National School SIDRA 2017: Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Lecture L7a: Control design with logic specifications*

Abstract. In this lecture we use the symbolic models presented in the previous lecture to address control design of nonlinear systems with logic specifications. This lecture is based on [5].

1 Notation

Symbol $\wedge$ denotes the logical conjunction. Given a set A, the symbol 2^A denotes the power set of A, that is the collection of all subsets of A. For a pair of sets A and B we abuse notation by writing $A \times B = A$ when $B = \varnothing$. Given two sets X and Y and relation $\mathcal{R} \subseteq X \times Y$, symbol $\mathcal{R}^{-1}$ denotes the inverse relation of $\mathcal{R}$, i.e., $\mathcal{R}^{-1} = \{(y,x) \in Y \times X | (x,y) \in \mathcal{R}\}$. Given $X' \subseteq X$ and $Y' \subseteq Y$, we denote $\mathcal{R}(X') = \{y \in Y | \exists x \in X' \text{ s.t. } (x,y) \in \mathcal{R}\}$ and $\mathcal{R}^{-1}(Y') = \{x \in X | \exists y \in Y' \text{ s.t. } (x,y) \in \mathcal{R}\}$. Symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{R}^+_0$ denote the set of non–negative integer, integer, real, positive real, and non–negative real numbers, respectively. Given $n \in \mathbb{N}$ and $n > 0$, symbol $[1;n]$ denotes $\{1, 2, ..., n\}$. Given $x \in \mathbb{R}^n$, symbol $x(i)$ denotes the i–th element of x and $|x|$ the infinity norm of x. Given $a \in \mathbb{R}$ and $X \subseteq \mathbb{R}^n$, symbol aX denotes the set $\{y \in \mathbb{R}^n | \exists x \in X \text{ s.t. } y = ax\}$. Given $a, b \in \mathbb{R}$ we set $[a, b[= \{x \in \mathbb{R} | a \leq x < b\}$. Given $\theta \in \mathbb{R}^+$ and $x \in \mathbb{R}^n$, we define $\mathcal{B}_{[\theta[}(x) = \{y \in \mathbb{R}^n | y(i) \in [x(i) - \theta, x(i) + \theta[, i \in [1;n]\}$. Note that for any $\theta \in \mathbb{R}^+$, $\{\mathcal{B}_{[\theta[}(x)\}_{x \in 2\theta\mathbb{Z}^n}$ is a partition of $\mathbb{R}^n$. Given $z \in \mathbb{R}^n$, symbol $[z]^n_\theta$ denotes the unique vector in $\theta\mathbb{Z}^n$ such that $z \in \mathcal{B}_{[\theta/2[}([z]_\theta)$. Given functions $f : X \to Y$ and $g : Y \to Z$ we denote by $g \circ f$ the composition of functions f and g that is the function $(g \circ f) : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$. A continuous function $\rho : \mathbb{R}^+_0 \to \mathbb{R}^+_0$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\rho(0) = 0$; function ρ is said to belong to class $\mathcal{K}_\infty$ if $\rho \in \mathcal{K}$ and $\rho(r) \to \infty$ as $r \to \infty$.

2 Control problem formulation

We consider a plant described by the following nonlinear control system:

$$\Sigma : \begin{cases} \dot{x}(t) = f(x(t), u(t)), \\ x(t) \in \mathbf{X} = \mathbb{R}^n, \\ u(t) \in \mathbf{U} \subseteq \mathbb{R}^m, t \in \mathbb{R}^+_0, \end{cases} \tag{1}$$

where $x(t)$ is the state and $u(t)$ is the input at time $t \in \mathbb{R}^+_0$. Control inputs u are assumed to belong to the class $\mathcal{U}$ of piecewise continuous functions from $\mathbb{R}^+_0$ to $\mathbf{U}$. For simplicity we assume that function f is such that Σ admits a unique solution for any initial state $x(0) \in \mathbf{X}$ and for any control input function $u \in \mathcal{U}$ and it is forward complete, i.e. starting from any initial state $x(0) \in \mathbf{X}$ and for any control input function $u \in \mathcal{U}$, the solution $\mathbf{x}(\cdot, x_0, u)$ to the differential equation Σ exists for any time $t \in \mathbb{R}^+_0$. We also assume here that state variables are available for control purposes. We also assume that the set $\mathbf{U}$ is finite as it is often the case in concrete applications.

