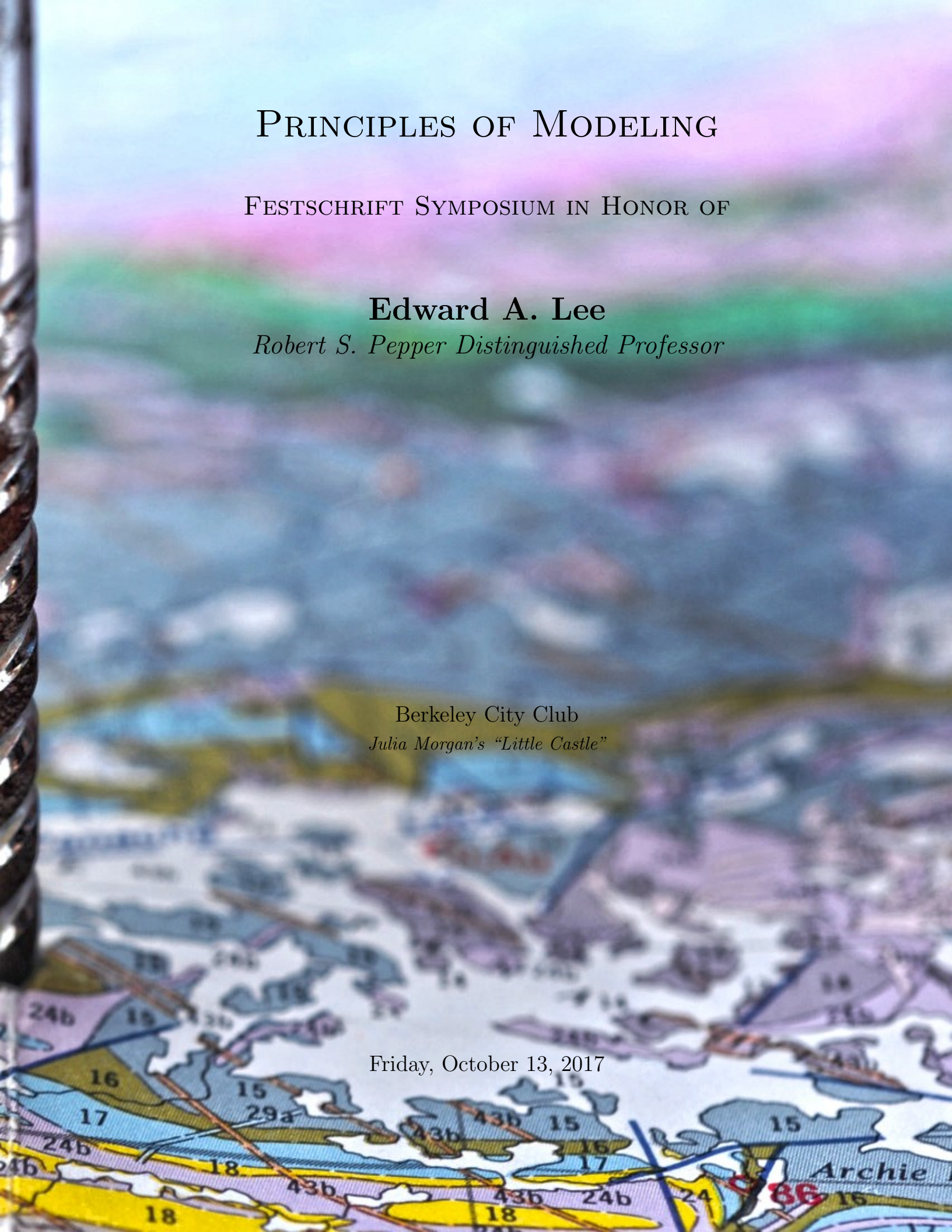
Principles of Modeling

Festschrift Symposium in Honor of

Edward A. Lee
Robert S. Pepper Distinguished Professor

Berkeley City Club
Julia Morgan's "Little Castle"

Friday, October 13, 2017



Preface

The Edward A. Lee Festschrift Symposium is a day-long symposium to celebrate the scholarship and teaching of Edward A. Lee, the Robert S. Pepper Distinguished Professor in Electrical Engineering and Computer Science at the University of California at Berkeley.

