ISSN 2186-7437

NII Shonan Meeting Report

No. 2015-14

Validated Numerics Meets Reachability Analysis for CPS Design

Daisuke Ishii
Kohei Suenaga
Walid Taha

September 28–October 1, 2015

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Validated Numerics Meets Reachability Analysis for CPS Design

Organizers:
Daisuke Ishii, Tokyo Institute of Technology
Kohei Suenaga, Kyoto University
Walid Taha, Halmstad University

September 28th - October 1st, 2015

Abstract Cyber-Physical Systems (CPSs) consist of computers that are coupled tightly to a physical environment through sensors and actuators. Both the hybrid systems and the dynamics research communities have produced formal tools that are very important for rigorous design of CPSs, namely reachability analysis and validated numerics, respectively. Unfortunately, CPS designers encounter some challenges when using both tools. In particular, formal methods often have a steep learning curve that hampers their adoption in industrial practice. When a tool does not work immediately, a difficulty lies in what users can do with the tool, and with various restrictions in its implementation. Similarly, validated numerics methods today exist mainly in the form of specialized libraries that are only accessible to experts in this domain. The central motivation for this Shonan meeting is the prospect that carefully designed, declarative, high-level languages that are natural to the hybrid systems domain can help overcome these challenges. This meeting will bring together researchers working in these areas to better understand these challenges and to develop a common, coordinated vision for addressing them.

Overview

The purpose of this meeting is to bring together researchers in several fields to develop a coordinated roadmap for computational tools for Cyber-Physical Systems; this meeting will bridge the gap between the hybrid systems community and the validated numerics community. Although both have developed methods for rigorous reasoning about dynamical systems, both faced challenges in making their tools available to practicing engineering. The meeting will focus on two key challenges: scalability and usability. Cyber-Physical Systems (CPSs) consist of computers that are connected tightly to physical environments through sensors and actuators. Examples of CPSs include robots, smart homes, vehicles, medical implants, and sensor networks. Mathematically, we can view CPSs as hybrid systems that exhibit both continuous and discrete changes. Many CPSs are also subject to real-time and reactive

constraints. CPSs are an engineering, multidisciplinary area that is rapidly gaining wide acceptance and traction in scientific, social, political, and commercial circles.

Both the hybrid systems community and the validated numerics community have produced formal tools that are important for rigorous design of CPSs. Reachability analysis of hybrid systems was proposed by the first community as an extension of the model checking method in the context of verification involving continuous quantities. To handle reachable sets of real-valued states, the proposed tools either abstract them into a discrete representation or over-approximate them using numerical objects such as intervals and polytopes. Since the development of interval analysis in 1960's, validated numerics has been used by the second community to produce powerful tools for solving mathematical problems that are formally correct. The achievements include the interval Newton methods, interval Taylor methods, constraint programming techniques, and inner approximation methods. Unfortunately, CPS designers encounter some challenges when using both reachability analysis and validated numerics. In particular, formal methods often have a steep learning curve that hampers their adoption in industrial practice. It is therefore important to provide tool support for users that fills in gaps in the background knowledge of logic, algebra, real analysis, etc. In the context of reachability analysis of hybrid systems, tools, e.g., HyTech, Uppaal, SpaceEx, have been developed. However, users may still face difficulties in analyzing their problems with these tools. Because each tool depends on the underlying verification algorithm and the form in which hybrid systems are represented, these aspects restrict the tractable class and size of the problems. When a tool does not work immediately, a difficulty lies in what users can do with the tool and with various restrictions in its implementation such as linearity of arithmetic constraints, and support for the description of large systems. Similarly, validated numerics methods today exist mainly in the form of specialized libraries that are only accessible to experts in this domain. Although integration of the reachability analysis and validated numerics is necessary to push forward the rigorous CPS development, there is still an enormous gap between them.

The central motivation for this Shonan meeting is the prospect that tools based on carefully designed, declarative, high-level modeling formalisms that are natural to the hybrid systems domain can help overcome these challenges. Such tools allow us to describe models and verification problems in a straightforward manner that is more easily usable by practitioners, and the interpreters transform the model and extract underlying subproblems to which scalable validated numerical methods can be applied. However, designing such tools requires close interdisciplinary cooperation between experts not only in language design but also in hybrid systems, reachability analysis, validated numerics, and practitioners. It seems particularly important and timely to connect the research communities in a way that can be as widely applicable across as many CPS domains as possible. This meeting will bring together researchers working in these areas to better understand these challenges and to develop a common, coordinated vision for addressing them. Expected outcomes include a survey of the state of the art and a roadmap for bridging the gap between the communities.