We now formalize the class of specifications we focus on in this lecture. Let Y_Q be a finite subset of the state space $\mathbb{R}^n$ of Σ. The specification is expressed as a regular language

$$L_Q \subset Y_Q^*, \tag{2}$$

where Y_Q^* is the Kleene closure of Y_Q. This class of specifications is rather rich as also discussed in lecture L4. For later purposes we recall from L4, how to formalize reachability specifications via regular expressions.

Example 1. **Reachability specification:** Starting from a set of initial states $I \subseteq \mathbb{R}^n$, my specification requires to reach in finite time a target set $T \subseteq \mathbb{R}^n$. Suppose that I and T have interior and are given as the unions of finite collections of hyperrectangles. Let $D \subseteq \mathbb{R}^n$ be a set representing the domain of interest and assume it has interior, is given as the union of a finite collection of hyperrectangles, and contains sets I and T. Consider the set I_η of points i_j in the lattice $\eta\mathbb{Z}^n$ that are far away from I no more than η, where $\eta \in \mathbb{R}^+$ represents the accuracy of the specification approximation, i.e. for any $i_j \in I_\eta$ there exists $x_j \in I$ such that $|i_j - x_j| \leq \eta$. Note that $I_\eta \neq \varnothing$ for any $\eta \in \mathbb{R}^+$. Consider the collection of points t_j in the set $T_\eta = T \cap (\eta\mathbb{Z}^n)$. Consider the collection of points d_j in the set $D_\eta = D \cap (\eta\mathbb{Z}^n)$. Under the assumptions placed on T and D, there exists $\hat{\eta} \in \mathbb{R}^+$ such that $T_\eta \neq \varnothing$ and $D_\eta \neq \varnothing$ for any $\eta \leq \hat{\eta}$, see[6]. The regular expression modeling the reachability specification corresponds to all and only words starting with symbols in I_η and with last symbols in T_η, i.e.

$$\left(\sum_{i_j \in I_\eta} i_j\right)\left(\sum_{d_j \in D_\eta} d_j\right)^*\left(\sum_{t_j \in T_\eta} t_j\right). \tag{3}$$

The corresponding regular language is given by:

$$I_\eta (D_\eta)^* T_\eta.$$

The class of controllers we consider is specified by:

$$C : \begin{cases} x_c(s+1) \in f_c(x_c(s)), \\ v(s) \in h_c(x_c(s)) \subseteq \mathbf{U}, \\ x_c(0) \in X_c^0 \subseteq X_c, \\ x_c(s) \in X_c, s \in \mathbb{N}, \end{cases} \tag{4}$$

where:

- X_c is the set of states of C;
- X_c^0 is the set of initial states of C;
- $f_c : X_c \to 2^{X_c}$ is the state transition map of C;
- $\mathbf{U}$ is the set of outputs of C;
- $h_c : X_c \to 2^{\mathbf{U}}$ is the output map of C;
- $x_c(s)$ is the state of C at step s;
- $v(s)$ is the output of C at step s.

We assume that set X_c is finite. Controller C is symbolic in the sense that sets X_c and $\mathbf{U}$ are finite. Moreover, it is non–deterministic, open–loop and dynamic. We will see that this class of controllers is general enough to enforce regular language specifications.
We denote by Σ^C the control system obtained by coupling Eqns. (1), (4) and a Zero order Holder (ZoH) block associating to the sequence $\{v(s)\}_{s\in\mathbb{N}}$, the control input $u \in \mathcal{U}$ defined for any $s \in \mathbb{N}$ by:

$$u(t) = v(s), \forall t \in [s\tau, (s+1)\tau[.$$

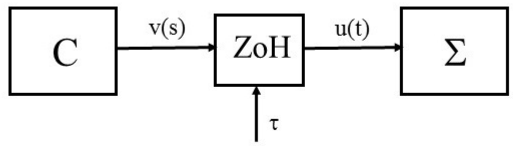

Fig. 1. Control scheme.

The control scheme we consider is depicted in Fig. 1.

We can now state the control problem we focus on:

Problem 1. Given the plant Σ, the specification L_Q in (2), a sampling time $\tau \in \mathbb{R}^+$ and a desired accuracy $\theta \in \mathbb{R}^+$, find the set $\mathbf{X}_0 \subseteq \mathbb{R}^n$ of initial states of the plant Σ and the controller C in (4) such that for any trajectory $x(\cdot)$ of Σ^C with $x(0) \in \mathbf{X}_0$, there exist an integer $s_f \in \mathbb{N}$ and a word $q_0 q_1 ... q_{s_f} \in L_Q$ such that

$$|x(s\tau) - q_s| \leq \theta, \tag{5}$$

for all $s \in [0; s_f]$.

