models for nonlinear control systems affected by disturbances,” *International Journal of Control*, vol. 88, no. 10, pp. 1422–1432, September 2012.
- [42] A. Girard, G. Pola, and P. Tabuada, “Approximately bisimilar symbolic models for incrementally stable switched systems,” *IEEE Transactions of Automatic Control*, vol. 55, no. 1, pp. 116–126, January 2010.
- [43] G. Pola, P. Pepe, M. Di Benedetto, and P. Tabuada, “Symbolic models for nonlinear time-delay systems using approximate bisimulations,” *Systems and Control Letters*, vol. 59, pp. 365–373, 2010.
- [44] G. Pola, P. Pepe, and M.D. Di Benedetto, “Symbolic models for time-varying time-delay systems via alternating approximate bisimulation,” *International Journal of Robust and Nonlinear Control*, 2014, DOI: 10.1002/rnc.3204, <http://arxiv.org/abs/1011.5835>. To appear.
- [45] A. Girard and G. Pappas, “Approximate bisimulation: a bridge between computer science and control theory,” *European Journal of Control*, vol. 17, no. 5–6, pp. 568–578, 2011.
- [46] A. Borri, G. Pola, and M. D. Di Benedetto, “A symbolic approach to the design of nonlinear networked control systems,” in *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, ser. HSCC ’12. New York, NY, USA: ACM, 2012, pp. 255–264. [Online]. Available: <http://doi.acm.org/10.1145/2185632.2185670>
- [47] A. Borri, G. Pola, and M. Di Benedetto, “Integrated symbolic design of unstable nonlinear networked control systems,” in *51th IEEE Conference on Decision and Control*, 2012, pp. 1374–1379.
- [48] M. Zamani, M. Mazo, M. Khaled, and A. Abate, “Symbolic abstractions of networked control systems,” 2016, available at arXiv: 1401.6396 [math.OC].
- [49] G. Pola, A. Borri, and M. D. Di Benedetto, “Integrated design of symbolic controllers for nonlinear systems,” *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 534–539, feb. 2012.
- [50] D. Angeli and E. Sontag, “Forward completeness, unboundedness observability, and their Lyapunov characterizations,” *Systems and Control Letters*, vol. 38, pp. 209–217, 1999.

- [51] ISO 11898-1:2003, *Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling*. ISO, Geneva, Switzerland.
- [52] H. Kopetz and G. Grunsteidl, “Ttp-a protocol for fault-tolerant real-time systems,” *Computer*, vol. 27, no. 1, pp. 14–23, Jan 1994.
- [53] 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, April 2017.
- [54] E. Clarke, O. Grumberg, and D. Peled, *Model Checking*. MIT Press, 1999.
- [55] C. Belta, A. Bicchi, M. Egerstedt, E. Frazzoli, E. Klavins, and G. Pappas, “Symbolic planning and control of robot motion,” *IEEE Robotics & Automation Magazine*, vol. 14, no. 1, pp. 61–70, March 2007.
- [56] K. J. Aström and R. M. Murray, *Feedback systems: an introduction for scientists and engineers*. Princeton University Press, 2010.
- [57] T. Gillespie, *Fundamentals of Vehicle Dynamics*. SAE BRASIL, 1992.
- [58] A. Girard and G. Pappas, “Approximation metrics for discrete and continuous systems,” *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.

We here recall from [58, 40], the notion of (alternating) approximate simulation relations and introduce the notion of strong alternating approximate simulation relations. Approximate feedback composition is also introduced and adapted from [21].

**Definition 6** Let  $S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i)$  ( $i = 1, 2$ ) be (pseudo)metric systems with the same output sets  $Y_1 = Y_2$  and (pseudo)metric  $d$ , and let  $\varepsilon \in \mathbb{R}_0^+$  be a given accuracy. Consider a relation  $\mathcal{R} \subseteq X_1 \times X_2$  satisfying the following conditions:

- (i)  $\forall x_1 \in X_{0,1} \exists x_2 \in X_{0,2}$  such that  $(x_1, x_2) \in \mathcal{R}$ ;
- (ii)  $\forall (x_1, x_2) \in \mathcal{R}, d(H_1(x_1), H_2(x_2)) \leq \varepsilon$ .

Relation  $\mathcal{R}$  is an  $\varepsilon$ -approximate simulation relation from  $S_1$  to  $S_2$  if it enjoys conditions (i), (ii) and the following one:

- (iii)  $\forall (x_1, x_2) \in \mathcal{R}$  if  $x_1 \xrightarrow[1]{u_1} x'_1$  then  $\exists x_2 \xrightarrow[2]{u_2} x'_2$  such that  $(x'_1, x'_2) \in \mathcal{R}$ .