The organizers will serve as scribes for introduction of the goals of the meeting, the presentations by participants from the above mentioned areas, and the development of a joint roadmap document. An organizer, Walid Taha, has founded several conferences and workshops, including ACM GPCE, SAIG Workshops, and CyPhy workshops on the domain

of CPSs. The PC of past CyPhy includes several invitees of this meeting. Another organizer, Kohei Suenaga, has contributed to a past successful Shonan meeting on hybrid systems.

Meeting Schedule

The primary goal of the meeting is to building connections between disciplines that have so far been relatively isolated, and that also have the potential to have significant impact on technological practice, especially in the area of cyber-physical systems. The meeting is planned in a way to encourage interaction between participants, and to provide concrete opportunities for collaboration both in the short term and the long term. Key outcomes of the meeting will include a) brief introductions to individual participants and their interests, b) collaboratively developed tutorials of particular importance to participants, and c) a roadmap for addressing the most important challenges that stand in the way of broader utility.

Table 1. Overview of the meeting schedule

<table>
<tr><th></th><th>9/27</th><th>9/28</th><th>9/29</th><th>9/30</th><th>10/1</th></tr>
<tr><td>9:00 - 9:30</td><td rowspan="8">Early check-in can be negotiated with organizers</td><td>Opening Session</td><td rowspan="2">S5 - Tutorials
- 30m+15 Q&A
- T1,T2,T3</td><td rowspan="2">S7 - Challenges (40m) and Milestones (35m)</td><td rowspan="2">S8 - Roadmap</td></tr>
<tr><td>9:30 - 10:15</td><td>S1 - Disciplines</td></tr>
<tr><td>10:15 - 10:45</td><td colspan="3">Break</td></tr>
<tr><td>10:45 - 12:00</td><td>S2 - Introductions</td><td>S5 - Tutorials</td><td>S7 - Strategies and Tactics (30m) & Timeline (30m)</td><td>Closing Session
- Action Plan
- Summary</td></tr>
<tr><td>12:00 - 1:30</td><td colspan="3">Lunch</td></tr>
<tr><td>1:45 - 2:00</td><td>Group photo</td><td></td><td></td><td rowspan="6"></td></tr>
<tr><td>2:00 - 2:45</td><td>S3 - Introductions</td><td>S5 - Tutorials
- T4</td><td rowspan="3">Excursion</td></tr>
<tr><td>2:45 - 3:15</td><td colspan="2">Break</td></tr>
<tr><td>3:15 - 5:00</td><td>Check-in</td><td rowspan="2">S4 - D-Groups</td><td>S5 - Tutorials
- T5, T6</td></tr>
<tr><td>5:00 - 6:00</td><td>S6 - Roadmap</td></tr>
<tr><td>6:00 - 7:30</td><td rowspan="2">Welcome Banquet</td><td colspan="2">Dinner</td><td>Banquet</td></tr>
<tr><td>7:30 - 9:00</td><td colspan="2" rowspan="2">Free Time
- Discussions in common areas
- 8PM: Demos in the lounge</td><td rowspan="2"></td></tr>
<tr><td>9:00 - 12:00</td><td>Free Time</td></tr>
</table>

September 28th, Monday

AM

- **9:00 - 9:30 Opening Session**
  - Welcome (1 minutes)

