Taming Delays in Cyber-Physical Systems [⋆]

Naijun Zhan

State Key Lab. of Comput. Sci., Institute of Software, CAS
znj@ios.ac.cn

Extended Abstract

Historical motivation (predating digital control):

> *"Despite [...] very satisfactory state of affairs as far as [ordinary] differential equations are concerned, we are nevertheless forced to turn to the study of more complex equations. Detailed studies of the real world impel us, albeit reluctantly, to take account of the fact that the rate of change of physical systems depends not only on their present state, but also on their past history."*
>
> [Richard Bellman and Kenneth L. Cooke, 1963, see [1]]

Conventional embedded systems have over the past two decades vividly evolved into an open, interconnected form that integrates capabilities of computing, communication and control, thereby triggering yet another round of global revolution of the information technology. This form, now known as cyber-physical systems (CPS), has witnessed an increasing number of safety-critical systems particularly in major scientific projects vital to people's livelihood. Prominent examples include automotive electronics, health care, nuclear reactors, high-speed trains, aircrafts, spacecrafts, etc., in which a malfunction of any software or hardware component would potentially lead to catastrophic consequences. Meanwhile with the rapid development of feedback control, sensor techniques and computer control, time delays have become an essential feature underlying both the continuous evolution of physical plants and the discrete transition of computer programs, which may well annihilate the stability/safety certificate and control performance of embedded systems. Traditional engineering methods, e.g., testing and simulations, are nevertheless argued insufficient for the zero-tolerance of failures incurred in time-delayed systems in a safety-critical context. Therefore, how to rigorously verify and design reliable safety-critical embedded systems involving delays tends to be a grand challenge in computer science and the control community.

In contrast to delay-free systems, time-delayed systems yield substantially higher theoretical complexity thus rendering the underlying design and verification tasks exceedingly harder, e.g., unlike Ordinary Differential Equations (ODEs) being Markovian process, Delay Differential Equations (DDEs) turn

[⋆] This work is partly funded by NSFC under grant No. 61625206 and 61732001.

out to be non-Markovian, heavily depending on their execution histories, and consequently any solution to a DDE is an infinite dimensional functional, rather than a point in the n-dimensional Hilbert space like ODE's. The major problems that we faced include the formal verification and controller synthesis of time-delayed, networked hybrid systems.

Though time delays have been extensively studied in the literature of mathematics and control theory from a qualitative perspective, automatic verification and synthesis methods addressing feedback delays in hybrid discrete-continuous systems are still in their infancy. In this extended abstract, we summarize our recent efforts towards the above issues, including

- Firstly, we will discuss how to synthesize controllers for time-delayed discrete systems, based on the work in [3]. The basic idea is to reduce the controller synthesis problem to a two-player delay safety game, further to a two-player delay-free safety game with memory. Based on the reduction, an efficient incremental synthesis algorithm is presented. According to the work in [4], we further discuss generalized settings of controller synthesis where messages may arrive out of order or even get lost, and show –on top of the incremental synthesis– the equivalence of qualitative controllability over these settings.
- Then, we discuss bounded reachability analysis of DDEs, mainly focusing on two approaches: the first one is to extend the technique of *simulation* plus *sensitivity analysis* for ODEs [6] to DDEs [2]; the other is to extend the set-boundary reachability analysis methods for ODEs [8] to DDEs [7].
- Finally, we discuss unbounded verification of DDEs, mainly focusing on the following two approaches: the first one is to deal with DDEs of the form

  $$\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{x}(t) = f(\boldsymbol{x}(t-\delta))$$

  by exploiting *interval Taylor models* and *stability analysis*. The basic idea can be sketched as follows:
  1. predefine a parametric interval polynomial containing all possible solutions of the DDE on the given segment,
  2. derive an operator between the paramenters of the solution on the previous segment and the ones on the next segment, forming a time-invariant discrete dynamical system,
  3. exploit the stability analysis of the resulted time-invariant dynamical system, thus reducing the safety verification and stability analysis to bounded cases.

  The detail can be found in [9]; the other approach is to deal with the general DDEs of the form

  $$\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{x}(t) = f(\boldsymbol{x}(t), \boldsymbol{x}(t-\delta_1), \ldots, \boldsymbol{x}(t-\delta_n))$$

  by using *linearisation* and *spectral analysis*. The reader can refer to [5] for the detail. The basic idea can be sketched as follows:
  1. linearise a non-linear DDE,

2. exploit spectral analysis to obtain the stability of the linear part,
3. reduce unbounded verification and analysis to bounded case.

Finally, we will also discuss trends and challenges in the formal verification and synthesis of time-delayed systems.

Acknowledgements

First of all, I thank Mingshuai Chen and Bai Xue for their useful comments on the early version of the manuscript which improve the presentation so much.

I would like to take this opportunity to thank all collaborators involved in this research, including Martin Fränzle, Bai Xue, Liang Zou, Mingshuai Chen, Peter Nazier Mosaad, Yangjia Li, Shenghua Feng, etc.

References

1. Richard Bellman and Kenneth L. Cooke. Differential-difference equations. Technical Report R-374-PR, The RAND Corporation, Santa Monica, California, January 1963.
2. Mingshuai Chen, Martin Fränzle, Yangjia Li, Peter Nazier Mosaad, and Naijun Zhan. Validated simulation-based verification of delayed differential dynamics. In *FM'16*, volume 9995 of *Lecture Notes in Computer Science*, pages 137–154, 2016.
3. Mingshuai Chen, Martin Fränzle, Yangjia Li, Peter Nazier Mosaad, and Naijun Zhan. What's to come is still unsure - synthesizing controllers resilient to delayed interaction. In *ATVA'18*, volume 11138 of *Lecture Notes in Computer Science*, pages 56–74, 2018.
4. Mingshuai Chen, Martin Fränzle, Yangjia Li, Peter Nazier Mosaad, and Naijun Zhan. Indecision and delays are the parents of failure: Taming them algorithmically by synthesizing delay-resilient control. *Acta Informatica*, 2019. Under minor revision.
5. Shenghua Feng, Mingshuai Chen, Naijun Zhan, Martin Fränzle, and Bai Xue. Taming delays in dynamical systems: Unbounded verification of delay differential equations. In *CAV'19*, volume 11561 of *Lecture Notes in Computer Science*, pages 650–669, 2019.
6. Tarik Nahhal and Thao Dang. Test coverage for continuous and hybrid systems. In *CAV'07*, volume 4590 of *Lecture Notes in Computer Science*, pages 449–462. Springer, 2007.
7. Bai Xue, Peter Nazier Mosaad, Martin Fränzle, Mingshuai Chen, Yangjia Li, and Naijun Zhan. Safe over- and under-approximation of reachable sets for delay differential equations. In *FORMATS'17*, volume 10419 of *Lecture Notes in Computer Science*, pages 281–299, 2017.
8. Bai Xue, Zhikun She, and Arvind Easwaran. Under-approximating backward reachable sets by polytopes. In *CAV'16*, volume 9779 of *Lecture Notes in Computer Science*, pages 457–476, 2016.
9. Liang Zou, Martin Fränzle, Naijun Zhan, and Peter Nazier Mosaad. Automatic verification of stability and safety for delay differential equations. In *CAV'15*, volume 9207 of *Lecture Notes in Computer Science*, pages 338–355, 2015.