The theme of the symposium is "Principles of Modeling," because Edward has long been devoted to research that centers on the role of models and is a fervent advocate of a principled use of models in science and engineering. Edward is interested in the use and limitations of models, their formal properties, their role in cognition and interplay with creativity, and, finally, their relationship with reality and physics. He warns not to "confuse the map with the territory" and cautions that "all models are wrong," but identifies tremendous value in the use of models, given that they provide meaningful abstractions. He also emphasizes that, for engineers, modeling is a "two-way street," as they can, unlike scientists, manipulate both the model and the thing being modeled. Edward's research covers a broad range of topics, among which are: determinism, time, concurrency, cyber-physical systems, and signal processing.

The symposium is dedicated to Edward's lifelong ideas and influences, and some of Edward's closest collaborators and most prominent colleagues will be delivering talks during the event. They have also been invited to contribute a paper to a so-called Festschrift, which will be published by Springer in their Lecture Notes in Computer Science (LNCS) series. The term "Festschrift" is borrowed from German, and could be translated as celebration publication or celebratory (piece of) writing (literally 'party-writing'; cognate with 'feast-script'). Sometimes, the Latin term liber amicorum (literally: "book of friends") is used for a Festschrift.

The Festschrift articles will be published in a post-proceedings.

Acknowledgements

Festschrift Authors

The following invited authors have contributed an article to the Festschrift:
Gul Agha, Rajeev Alur, Murat Arcak, Sanjoy Baruah, Shuvra Bhattacharyya, David Broman, Janette Cardoso, Werner Damm, Stephen Edwards, Marc Geilen, Alain Girault, Radu Grosu, Soonhoi Ha, Reinhard von Hanxleden, Tom Henzinger, Christoph Kirsch, Hermann Kopetz, Jie Liu, Dave Messerschmitt, Marco di Natale, Bernard Rumpe, Sanjit Seshia, Alberto Sangiovanni-Vincentelli, Bruno Sinopoli, Marjan Sirjani, Walid Taha, Martin Trngren, Stavros Tripakis, Hans Vangheluwe, Reinhard Wilhelm

Organizers

This event is organized by Patricia Derler, Marten Lohstroh, and Marjan Sirjani with support from Christopher Brooks and Mary Stewart.

Publisher

We thank Springer for publishing the contributed essays in their special "Festschrift" LNCS series.

Sponsors

We are grateful to Prabal Dutta, Edward A. Lee, Jan Rabaey, Alberto Sangiovanni-Vincentelli, and Sanjit Seshia for sponsoring this event.

Volunteers

Thanks to Tommasso Dreossi, Jessica Gamble, Antonio Iannopollo, Gil Lederman, Mehrdad Niknami, Charlotte Jones, Matt Weber, and Ben Zhang for their assistance during the event.

Program

8:00am to 8:30am: Continental Breakfast

8:30am Opening

8:30am to 8:40am: **Marten Lohstroh** *(University of California, Berkeley)* Welcome

8:40am: Cyber-physical Systems
Chair: Prabal Dutta *(University of California, Berkeley)*

10:00am to 10:20am: Break

11:00am: About Time
Chair: Patricia Derler *(National Instruments)*

11:40am: Lunch

12:00pm to 12:20pm: **John Eidson** *(University of California, Berkeley)* A Tribute to Edward A. Lee

12:40pm: Modeling and Simulation
Chair: Janos Sztipanovits *(Vanderbilt University)*

12:40pm to 1:00pm: **David Broman** *(KTH Royal Institute of Technology)* Hybrid Simulation Safety: Limbos and Zero Crossings 10

1:00pm to 1:20pm: **Janette Cardoso** *(Institut Suprieur de l'Aronautique et de l'Espace)* Ptolemy-HLA: a CPS Distributed Simulation Framework 10

1:20pm to 1:40pm: **Christoph Kirsch** *(University of Salzburg)* You Can Program What You Want but You Cannot Compute What You Want 11

1:40pm to 2:00pm: **Marjan Sirjani** *(Mlardalen University, Reykjavik University)* Power is Overrated, Go for Friendliness! 11

2:15pm: Panel Discussion: "What Good is Determinism, Anyway?"
Moderator: Stephen Edwards *(Columbia University)*

2:15pm to 3:15pm: Panelists:
Gul Agha *(University of Illinois at Urbana-Champaign)*
Ruzena Bajcsy *(University of California, Berkeley)*
Thomas Henzinger *(Institute of Science and Technology Austria)*
Hermann Kopetz *(Vienna University of Technology)*