System  $S_1$  is  $\varepsilon$ -simulated by  $S_2$  or  $S_2$   $\varepsilon$ -simulates  $S_1$ , denoted  $S_1 \preceq_\varepsilon S_2$ , if there exists an  $\varepsilon$ -approximate simulation relation from  $S_1$  to  $S_2$ . Relation  $\mathcal{R}$  is an alternating  $\varepsilon$ -approximate ( $A\varepsilon A$ ) simulation relation from  $S_1$  to  $S_2$  if it enjoys conditions (i), (ii) and the following one:

(iii')  $\forall (x_1, x_2) \in \mathcal{R} \forall u_1 \in U_1(x_1) \exists u_2 \in U_2(x_2)$  such that  $\forall x_2 \xrightarrow{\frac{u_2}{2}} x'_2 \exists x_1 \xrightarrow{\frac{u_1}{1}} x'_1$   
with  $(x'_1, x'_2) \in \mathcal{R}$ .

Relation  $\mathcal{R}$  is a strong alternating  $\varepsilon$ -approximate (strong  $A\varepsilon A$ ) simulation relation from  $S_1$  to  $S_2$  if it enjoys conditions (i), (ii) and the following one:

(iii'')  $\forall (x_1, x_2) \in \mathcal{R} \forall u_1 \in U_1(x_1), u_2 = u_1 \in U_2(x_2)$  and  $\forall x_2 \xrightarrow{\frac{u_2}{2}} x'_2 \exists x_1 \xrightarrow{\frac{u_1}{1}} x'_1$   
such that  $(x'_1, x'_2) \in \mathcal{R}$ .

System  $S_1$  is strongly alternatingly  $\varepsilon$ -simulated by  $S_2$  or  $S_2$  strongly alternatingly  $\varepsilon$ -simulates  $S_1$ , denoted  $S_1 \preceq_{\varepsilon}^{s, \text{alt}} S_2$ , if there exists a strong  $A\varepsilon A$  simulation relation from  $S_1$  to  $S_2$ .

The notion of strong  $A\varepsilon A$  simulation relation has been inspired by the notion of feedback refinement relations recently introduced in [53]. Interaction between plants and controllers in the systems domain is formalized as follows:

**Definition 7** [21] Consider a pair of (pseudo)metric systems  $S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i)$  ( $i = 1, 2$ ) with the same output sets  $Y_1 = Y_2$  and (pseudo)metric  $d$ , and let  $\varepsilon \in \mathbb{R}_0^+$  be a given accuracy. Let  $\mathcal{R}$  be a strong  $A\varepsilon A$  simulation relation from  $S_2$  to  $S_1$ . The  $\varepsilon$ -approximate feedback composition of  $S_1$  and  $S_2$ , with composition relation  $\mathcal{R}$ , is the system  $S_1 \times_{\varepsilon}^{\mathcal{R}} S_2 = (X, X_0, U, \longrightarrow, Y, H)$ , where  $X = \mathcal{R}^{-1}$ ,  $X_0 = X \cap (X_{0,1} \times X_{0,2})$ ,  $U = U_1$ ,  $(x_1, x_2) \xrightarrow{u} (x'_1, x'_2)$  if  $x_1 \xrightarrow{\frac{u}{1}} x'_1$  and  $x_2 \xrightarrow{\frac{u}{2}} x'_2$ ,  $Y = Y_1$  and  $H(x_1, x_2) = H_1(x_1)$  for any  $(x_1, x_2) \in X$ .

We conclude with a useful technical lemma.

**Lemma 1** [21] Let  $S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i)$  ( $i = 1, 2, 3$ ) be (pseudo)metric systems with the same output sets  $Y_1 = Y_2 = Y_3$  and (pseudo)metric  $d$ . Then, the following statements hold:

(i) for any  $\varepsilon_1 \leq \varepsilon_2$ ,  $S_1 \preceq_{\varepsilon_1}^{(s, \text{alt})} S_2$  implies  $S_1 \preceq_{\varepsilon_2}^{(s, \text{alt})} S_2$ ;

(ii) if  $S_1 \preceq_{\varepsilon_{12}}^{(s, \text{alt})} S_2$  with relation  $\mathcal{R}_{12}$  and  $S_2 \preceq_{\varepsilon_{23}}^{(s, \text{alt})} S_3$  with relation  $\mathcal{R}_{23}$  then  $S_1 \preceq_{\varepsilon_{12} + \varepsilon_{23}}^{(s, \text{alt})} S_3$  with relation  $\mathcal{R}_{12} \circ \mathcal{R}_{23}$ ;

(iii) for any  $\varepsilon \in \mathbb{R}_0^+$  and any strong  $A\varepsilon A$  simulation relation  $\mathcal{R}$  from  $S_2$  to  $S_1$ ,  $S_1 \times_{\varepsilon}^{\mathcal{R}} S_2 \preceq_{\varepsilon} S_2$ .