    - Pointing out the organizers for everyone (3 minutes)
    - Introducing the Shonan Village Center (10 minutes)
    - Explaining the goals of the meetings and expected outcomes (based on the proposal): (10 minutes)
        - Tutorial ("expository") surveys of the state of the art in different areas
            - We may want to make these into tutorial documents at the same time
        - Roadmap for bridging the gap between the disciplines
        - Shonan meeting report
- **9:30 - 10:15 Session 1** - Selecting Disciplinary topics, groups, and Interdisciplinary groups
    - Entire attendance brainstorming on topics to be informed about
        - Brainstorming research topics that we would like to be informed about (such as validated numerics (interval analysis, solvers and optimizers), reachability, programming languages (semantics, implementation), control theory, modeling, etc) but maybe made a bit more specific
    - Assign 5 to 7 names to each topic - This defines D-Groups
        - Participants divide themselves into equal-sized 4 Disciplinary groups
        - Then, divide themselves also into equal-sized 5 Interdisciplinary groups
- **10:15 - 10:45 Short Break**
- **10:45 - 11:30 Session 2** - Introductions within interdisciplinary groups (I-Groups)
    - Breaking into interdisciplinary groups (5 groups, 4 to 6 people per group)
    - Group is responsible for mutual introductions with the group and making some Google Docs slides to introduce each member
    - We suggest that I-Groups stay together during lunch to continue the introductions
- **11:30 - 12:00 Session 2** - I-Groups introduce members to entire attendance
    - Two presentations, about 10 minutes each
- **12:00 - 1:45 Lunch**

PM

- **1:45 - 2:00 Group photo shooting** (right after lunch)
- **2:00 - 2:45 Session 3** - I-Groups introduce members to entire attendance
    - Three presentations, about 10 minutes each
- **2:45 - 3:15 Break**
- **3:15 - 6:00 Session 4** - Disciplinary (D)-groups can start working on the different tutorial presentation
- **6:00 - 8:00 Dinner**
- **8:00 - 9:00** INTLAB demonstration by Prof. Rump

September 29th, Tuesday

AM

- **9:00 - 9:45** - Group work for preparing presentations
- **9:00 - 12:00 Session 5** - Presentation of first three disciplinary tutorials, with 1 hour or 30 minutes for presentation and 15 minutes for discussion
    - **9:45 - 10:45 Tutorial 1** (validated numerics)
        - 10:45 - 11:00 Questions
    - **11:00 - 11:30 Short Break**
    - **11:30 -12:00 Tutorial 2** (control theory)
        - 12:00 - 12:15 Questions
    - **12:15 - 12:45 Tutorial 3** (programming languages & semantics)
        - 12:45 - 1:00 Questions
- **1:00 - 2:30 Lunch**

PM

- **3:00 - 3:45 Session 5** - Presentation of first three disciplinary tutorials, with 30 minutes for presentation and 15 minutes for discussion
    - **3:00 - 3:30 Tutorial 4** (verification, reachability analysis)
        - 3:30 - 3:45 Questions
- **3:45 - 4:15 - Short Break**
- **4:15 - 6:00 Sessions 6** - Brainstorming Session for Roadmaps
    - Collecting ideas from audience about:
        - Significant challenges
        - Major milestones (success landmarks)
        - Strategies and tactics to achieve these milestones
        - A timeline for achieving these milestones
        - Resources needed for achieving these milestones
- **6:00 - 8:00 Dinner**
- **8:00 - 10:00** Tool demonstrations (Acumen, HydLa, HySIA)

September 30th, Wednesday

AM

- **Session 7** - Fast-paced session to document the overall view of the roadmap
    - **9:00 - 9:40**
        - D-Groups document challenges in slides
    - **9:40 - 10:15**
        - I-Groups document milestones in slides
    - **10:15 - 10:30 Break**
    - **10:30 - 11:00**
        - D-Groups document strategies and tactics to achieve these goals
    - **11:00 - 11:30**
        - I-Group document timeline needed to achieve these milestones

        - **11:30 - 12:00**
            - D-Groups document resources needed for achieving these milestones
    - **12:00 - 1:30 Lunch**

PM

- Excursion/banquet

October 1st, Thursday

AM

- **9:00 - 10:15 Session 8** - Presentation of road-map slides
- **10:15 - 10:45 Break**
- **10:45 - 11:30 Session 9** - Plans for follow up work to turn slides into surveys and a roadmap document
- **11:30 - 12:00 Closing Session** - Presentation of summary

Overview of Sessions

Session 1

The following disciplinary topics were proposed:

- D1: Control theory
- D2: Languages and semantics
- D3: Verification
- D4: Validated numerics

Accordingly, the following Disciplinary groups (D-groups) were formed:

- D1: A. Goldsztejn, R. Wisniewski, T. Ushio, A. Chapoutot, Y. Tazaki, and T. J. Koo
- D2: A. Duracz, J. Inoue, M. Martel, S. Matsumoto, M. Mousavi, and K. Ueda
- D3: I. Hasuo, D. Ishii, S. Nakajima, S. Ratschan, K. Suenaga, A. Wąsowski, and R. Yanase
- D4: A. Griewank, M. Miyajima, N. Nedialkov, K. Ozaki, S. Rump, W. Taha, and A. Takayasu