3:30pm: Future Avenues
Chair: Gul Agha *(University of Illinois at Urbana-Champaign)*

3:30pm to 3:50pm: **Dave Messerschmitt** *(University of California, Berkeley)* Is Terminological Innovation a Good Idea? 12

3:50pm to 4:10pm: **Rajeev Alur** *(University of Pennsylvania)* Interfaces for Stream Processing Systems 12

4:10pm to 4:30pm: **Richard Murray** *(California Institute of Technology)* Modeling, Analysis, and Design of Biomolecular Feedback Systems 13

4:30pm to 4:50pm: **Bruno Sinopoli** *(Carnegie Mellon University)* Modeling

4:50pm: Closing

4:50pm to 5:00pm: **Christopher Brooks** *(University of California, Berkeley)*
Closing Remarks

5:00pm: Reception

5:00pm to 8:00pm: Reception with Hors d'Oeuvres (Members Lounge and Terrace)

Cyber-Physical Systems Education: Explorations and Dreams

8:40am to 9:00am

Sanjit Seshia
University of California, Berkeley

As the field of cyber-physical systems (CPS), as an intellectual discipline, enters its second decade, it is worth reflecting on what we have learned from the various explorations in CPS education, related technologies, and their interplay with research. This article addresses this topic and attempts to extrapolate these explorations to "dreams" for what the future may bring.

Multi-Paradigm Modeling for Cyber-Physical Systems

9:00am to 9:20am

Hans Vangheluwe
University of Antwerp and McGill University

Multi-Paradigm Modelling (MPM) has been proposed to tackle the complexities found in Cyber-Physical Systems (CPS). MPM advocates the explicit modelling of all pertinent parts and aspects of complex systems explicitly, using the most appropriate abstraction(s) and formalism(s). It addresses and integrates three orthogonal dimensions: (1) multi-abstraction modelling, concerned with the (refinement, generalization, ...) relationships between models, (2) multi-formalism modelling, concerned with the (multi-view, multi-component, ...) coupling of and transformation between models described in different formalisms, and (3) explicitly modelling the often complex, concurrent workflows. The core methods and techniques that enable MPM are model management, (domain-specific) modelling language engineering, and workflow modelling. In this paper, an overview of the different types of challenges, as well as suggested MPM solutions will be presented.

Autonomous Retailing: A Frontier for Cyber-Physical Systems

9:20am to 9:40am

Jie Liu
Microsoft Research

Retail is one of the largest economic sectors, accounting for almost $5Trillion sales in US alone. With the proliferation of e-commerce, mobile devices, and digitization of shopping journeys, retail is going through profound transformations that will touch everyone's life. Physical stores, which still account of 85% total retail sales, and 95% of grocery sales, must be considered holistically with online and mobile shopping channels. The future of retail will inevitably combine online (digital) and store (physical), and give individual customers superb experience and control.

Autonomous retailing is a retail process where a physical store is aware of everything inside products, people, and activities, and understands its shoppers intent, without

explicit help from human workers. Amazon Go is an example of a cyber-physical store that allows shoppers to pick up products and walk out of the store, without going through a checkout lane. The store recognizes all products, tracks every shopper, and understands key shopper activities, such as picking up and returning products. But the ultimate autonomous retailing must also take shoppers interests, intents, and personalities into account, and be a cyber-physical-human system. It must help shoppers navigate, find, and choose the right products at the right prices. It may incentivize shoppers to adopt good behaviors and avoid malicious behaviors.

In this paper, I discuss the vision of autonomous retailing, its system requirements, and an agent framework that fuses physical and digital data to serve individual shoppers.

Compressed Sensing In Cyber Physical Social Systems

9:40am to 10:00am

Radu Grosu
Vienna University of Technology

We survey the main results in Compressed Sensing and Social Networks, and discuss the impact they have on Cyber Physical Social Systems. CPSS are currently emerging on top of the Internet of Things. Moreover, inspired by randomized Gossip Protocols, we introduce TopGossip, a new compressed-sensing algorithm for the prediction of the top-k most influential nodes in a social network. TopGossip is able to make this prediction by sampling only a relatively small portion of the social network, and without having any prior knowledge of the network structure itself, except for its set of nodes. Our experimental results on three well-known benchmarks, Facebook, Twitter, and Barabasi, demonstrate both the efficiency and the accuracy of the TopGossip algorithm.