The control problem above can be viewed as an approximating version of the classical supervisory control problem for discrete–event–systems.

3 Solution

We first recall from L6 the construction of symbolic models in the stable case.

Definition 1. *Given Σ, a sampling time $\tau \in \mathbb{R}^+$ and a state space quantization $\eta \in \mathbb{R}^+$, define*

$$T_{\tau,\eta}(\Sigma) = (X_{\tau,\eta}, X_{0,\tau,\eta}, U_{\tau,\eta}, \underset{\tau,\eta}{\longrightarrow}, X_{m,\tau,\eta}, Y_{\tau,\eta}, H_{\tau,\eta}),$$

where

- $X_{\tau,\eta} = X_{0,\tau,\eta} = X_{m,\tau,\eta} = [\mathbf{X}]_\eta^n$;
- $U_{\tau,\eta}$ *is the set of constant input functions* $u : [0, \tau[\rightarrow \mathbf{U}$;
- $\xi \underset{\tau,\eta}{\overset{u}{\longrightarrow}} \xi'$ *if* $\xi' = [\mathbf{x}(\tau, \xi, u)]_\eta^n$;
- $Y_{\tau,\eta} = \mathbb{R}^n$ *and*
- $H_{\tau,\eta}(x) = x$ *for all* $x \in X_{\tau,\eta}$.

Theorem 1. *Consider control system Σ and suppose it admits a δ–GAS Lyapunov function V and hence, satisfying conditions of Definition 5 in lecture L6, for some $\kappa \in \mathbb{R}^+$ and $\mathcal{K}_\infty$ functions α_1 and α_2 and the following inequality*

$$\forall x, y, z \in \mathbb{R}^n, \ |V(x, y) - V(x, z)| \leq \gamma(|y - z|). \tag{6}$$

for some $\mathcal{K}_\infty$ function γ. Then, for any desired accuracy $\mu \in \mathbb{R}^+$ and any sampling time $\tau \in \mathbb{R}^+$, select quantization parameter $\eta \in \mathbb{R}^+$ satisfying:

$$\eta \leq \min\left\{\gamma^{-1}((1-e^{-\kappa\tau})\alpha_1(\mu)), (\alpha_2^{-1} \circ \alpha_1)(\mu)\right\}. \tag{7}$$

Then, relation $\mathcal{R}_\mu \subseteq X_\tau \times X_{\tau,\eta}$ specified by

$$(x,\xi) \in \mathcal{R}_\mu \Leftrightarrow V(x,\xi) \leq \alpha_1(\mu) \tag{8}$$

is a μ–approximate bisimulation relation between $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$. Consequently, $T_\tau(\Sigma)$ and $T_{\tau,\eta}(\Sigma)$ are approximately bisimilar with accuracy μ.

We now represent the specification as a metric transition system (remember lecture L4). Since L_Q is a regular language there exists a symbolic transition system

$$S'_Q = (X'_Q, X'_{0,Q}, Y_Q, \underset{\prime,Q}{\longrightarrow}, X'_{Q,m}, Y'_Q, H'_Q),$$

such that its input marked language coincides with the language specification, i.e., $\mathcal{L}^u_m(S'_Q) = L_Q$. Without loss of generality, S'_Q can be chosen as deterministic, accessible and nonblocking, see e.g. [1]. Construction of S'_Q can be done by resorting to standard algorithms available in the literature, see e.g. [4], translating regular expressions to finite state automata. Automatic tools for constructing S'_Q are also well known, see e.g. [2].

Example 1. (Continued.) Suppose for simplicity that sets I_η, D_η and T_η are singleton and define:

$$I_\eta = \{a\}, \quad D_\eta = \{b\}, \quad T_\eta = \{c\}.$$

Regular expression in (3) becomes:

$$ab^*c. \tag{9}$$

The corresponding regular language becomes:

$$\{a\}\{b\}^*\{c\}.$$

Let $Y_Q = \{a, b, c\}$ and a specification L_Q be given by (9). A symbolic transition system S'_Q such that $\mathcal{L}^u_m(S'_Q) = L_Q$ is reported in Fig. 2. Note that S'_Q is deterministic, accessible and nonblocking.