Interdisciplinary groups (I-groups) were formed as follows:

- I1: T. J. Koo, M. Mousavi, N. Nedialkov, and A. Wąsowski
- I2: S. Nakajima, D. Ishii, K. Ozaki, Y. Tazaki, and A. Duracz
- I3: A. Chapoutot, K. Ueda, I. Hasuo, and A. Takayasu
- I4: A. Goldsztejn, M. Martel, S. Ratschan, and W. Taha
- I5: R. Yanase, S. Matsumoto, S. Rump, and R. Wisniewski
- I6: T. Ushio, J. Inoue, K. Suenaga, and S. Miyajima

Session 2-3

Each I-group introduced the members and proposed ideas for possible collaborations in this meeting. The proposed ideas are summarized as follows:

Group I1:

- Validated numerics for (LTL + first order logic + reals)
- Simulation for systems with rich data
- Event detection and sampling for robust partitioning in testing hybrid systems
- Interval-based reachability analysis
- Disambiguating and generating design guidelines for concurrent evaluations (e.g., using partial order techniques)

Group I2:

- Application area:
  - Fault localization combined in the context of energy conservation
- Systems that control theorists are interested in simulating robustly
  - Methods to deal with initial-time / physical parameter uncertainty
- Explore application of bisimulation to abstraction of CPS
  - Apply concepts from C.S. to CPS

Group I3:

- A few joint research papers on, and systems, for:
  - Combining numerical techniques and formal, symbolic ones
    - Verified/validated numerics, and
    - relational abstraction, abstract interpretation, CEGAR, …
  - Expressing complex, "real" dynamics in formal modeling (like PDEs)

Group I4:

- High level language for modeling hybrid systems
  - Simulink: no exact semantics for continuous neither discrete events
  - Hybrid automaton: too low level
- Validated simulation and safety verification for high level language
- Consolidating and comparing validated ODE and hybrid ODE libraries (VNODE, Dyn-IBEX, CAPD, Flow*, Ishii, etc.)
- Connecting libraries to modeling tools (semantics)
- Find ways to preserve results and experiences about implementations

Group I5:

- A joint software combining certificates of positivity with optimisation and interval arithmetics
- Collaboration on optimisation with error bounds on the solution.
- Verification of stability with interval arithmetics

Group I6:

- What is "verification"?
  - Validated numerics: giving guaranteed error bounds
  - Programming languages: proving a program satisfies specs
- What is a "system"?
  - Validated-numerics: a set of equations
  - Control and languages: anything that evolves over time
- Possible collaborations
  - Program verification using the techniques in numerics and control
  - Computer-aided theorem prover for existence/uniqueness/stability of solutions
    - Program extraction for controller synthesis
  - Understanding similar concept in each discipline
    - Stability in control ↔ Termination in PL

Session 4-5

Tutorial 1 (Group D4, reliable numerical computations)
This tutorial first explains what are reliable numerical computations. Then, tools are introduced such as interval arithmetics, Affine arithmetics and piecewise linearization. Finally, we describe some applications including nonlinear eigenvalue problems, global optimization, nonsmooth functions, ODEs, and parabolic PDEs.

Tutorial 2 (Group D1, control theory)
This tutorial explains (i) the basics of stability analysis of continuous time systems, and (ii) reachability and abstraction methods for hybrid systems.

Main task of stability analysis is to design a control input of the system so that the state converges to the desired trajectory. For linear systems, the asymptotically stability of a system is translated to some conditions on the eigenvalues of the system matrix. For certain systems, we can design a state-feedback controller that makes a system asymptotically stable. For nonlinear systems, Lyapunov function based methods and barrier certificate methods can be used to check the asymptotically stability of a system.

Hybrid systems can be described by hybrid automata. The behavior of hybrid systems can be formulated as transition systems that involve both discrete and continuous transitions. To compute pre- and post- image of such a transition system, the level set methods are proposed. In the analysis of hybrid systems, finite-state abstraction is useful for applying symbolic techniques; one approach is to compute quotient transition systems. For abstracting hybrid systems, a method called approximate bisimulation is proposed.

