Control of Cyber-Physical Systems with Logic Specifications

Giordano Pola
DISIM - DEWS
University of L’Aquila (Italy)

Piazza Duomo, L’Aquila, Italy

giordano.pola@univaq.it
Cyber-Physical Systems (CPS) are physical, biological and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core.
Critical aspects of CPS

- **Heterogeneity**: plants, controllers and specifications described in different mathematical frameworks
- **Non-ideal communication infrastructure**: control action delivered with delay on the basis of delayed and corrupted measure of the states of the plants, lack of information (packet drops), etc.
- **Complexity**: large number of possibly distributed sub-systems
- **Logic specifications**
- …
A three phases process:
#1. Construct the finite/symbolic model $T$ approximating the plant system $P$
#2. Design a finite/symbolic controller $C$ that solves the specification $S$ for $T$
#3. Refine the controller $C$ to the controller $C'$ to be applied to $P$

Advantages:
- Integration of software and hardware constraints in the control design of purely continuous or hybrid processes
- Relevant logic specifications can be addressed
Plant and controller

- **Plant:**

\[ P: \begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ x(t) \in \mathbb{R}^n, u(t) \in U \subset \mathbb{R}^m \end{cases} \]

- \( U \) finite set
- \( x(t, x_0, u) \) state reached at time \( t \) with initial state \( x_0 \) and control input \( u \)

- **Controller C: Finite State Machine**

  ![Finite State Machine Diagram]

  - Inputs of C: quantized measurements of the state of \( P \)
  - Outputs of C: control signal \( v(k) \) to be inferred to the plant \( P \)

- **Controlled plant** \( P^C \) obtained by coupling dynamics of \( P \) and \( C \) with \( \text{ZoH}: \{ u(t) = v(k), \forall t \in [k\tau, (k+1)\tau], k \in \mathbb{N} \} \)

  - \( \tau > 0 \) sampling time
Logic specifications: Regular languages

Recall
- Let Y be a finite set representing an alphabet
- A word over Y is a finite sequence with symbols in Y
- A language L over Y is a collection of words in Y

Definition
A language is regular if it can be represented by a Finite State Automaton (FSA)

Example
Y = \{ a, b \}
L = all words over Y starting with symbol a and ending with symbol b
L is regular because of existence of FSA:
Logic specifications: Regular languages

Alphabet: collection $Y$ of left-closed right-open hyper-cubes $Y_i$ of $\mathbb{R}^n$

$$Y_i = c_i + \prod_{i=1}^{n} [-\eta, \eta]$$

$$c_i \in 2\eta \mathbb{Z}^n$$

$Y$ is a partition of $\mathbb{R}^n$

We consider a specification expressed as a regular language $L_Q$ over $Y$

Specifications for CPS handled via regular language formalism:
- Reachability
- Controlled invariance in finite time horizon
- Obstacle avoidance in finite time horizon
- Motion planning
- Enforcing periodic orbits
- State-based switching specifications
- ...
Given
- the plant $P$
- a sampling time $\tau > 0$
- a regular language specification $L_Q$
- a desired accuracy $\theta > 0$

Find
- a controller $C$ with set of initial states $X_{c,0}$
- a relation of initial states $R_0 \subseteq \mathbb{R}^n \times X_{c,0}$ of $P^C$

such that the controlled plant $P^C$ satisfies the specification $L_Q$ up to the accuracy $\theta$, i.e.

for any trajectory $x(.)$ of $P^C$ with $(x(0), x_c(0)) \in R_0$, there exists a word $q_0 q_1 \ldots q_{k_f}$ of $L_Q$ such that

$$||x(k\tau) - q_k|| \leq \theta, \forall k \in [0; k_f]$$

Approximate equivalence notions

Time-delay systems

Introduction
Key assumptions on the plant P

**Definition [Angeli, TAC-2002]**
Plant $P$ is incrementally globally asymptotically stable ($\delta$-GAS) if there exists a $\mathcal{KL}$ function $\beta: \mathbb{R}^+_0 \times \mathbb{R}^+_0 \to \mathbb{R}^+$ such that for any $t \geq 0$, any initial conditions $x, x'$ and any input $u$