It is useful to define the dual symbolic transition system S_Q of transition system S'_Q, where states of S_Q are transitions of S'_Q and vice versa. More formally:

Definition 2. *Given transition system S'_Q, define the dual transition system*

$$S_Q = (X_Q, X_{Q,0}, U_Q, \underset{Q}{\longrightarrow}, X_{Q,m}, \mathbb{R}^n, H_Q) \tag{10}$$

where:

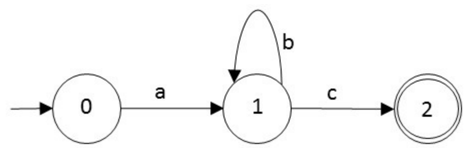

Fig. 2. Symbolic transition system S'_Q of Example 1.

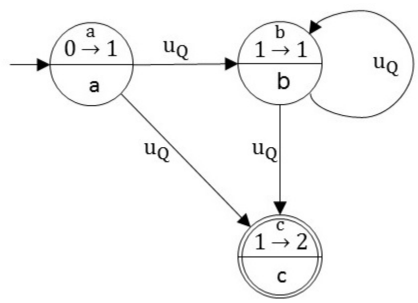

Fig. 3. Dual transition system S_Q of Example 1.

- *X_Q coincides with the set $\xrightarrow[\prime,Q]{}$ of transitions of S'_Q;*
- *$X_{Q,0}$ is the collection of states $x'_Q \xrightarrow[\prime,Q]{u'_Q} x'^{,+}_Q$ in X_Q with $x'_Q \in X'_{Q,0}$;*
- *$U_Q = \{u_Q\}$, where u_Q is a dummy input;*
- *$\xrightarrow[Q]{}$ is the collection of transitions*

$$\left(x^1_Q \xrightarrow[\prime,Q]{u'_Q} x^2_Q\right) \xrightarrow[Q]{u_Q} \left(x^3_Q \xrightarrow[\prime,Q]{u'_Q} x^4_Q\right)$$

  with $x^2_Q = x^3_Q$;
- *$X_{Q,m}$ is the collection of states $x'_Q \xrightarrow[\prime,Q]{u'_Q} x'^{,+}_Q$ in X_Q with $x'^{,+}_Q \in X'_{Q,m}$;*
- *$H_Q(x'_Q \xrightarrow[\prime,Q]{u'_Q} x'^{,+}_Q) = u'_Q$ for any state $x'_Q \xrightarrow[\prime,Q]{u'_Q} x'^{,+}_Q$ in X_Q.*

The construction above, when specialized from transition systems to Finite State Automata (FSA), coincides with the construction of dual FSA proposed in [3]. From the definitions above, it is readily seen that

$$\mathcal{L}^y(S_Q) = \mathcal{L}^u(S'_Q), \quad \mathcal{L}^y_m(S_Q) = \mathcal{L}^u_m(S'_Q) = L_Q.$$

Moreover, S_Q is symbolic, accessible and nonblocking. In the sequel and for ease of notation, we denote a state $x'_Q \xrightarrow[\prime,Q]{u'_Q} x'^{,+}_Q$ of X_Q by x_Q and a transition

$x_Q \xrightarrow[Q]{u_Q} x_Q^+$ of S_Q by $x_Q \xrightarrow[Q]{} x_Q^+$.

Example 1. (Continued.) The dual transition system S_Q of transition system S'_Q in Fig. 2 is reported in Fig. 3. It is easy to see that S_Q is symbolic, accessible and nonblocking.

Consider

$$\mathcal{I} : (\xrightarrow[Q]{}) \times \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \{\texttt{True}, \texttt{False}\}.$$

For any transition $x_Q \xrightarrow[Q]{} x_Q^+$ of transition system S_Q set

$$\mathcal{I}(x_Q \xrightarrow[Q]{} x_Q^+, \tau, \eta) = \texttt{True}, \tag{11}$$

if there exists $u \in \mathbf{U}$ such that

$$[H_Q(x_Q)]_\eta^n \xrightarrow[\tau,\eta]{u} [H_Q(x_Q^+)]_\eta^n, \tag{12}$$

and $\mathcal{I}(x_Q \xrightarrow[Q]{} x_Q^+, \tau, \eta) = \texttt{False}$, otherwise. Hence, $\mathcal{I}(x_Q \xrightarrow[Q]{} x_Q^+, \tau, \eta)$ is True, if the transition $x_Q \xrightarrow[Q]{} x_Q^+$ of S_Q can be matched by transition system $T_{\tau,\eta}(\Sigma)$ and False, otherwise.
Define the subsystem

