A Workshop on Robustness, Abstractions and Computations

Eric Feron * Patrick Cousot †

Sunday March 28, 2004,
University of Pennsylvania, Philadelphia, PA
Wu and Chen Auditorium, Levine Hall
8:30am – 5:00pm

The presentations made at the workshop are now available on-line at the following address:

`http://web.mit.edu/feron/Public/wkshop_pres/`

Abstract

A workshop devoted to the mathematical foundations of *Robustness, Abstractions and Computations* as well as their applications will be held at the University of Pennsylvania, March 28, 2004. This workshop will act as a forum to both identify and disseminate the existing technologies and mathematical results to a wide range of Engineering and Mathematical disciplines, and to identify the future research directions relevant to the promotion and use of computationally attractive abstractions.

*Department of Aeronautics and Astronautics, Laboratory for Information and Decision Systems, Room 33-213, Massachusetts Institute of Technology, Cambridge, MA 02139, `feron@mit.edu`

†Département de Mathématique et Informatique, Ecole Normale Supérieure, 45 rue d'Ulm, F-75230 Paris Cedex 05, France, `Patrick.Cousot@ens.fr`

background

Today's society is built upon highly complex infrastructures that bring to us many benefits, including cheap access to information, power and fast transportation. However, their complexity is ever increasing and their interconnections are often uncontrolled; these pose very serious challenges and quite possibly threats to our society as a whole. Large complex systems arise everywhere and include such cases as the Air Transportation System, the national road system, the internet, regional and national power systems, wireless communication networks and other largely distributed, networked services. Even traditional large-scale systems, such as cities, are progressively growing to gigantic and very complex proportions. Traditional engineered systems, such as aircraft engines, cars and computing devices also have grown tremendously in complexity through the introduction of real-time, embedded software systems aimed at better managing them.

Often these services and systems are supported by successive layers of software, whose goal is to achieve their efficient real-time regulation so as to make the entire system fail-safe, robust to uncertainties, expedient, clear and user-friendly. Many incidents and accidents have shown, however, that the complex engineered infrastructures that we witness today can undergo failures, and that the engineering community remains relatively vulnerable to these failures, because it does not always understand the nature and scope of the failures encountered and because it also lack the tools to analyze the *robustness* characteristics of these systems, or simply to prove that these systems work according to specifications.

As a consequence of these problems, many research efforts have been undertaken that aim at palliating this situation by developing new modeling environments aimed at supporting rigorous analysis of software and embedded systems. It is often seen that the traditional modeling paradigm, whereby nature is approximated by simple, exact mathematical expressions is often completely inapplicable to man-made, complex systems, either because such models would have to be extremely detailed, or because the new dominant factors in the evolution of such systems do not come from nature's laws but from rigidly imposed, man-made relations. This is for example the case of most networked services available today (transportation, power distribution, telecommunications etc.) Most, if not all, engineering disciplines have concluded that the new modeling paradigms, to be able to tackle new system complexity, must rely on hierarchical structures and must be able to approximate and simplify many of the often imprecisely known relations that link the individual elements of the system in a rigorous way. The lat-

ter issue has been found to be best handled via the use of *abstractions*, that is, complex interrelations are embedded into simply described *classes* of such interrelations. These classes are often described in simpler terms than the original interrelations and may lend themselves to easier, although admittedly more conservative analyses. Such abstractions have been widely promoted in Systems and Control theory, Software engineering, Axiomatic system design, Propulsion and aerodynamics, transportation systems. Often, the introduction of such abstract models of complex systems has been accompanied by the development of extremely efficient methods for analyzing, manipulating and designing such abstracted systems. Such methods include fixed-point iteration algorithms, optimal control, and mathematical programming.

Activities

Although there is no scarcity of conferences and symposia where some of the research aspects outlined above are discussed, a forum to discuss these aspects in a unified manner on a common ground is now necessary.

A 1-day workshop will be held on March 28, 2004, immediately following the 7th international workshop on hybrid systems: computation and control, to be held in Philadelphia, PA. Invited workshop participants will be given the opportunity to present their work and debating it with the other participants. The focus of the presentations will deliberately focus on the mathematical aspects of the methods and approaches of the participants.

