Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Basilica di Santa Maria di Collemaggio, L’Aquila (Italy), 1287

Lecture L15: Conclusions

Speaker: Giordano Pola
We considered a fairly general model of CPSoS
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 systems composed of several, possibly distributed sub-systems

Logic specifications
The approach we took …

... a complementary approach:

- Single plants with no disturbances and delays
- Control design with logic specifications
- Efficient algorithms for control design
- Single plants with disturbances
- Single plants with delays
- Single, possibly unstable, plants
- Single plant, controller and communication infrastructure
- Decentralized control of networks of control systems with 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 processes
- Logic specifications can be addressed
Advantages of the approach

- Correct-by-design approach handling nonidealities of CPSoS
- Systematic approach to enforce logic specifications
- The «completeness property»
  - A control strategy enforcing a (logic) specification on one system exists if and only if it exists on a bisimilar one
  - If the system is incrementally stable then an approximated bisimilar symbolic model can be effectively constructed
  - Example 1 in Lecture L6a shows that unstable linear systems do not admit approximated bisimilar symbolic models
- Incremental forward completeness
  - Mild assumption: at present there is no example of a FC nonlinear system that is not δ-FC!
  - Since symbolic models obtained are in simulation (and not bisimulation) with the original model, here the completeness property is lost in general
Disadvantages of the approach: Computational complexity!

Approaches to tame complexity:

Methodological approaches:
- On-the-fly algorithms
  Example in L7b with s.c.c. gain 57491 and t.c.c. gain 419!
- Decentralized control architectures
  Example in L13 with t.c.c. gain 1046!
- Multi-resolution approaches (see e.g. [Girard et al., TAC16])
- ...

Software tools:
- PESSOA (use of BDD)
  Example in L11 where construction of symbolic model of 34020088 transitions + control (without on-the-fly techniques) in 536s!
- SCOTS (performs even better than PESSOA!)
- ...

Dedicated computing architectures:
- Parallel computing (not explored yet!)
- ...

s.c.c. = space computational complexity
t.c.c. = time computational complexity
Control of CPSoS with an inter-disciplinary approach …

Methods from:

- **Control theory**
  nonlinear and time delay-systems, incremental stability, …

- **Discrete-event systems**
  regular languages, operators on automata, …

- **Theoretical computer science**
  bisimulation theory and its variants, …

- **Mathematics**
  approximation of functional spaces, …

- **Telecommunication**
  modeling of nonideal communication infrastructures, …
Some advanced methods used from control theory

Hierarchy of stability notions for nonlinear (and time-delay) systems

\[ \delta\text{-IDSS} \implies \delta\text{-ISS} \implies \delta\text{-GAS} \implies \delta\text{-FC} \]

\[ \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \]

\[ \text{IDSS} \implies \text{ISS} \implies \text{GAS} \implies \text{FC} \]
Some additional topics on Formal Methods @ UNIVAQ

- **Control of PWA systems with logic specifications**
  by G Pola and M D Di Benedetto
  - Pola, Di Benedetto, Sequences of Discrete Abstractions for Piecewise Affine Systems, ADHS-2012

- **Approximate diagnosability for metric and nonlinear control systems**
  by G Pola, M D Di Benedetto and Elena De Santis (UNIVAQ)
  - Pola, De Santis, Di Benedetto, Approximate diagnosability of metric transition systems, SEFM-2017, accepted

- **Stochastic equivalences and control for linear and descriptor systems**
  by G Pola, M D Di Benedetto, Costanzo Manes (UNIVAQ) and Arjan J. van der Schaft (Univ. of Groningen, NL)
  - Pola, Manes, van der Schaft, Di Benedetto, Equivalence notions for discrete-time stochastic linear control systems, TAC-2017, provisionally accepted as Paper
  - Pola, Manes, Di Benedetto, On external behavior equivalence of continuous–time stochastic linear control systems, CDC-2016
  - Pola, Manes, van der Schaft, Di Benedetto, Model reduction of continuous–time stochastic linear control systems via bisimulation equivalence, CDC-2016

- …
Future directions

Methodological issues

- Stochastic CPSoS
- Co-design of control algorithms with communication infrastructures
- Software tools
- ...

Application domains

- Autonomous vehicle control with nonideal communication infrastructures
- Other applications: Micro-grid, Systems biology, ...
- ...

International collaborations on formal methods

- Paulo Tabuada, UCLA (USA)
- Antoine Girard, CNRS (France)
- Karl Henrik Johansson, KTH (Sweden)
- Majid Zamani, University of Munchen (Germany)
- Manuel Mazo, TUDelft (The Netherlands)
- Dimos Dimarogonas, KTH (Sweden)
References on formal methods for the control of CPSoS @ UNIVAQ

17. [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
22. [Pola et al., IFACWC11] Pola, G., Di Benedetto, M.D., De Santis, E., A Compositional Approach to Bisimulation of Arenas of Finite State Machines, 18th IFAC World Congress, Milan, Italy, August-September 2011, pp. 7006-7011
24. [Borri et al., CDC10] Borri, A., Pola, G., Di Benedetto, M.D., An integrated approach to the symbolic control design of nonlinear systems with infinite states specifications, 49th IEEE Conference on Decision and Control, Atlanta, Georgia, USA, December 2010, pp. 1528-1533
27. [Pola et al., CDC08] Pola, G., Tabuada, P., Symbolic models for nonlinear control systems affected by disturbances, 47th IEEE Conference on Decision and Control, Cancun, Mexico, December 2008, pp. 251-256