$$S_{Q,\eta}^c = (X_Q^c, X_Q^{0,c}, U_Q^c, \xrightarrow[Q,\eta,c]{}, X_{Q,m,c}, Y_Q^c, H_Q^c), \tag{13}$$

of S_Q, where $\xrightarrow[Q,\eta,c]{} \subseteq \xrightarrow[Q]{}$ contains all and only transitions $x_Q \xrightarrow[Q]{} x_Q^+$ of S_Q satisfying (11). Transition system $S_{Q,\eta}^c$ is blocking in general. For this reason we define

$$\mathrm{Trim}(S_{Q,\eta}^c) = (X_{\mathrm{T}}, X_{\mathrm{T},0}, U_{\mathrm{T}}, \xrightarrow[\mathrm{T}]{}, X_{\mathrm{T},m}, Y_{\mathrm{T}}, H_{\mathrm{T}}) \tag{14}$$

that is by definition of Trim, accessible and co–accessible and hence, nonblocking.
In the sequel we make the following

Assumption 1 *Transition system* $\mathrm{Trim}(S_{Q,\eta}^c)$ *is not empty.*

Define the following set:

$$\mathbf{X}_0 = \mathcal{R}_\mu^{-1}([H_{\mathrm{T}}(X_{\mathrm{T},0})]_\eta^n\}). \tag{15}$$

Entities defining controller C in (4) are then specified by:

$$\begin{array}{l} X_c^0 = X_{\mathrm{T},0}, \\ X_c = X_{\mathrm{T}}, \\ f_c(x_{\mathrm{T}}) = \{x_{\mathrm{T}}^+ \in X_{\mathrm{T}} | \exists x_{\mathrm{T}} \xrightarrow[\mathrm{T}]{} x_{\mathrm{T}}^+\}, \\ h_c(x_{\mathrm{T}}) = \left\{ \begin{array}{c} u \in \mathbf{U} | \exists x_{\mathrm{T}}^+ \in f_c(x_{\mathrm{T}}) \text{ s.t.} \\ [H_{\mathrm{T}}(x_{\mathrm{T}})]_\eta^n \xrightarrow[\tau,\eta]{u} [H_{\mathrm{T}}(x_{\mathrm{T}}^+)]_\eta^n \end{array} \right\}. \end{array} \tag{16}$$

The following result holds.

Theorem 2. *Consider control system Σ and suppose it admits a δ–GAS Lyapunov function V and hence, satisfying conditions of Definition 5 in lecture L6, for some $\kappa \in \mathbb{R}^+$ and $\mathcal{K}_\infty$ functions α_1 and α_2 and the inequality (6) for some $\mathcal{K}_\infty$ function γ. For any desired accuracy $\theta \in \mathbb{R}^+$ and sampling time $\tau \in \mathbb{R}^+$ select $\mu \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$ satisfying (7) and*

$$\mu + \eta/2 \leq \theta. \tag{17}$$

Suppose that Assumption 1 holds. Then, set $\mathbf{X}_0$ in (15) and controller C in (4) specified by (16) solve Problem 1.

The proof of the result above can be found, for discrete–time nonlinear systems in [5].

Remark 1. (*The completeness property*) We point out that Assumption 1 is not limiting in the sense that if

$$\text{Trim}(S^c_{Q,\eta}) = \varnothing,$$

then, the notion of approximate bisimulation we consider guarantees that the so-called "completeness property" in the control, in an approximating sense: if a solution exists to our control problem, then such a solution can be found by using our approach, within some accuracy.

References

1. C.G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, 1999.
2. Dan Caugherty. JFLAP: An interactive formal languages and automata package, 1990. Available online at http://www.jflap.org/.
3. E.A. Gol, M. Lazar, and C. Belta. Language–guided controller synthesis for linear systems. *IEEE Transactions of Automatic Control*, 59(5):1163–1176, May 2014.
4. M.V. Lawson. *Finite Automata*. CRC Press, 2004.
5. G. Pola, P. Pepe, and M. D. Di Benedetto. Decentralized approximate supervisory control of networks of nonlinear control systems. *IEEE Transactions on Automatic Control*, 2017. Submitted for publication. Available online at arxiv.org/abs/1606.04647 [math.OC].
6. M. Zamani, M. Mazo, G. Pola, and P. Tabuada. Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions of Automatic Control*, 57(7):1804–1809, July 2012.