automatic verification and synthesis of complex systems

lecturers

Dr. Mazo Jr., Delft University of Technology
Dr. A. Abate, University of Oxford

objective

The use of concepts, techniques, and algorithms originated in the literature on Formal Verification in the Computer Sciences has recently become common and successful within the Systems & Control community. Known formal notions that are fundamental in Computer Science, such as that of symbolic (finite) abstraction, or that of bisimulation relation, are increasing their presence in the study of continuous dynamical and control systems, thanks to their ability to provide formal and algorithmic solutions to complex analysis and controller synthesis problems. Their use is particularly cogent in the area of Cyber-Physical Systems, where physical models share dynamics, control, and computational aspects. The use of techniques from formal methods thus targets two goals: formal analysis and synthesis, as well as computational solutions.

This course aims are providing an introduction to the area, and to lead the student to appreciate the most modern developments in this research field. The course is inter- disciplinary and could likewise target a systems and control audience, as well as a computer science audience open to learn about dynamical and control models and problems.

More specifically, the goals of the course are:

- To establish a sufficiently strong common ground to enable entering the inter-disciplinary research field of Verification and Control of complex systems employing symbolic methods.
- To illustrate the relevance of these new techniques in the design of embedded controllers, and in the analysis of safety requirements.
- To provide the students with a new set of tools to solve complex practical control problems, relying on recent theoretical achievements as well as modern software tools. By taking the course, the student will learn:
- To model a cyber-physical system via complex models such as hybrid or networked models, with possible non-determinism and stochasticity.
- To appreciate the power of formal verification and controller synthesis approaches, based on notions of equivalence or abstraction, and relying on computational symbolic algorithms.
- To verify a complex dynamical model over rich specifications expressed in known logical frameworks or computational structures.
- To synthesise digital controllers over physical models by the aforementioned techniques and software.

- To run dedicated modern software tools in the area, inclusive abstraction tools (see below) and model checkers in the industrial practice.

contents

The course is structured into four lectures. The content of the four sessions cover the following topics:
(1) Introduction to problems of Verification and Control in a generalised setting. Models – notion of general transition systems (as special examples, discussions of finite- state machines, ODEs, hybrid
systems). Determinism and non-determinism. Properties – modal and temporal logics, specifications, automata (examples in safety, liveness, reachability). Automatic verification of specifications over systems: reachability, safety, model checking.
(2) Shortcomings of classical analysis of complex models – the need for formal abstractions. Model abstractions – notions of equivalences and preorders: bisimulation and simulation relations. Approximate notions of abstractions. Metrics over models. Refinements.
(3) Non-determinism vs structural uncertainty: motivating probabilistic models – from Markov Chains to Stochastic Hybrid Systems. Stochastic counterparts of the notions and relations discussed in session 1 and 2.
(4) Overview of Software tools for abstraction, verification, and controller synthesis. Verification via reachability. Verification via model checking. Case studies.
Presentation of the final course assignment.

prerequisites

Undergraduate courses on systems and control over the state space. Familiarity with MATLAB and, in general, basic programming notions would be helpful for the final assign- ment of the course. Mathematical maturity, as well as a genuine interest to bridge between two scientific areas (systems & control, and formal methods).

course material

- P. Tabuada, Verification and Control of Hybrid Systems, Springer, 2009 (Selected chapters, available on line under institutional subscription)
- C.Baier and J-P. Katoen, Principles of Model Checking, MIT Press, 2008 (Selected chapters)
- Lectures notes, handouts, and homework material, to be distributed during the course.
- Software for formal verification and synthesis:

– PESSOA, https://sites.google.com/a/cyphylab.ee.ucla.edu/pessoa/
– FAUST2, http://sourceforge.net/projects/faust2/

homework assignments

There would be two homework assignments, each of which would amount to 15% of the final grade and will be aligned with the content of the first three sessions. The remaining 70% would come from a final computer-based assignment, in which the students synthesize or verify a simple control system with existing software packages discussed in the fourth session.