$$\|x(t, x, u) - x(t, x', u)\| \leq \beta(\|x - x'\|, t)$$

**Remark** $\delta$-GAS can be checked by using Lyapunov-like inequalities
Key assumptions on the plant $P$

**Definition [Zamani et al., TAC-2012]**

Plant $P$ is incrementally forward complete ($\delta$-FC) if there exists a continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}^+$ such that for every $s \in \mathbb{R}^+$, function $\beta(., s)$ belongs to class $\mathcal{K}_\infty$ and for any $x, x' \in \mathbb{R}^n$ and any $u$

$$\|x(t, x, u) - x(t, x', u)\| \leq \beta(\|x - x'\|, t)$$

**Remarks**

- Any (possibly unstable) linear system is $\delta$-FC
- $\delta$-FC can be checked by using Lyapunov-like inequalities
- $\delta$-GAS implies $\delta$-FC while the converse is not true
Contribution
For $\delta$-FC (and hence $\delta$-GAS) plants, we designed algorithms solving the control problem for any desired sampling time $\tau > 0$ and accuracy $\theta > 0$

Remarks
- Symbolic model $T$ of $P$ obtained by time and state space discretization of $P$
- If $P$ is $\delta$-GAS then $T$ is an approximate bisimulation [5] of time discretization of $P$
- If $P$ is $\delta$-FC then $T$ is an alternating approximate simulation [4] by time discretization of $P$
- Design of controllers inspired by supervisory control algorithms
- The «completeness property»: If $P$ is $\delta$-GAS then a control strategy enforces a given specification on $P$ if and only if it can be found on $T$ (guaranteed by approximate bisimulation)

Based on:
Including more features of CPS

- **Stable nonlinear switched systems**
  TOOLS: $\delta$-UGAS and its check through common and multiple Lyapunov functions with Antoine Girard and Paulo Tabuada

- **Stable nonlinear control systems with disturbance inputs**
  TOOLS: $\delta$-ISS, alternating approximate bisimulation and spline analysis with Paulo Tabuada, Alessandro Borri and Maria Domenica Di Benedetto

- **Stable nonlinear time-delay systems**
  TOOLS: $\delta$-ISS, $\delta$-IDSS, alternating approximate bisimulation and spline analysis with Pierdomenico Pepe and Maria Domenica Di Benedetto

- **Networked control systems**
  TOOLS: strong alternating approximate simulation and bisimulation with Alessandro Borri and Maria Domenica Di Benedetto

- **Decentralized supervisory control**
  TOOLS: extensions of supervisory control to concurrent settings with Pierdomenico Pepe and Maria Domenica Di Benedetto

- **Control design of stable nonlinear systems with outputs**
  TOOLS: $\delta$-GAS, approximate bisimulation with Maria Domenica Di Benedetto and Alessandro Borri
Networked control systems

Nonidealities considered:

- Quantization errors
- Bounded time-varying network access times
- Bounded time-varying communication delays induced by the network
- Limited bandwidth
- Bounded packet losses
- Bounded time-varying computation time of computing units
We proposed an approach based on formal methods for the control of CPS with logic specifications

Future work: Design of efficient control algorithms and their software implementation

Thanks!
References on formal methods for the control of CPS

5. [Pola et al., TAC18] Pola, G., Pepe, P, Di Benedetto, M.D., Decentralized Approximate Supervisory Control of Networks of Nonlinear Control Systems, IEEE Transactions on Automatic Control, 63(9):2803-2817, September 2018
18. [Borri et al., NECSYS13] Borri, A., Dimarogonas, D.V., Johansson, K.H., Di Benedetto, M.D., Pola, G., Decentralized symbolic control of interconnected systems with application to vehicle platooning, 4th IFAC Workshop on Distributed Estimation and Control in Networked Systems, Koblenz, Germany, September 2013, pp. 285-292