Confirmed speakers include:

- Rajeev Alur, University of Pennsylvania. 'From Hybrid Models to Executable Software'
- Alexandre Bayen, Stanford University. 'Viability techniques to compute solutions to safety critical engineering problems'
- Patrick Cousot, Ecole Normale Supérieure, Paris. 'Abstract Interpretation of Computations'
- Eric Feron, MIT. 'Abstraction mechanisms across the board: A short introduction'
- Alexandre Megretski, MIT, 'Approximating Analog Systems by Finite State Automata'

- George Pappas, University of Pennsylvania. 'Bi-simulations : From exact to approximate'
- Pablo Parrillo, ETH Zurich. 'Sum of Squares (SOS) Relaxations for System Analysis: Possibilities and Perspectives'
- Jaime Peraire, MIT. 'Guaranteed bounds for the numerical solutions to a class of Partial Differential Equations'
- Claire Tomlin, Stanford University. 'Computational methods for hybrid system analysis and control'

Program:

8:30 - 9:00	Eric Feron
9:00 - 9:30	Patrick Cousot
9:30 - 10:00	Pablo Parrillo
10:00 - 10:30	Coffee Break and discussions
10:30 - 11:00	Alex Bayen
11:00 - 11:30	Jaime Peraire
11:30 - 12:00	Rajeev Alur
12:00 - 1:30	Lunch
1:30 - 2:00	Claire Tomlin
2:00 - 2:30	George Pappas
2:30 - 3:00	Alexandre Megretski
3:00 - 4:00	Open session - Impromptu presentations from audience
4:00 - 5:00	Group discussion
5:00	Adjourn

Abstracts (partial list)

Patrick Cousot, Ecole Normale Supérieure, Paris, 'Abstract Interpretation of Computations'

Following the exponential growth of hardware complexity, the current exponential expansion of software in all application domains, leads to the unfortunate situation where software engineers can build increasingly large software but are less and less confident in the quality of the software they build. Commercial software with more than one bug every thousand lines is not so uncommon. This situation is not tolerated in control/command systems involving large and complex real-time embedded safety critical software for which the development costs to achieve high-quality objectives are therefore rapidly becoming prohibitive. Because present-day engineering, which is almost exclusively manual, with very few automated tools, does not scale up, a grand challenge is therefore to develop knowledge, methods, technologies and tools to master software complexity. This means that one must be able to model the computations/executions of software in any possible environment (its so-called semantics) at various levels of abstraction. This is the purpose of abstract interpretation, a theory of the approximation of semantics aimed at supporting rigorous reasoning about software. Applications of abstract interpretation include proof methods as well as automatic software manipulation tools such as static analyzers. Static analyzers aim at proving properties of software execution using classes of conservative abstractions (that are simplifying approximations to cope with undecidability). The talk will introduce the basic elements of the theory of abstract interpretation and provide the example of ASTRÉE, a static analyzer developed at the École normale supérieure (`http://www.astree.ens.fr`) that was able to prove completely automatically the absence of any run-time error in the primary flight control software of the Airbus A340 fly-by-wire system, a world première.

Alexandre Megretski, MIT, 'Approximating Analog Systems by Finite State Automata'

Basic components of a robustness-based approach to designing finite alphabet feedback for analog systems are discussed, including approximation of analog systems by finite state automata, as well as analogs of the small gain theorem and H-Infinity design procedures.

Pablo Parrillo, ETH Zurich, 'SOS Relaxations for System Analysis: Possibilities and Perspectives'

We present an overview of the theory and applications of sum of squares (SOS) relaxations in system and robustness analysis. The developed techniques, based on convex optimization and results from real algebraic geometry, unify and generalize many well-known existing methods, such as those based on the S-procedure. The ideas and algorithms will be illustrated through examples, emphasizing recent developments as well as future challenges.

Claire J. Tomlin, Aeronautics and Astronautics Stanford University: 'Computational methods for hybrid system analysis and control'

In this talk, abstraction methods that we have designed to analyze hybrid systems will be presented. Emphasis will be placed on the algorithms and software that we are developing for efficient application of these methods. These algorithms are based on approximation techniques for hybrid systems reach set computations, using a derivative of predicate abstraction. The methods will be presented in the context of the 'reverse engineering' of biological cell networks. Joint work with Ronojoy Ghosh.