Tutorial 3 (Group D2, languages and semantics)
Formal semantics of a programming language is needed to rigorously define what a program does. This tutorial first overviews various ways to give semantics of a program. These semantic models include operational, denotational, axiomatic semantics.

To develop formal semantics for hybrid systems, there are several challenges and design decisions. Design decisions for the time domain, concurrency, nondeterminism, and error bounds are discussed. As examples of semantics models for hybrid systems, we explain hybrid transition systems and timed state sequences.

The tutorial will also explain related notions such as equivalence/refinement of models and symbolic execution.

Tutorial 4 (Group D3, reachability analysis)
Verification (or model-checking) techniques have been developed for discrete, probabilistic, timed, hybrid, and/or concurrent systems.

Basic verification technique is to reduce the problem into a reachability problem. When the system has finite or bounded state space, we can perform an exhaustive search of a counter example that reaches the bad state. When the system has infinite and unbounded space, additional techniques for state-space abstraction will be needed, e.g., inductive invariants, predicate abstraction, and phase portrait techniques.

A difficulty in the verification with abstraction is to find a proper abstraction of a model so that the search space is kept small and it does not contain any spurious

counterexample. To compensate these requirements, the CEGAR (counter-example guided abstraction refinement) method is proposed. CEGAR is a simple procedure that repeats four steps: 1) computation of abstraction, 2) verification against the abstraction, 3) feasibility checking of a found counterexample, and 4) refinement of the abstraction.

Session 6-8

The following interdisciplinary topics were proposed and discussed:

- Understanding CPS Modeler Semantics (A. Chapoutot)
- Challenges in Control (T. Ushio, Y. Tazaki, and R. Wisniewski)
- CPS Software Challenge (A. Mori)
- Coping with complexity of real-world systems (I. Hasuo)
- Problem Solving Environments for CPSs (W. Taha, K. Ueda, and D. Ishii)
- Compositional verification (K. Suenaga)
- Semantics and simulation for partial models (J. Inoue, K. Ueda, S. Matsumoto, A. Duracz, and A. Wąsowski)
- Semantics with Uncertainty (J. Inoue)
- Doing Interval Methods Right (J. Inoue)
- Efficient Program Reversal (A. Griewank)
- Stiffness is a problem for validated ODE solvers (N. Nedialkov, F. Bartha, A. Chapoutot., and A. Goldsztejn)
- Advances in validated DDE integration (F. Bartha, A. Chapoutot, and A. Goldsztejn)
- Challenges in interval arithmetic (Miyajima, Ozaki, and Yamanaka)
- FEniCS with interval arithmetic? (A. Takayasu)

Session 9

We discussed tentative plans for continuing the discussions to fill the gap between the CPS research communities. The plans include writing tutorial papers based on the materials prepared in this meeting, and organizing other meetings e.g. a Dagstuhl-like seminar or a workshop.

List of Participants

Ferenc Bartha, Rice University, USA

Alexandre Chapoutot, ENSTA Paristech, France

Adam Duracz, Halmstad University, Sweden

Alexandre Goldsztejn, CNRS/IRCCyN, France

Andreas Griewank, Humboldt University Berlin, Germany

Ichiro Hasuo, University of Tokyo, Japan

Jun Inoue, AIST, Japan

John Koo, ASTRI, Hong Kong

Matthieu Martel, Universit de Perpignan Via Domitia, France

Shota Matsumoto, Waseda University, Japan

Shinya Miyajima, Gifu University, Japan

Akira Mori, AIST, Japan

Mohammad Reza Mousavi, Halmstad University, Sweden

Shin Nakajima, National Institute of Informatics, Japan

Ned Nedialkov, McMaster University, Canada

Katsuhisa Ozaki, Shibaura IT University, Japan

Stefan Ratschan, Academy of Sciences of the Czech Republic

Siegfried Rump, Hamburg University of Technology, Germany

Akitoshi Takayasu, Waseda University, Japan

Yuichi Tazaki, Nagoya University, Japan

Kazunori Ueda, Waseda University, Japan

Toshimitsu Ushio, Osaka University, Japan

Andrzej Wąsowski, IT University of Copenhagen, Denmark

Rafael Wisniewski, Aalborg University, Denmark

Naoya Yamanaka, Teikyo Heisei University, Japan

Ryo Yanase, Kanazawa University, Japan