International Symposium on Mathematical Theory of Networks and Systems

Mini-Course Proposal

Automated Verification and Synthesis of Complex Systems

Organizers: **Majid Zamani**[1], **Ilya Tkachev**[2], **Manuel Mazo**[2], and **Alessandro Abate**[3]

[1]Design Engineering Department
[2]Delft Center for Systems and Control
Delft University of Technology
{m.zamani,i.tkachev,m.mazo}@tudelft.nl

[3]Department of Computer Science
University of Oxford
alessandro.abate@cs.ox.ac.uk

February 27, 2014

Motivation

The use of concepts, techniques, and algorithms originated in the literature on *Formal Verification* in Computer Science has recently become common within the Systems & Control community. Formal notions which are fundamental in Computer Science, such as symbolic (finite) abstraction, or bisimulation relation, are increasing their presence in the study of continuous dynamical and control systems thanks to their ability to provide algorithmic solutions for complex problems. Moreover, such notions provide new insights into similar concepts already employed in Systems & Control theory: e.g. the notion of abstraction is strongly related to that of model reduction for continuous dynamical systems.

The process of constructing abstractions consists of mapping a complex system with (possibly infinitely) many states into a simpler (e.g. finite) one, called the abstract model, which is easier to study. This procedure is often formalized by means of establishing (bi)simulation relations between the new abstract model and the original one. The construction of finite abstractions of infinite state systems, like traditional control systems described by differential equations, enables the use of mature techniques available in the Computer Science literature. As a result, these abstractions make possible to leverage automated control synthesis and verification algorithms, developed for finite systems, to problems over infinite (stochastic) hybrid systems. Examples of specifications

that can be verified or enforced in this way include: reachability, safety, and more complex properties expressed as formulas in linear temporal logic (LTL) or as automata on infinite strings.

Being particularly suited to the analysis and design of hybrid systems, the described methods are particularly relevant to address problems over cyber-physical systems (CPS): i.e. systems in which discrete computing devices interact with the continuous physical world. These novel techniques can solve many complex problems that until recently could not be addressed in a formal methodological way using classical approaches, such as satisfaction of logic specifications for (stochastic) hybrid systems. Furthermore, these approaches have demonstrated their practical relevance with many available model checkers and synthesis tools expecting to grow from being exclusively of academic interest to becoming industrially relevant techniques.

Objectives of the Mini-Course

The objectives of this mini-course is to introduce the participants to the topics of correct-by-design synthesis and verification of embedded control software using the methods introduced in the previous section. The main objectives are:

- Make participants new to the topic familiar with relevant concepts and techniques in computer science such as: temporal logics, automata, simulation relations, safety/reachability games, etc.
- Introduce abstraction techniques to construct finite-state models of infinite (stochastic) hybrid systems.
- Introduce algorithmic techniques to automatically synthesize hybrid controllers satisfying some specifications of interest.
- Illustrate the introduced concepts on the MATLAB-based toolbox Pessoa and on a newly developed toolbox for stochastic hybrid systems.
- Exhibit the audience to new directions and areas in formal methods with applications in control.
- Suggest novel applications of the discussed formal techniques.

Additionally, we hope that the active discussions with the participants will lead to fruitful interactions.

Themes of the Mini-Course

The structure of the mini-course is illustrated in Table 1. In the first talk of the mini-course (25 minutes), we provide an introduction on CPS and the necessity of novel techniques for their analysis and design. Moreover, a unified framework is provided to model discrete computing devices, physical plants, as well as their interactions. In the second talk of the mini-course (25 minutes), we briefly explain complex logic specifications relevant to study CPS and the ways to enforce them over CPS. In the third and fourth talks of the mini-course

Speakers	Titles of the talks
Manuel Mazo Jr	Formal verification and synthesis of cyber-physical systems: An automated approach
Alessandro Abate	Complex specifications for cyber-physical systems
Majid Zamani	Discrete abstractions of non-probabilistic complex systems
Ilya Tkachev	Discrete abstractions of stochastic complex systems
Manuel Mazo Jr & Alessandro Abate	Tools tutorials, open problems, and future challenges

Table 1: Structure of the mini-course.

(25 minutes each), we overview some existing discrete synthesis techniques providing abstractions for (stochastic) CPS. In the last talk of the mini-course (25 minutes), we illustrate the covered concepts on some developed tools such as Pessoa and conclude the course by providing some open problems and future directions.