Computing Average Response Time

11:00am to 11:20am

Thomas Henzinger
Institute of Science and Technology Austria

Responsiveness — the requirement that every request to a system be eventually handled — is one of the fundamental liveness properties of a reactive system. Average response time is a quantitative measure for the responsiveness requirement used commonly in performance evaluation. We show how average response time can be computed on state-transition graphs, on Markov chains, and on game graphs.

Abstraction and Refinement of Time in Hierarchically Decomposable Underspecified Architecture Simulations

10:40 am to 11:00am

Bernhard Rumpe
RWTH Aachen University

Based on an elaborated theory for the modeling of underspecification resp. nondeterminism, hierarchical composition, refinement that is compatible with composition, and finally provenly correct evolution patterns, we discuss how such a theory can be practically applied for the development of CPS in three stages:

(a) Function nets model the CPS system and subsystem functions, (b) software architectures decompose them into manageable units of functionality, and (c) software modules are mapped to physical and usually unreliable and resource constrained hardware.

Through an orchestrated efficient simulation, we can early identify potential bottlenecks, function failures, hardware risks, etc.

All models as well as the simulation take advantage of the compositionality and the timing refinement properties of the theory.

In summary, we discuss how the elaborated theory shapes the simulation and the results.

Anytime Algorithms in Time-Triggered Control Systems

11:00am to 11:20am

Hermann Kopetz
Vienna University of Technology

The deterministic temporal behavior of a time-triggered computer platform provides an ideal base for the implementation of a real-time control system. The temporal predictability requires that the durations of the time-slots for the execution of the control algorithms be specified a priori at design time. Since the indeterminism of state of the art hardware makes it difficult to arrive at a tight worst-case-execution-time (WCET) bound for the execution of a conventional control algorithm we propose to use anytime algorithms in a time-triggered control systems. An anytime algorithm trades precision for execution time (latency). It gives the designer the freedom to select a duration for a time-slot that on the one side is sufficient to achieve the required precision and on the other side will not introduce an extensive latency that has a detrimental effect on the quality and stability of a closed-loop control system. This paper presents guidelines for the design of the durations of the time-slots in time-triggered control systems that deploy anytime algorithms.

Predictability Issues in Mixed-Criticality Real-Time Systems

11:20am to 11:40am

Sanjoy Baruah
Washington University in St. Louis

Predictibility is often listed as an explicit requirement for safety-critical real-time systems. In system designs, this requirement is typically met by establishing that salient run-time temporal properties of the system being designed can be predicted prior to run-time. But what of real-time systems supporting multiple functionalities that are not all equally critical? In such systems, it may be necessary to establish predictability of highly critical functionalities to a higher level of assurance than is needed for lower-criticality functionalities. We will study the implications of this fact on the deterministic modeling of real-time systems, and explore means for achieving more resource-efficient implementations of mixed-criticality real-time systems.

Hybrid Simulation Safety: Limbos and Zero Crossings

12:40pm to 1:00pm

David Broman
KTH Royal Institute of Technology

Physical systems can be naturally modeled by combining continuous and discrete models. Such hybrid models may simplify the modeling task of complex system, as well as increase simulation performance. Moreover, modern simulation engines can often efficiently generate simulation traces, but how do we know that the simulation results are correct? If we detect an error, is the error in the model or in the simulation itself? This paper discusses the problem of simulation safety, with the focus on hybrid modeling and simulation. In particular, two key aspects are studied: safe zero-crossing detection and deterministic hybrid event handling. The problems and solutions are discussed and partially implemented in Modelica and Ptolemy II.

Ptolemy-HLA: a CPS Distributed Simulation Framework

1:00pm to 1:20pm

Janette Cardoso
Institut Suprieur de l'Aronautique et de l'Espace

The HLA-PTII co-simulation framework leverages two open source tools: Ptolemy II and HLA/CERTI for the simulation of Cyber-Physical Systems (CPS). This framework allows to deal with three important issues: (i) Distribution of a simulation, allowing the scaling up for big models and performance, (ii) Interoperability of tools, allowing reusability and interfacing with other simulators or real devices/systems, (iii) Heterogeneous simulations (discrete events, continuous time).

The framework extends Ptolemy by coordinating the time advancement of various Ptolemy instances with the help of the time management services of HLA, and by allowing data communication between various Ptolemy instances with the help of the data management services of HLA.

These additions allow for producing HLA federates (ie, simulators) in a Federation (ie, a distributed simulation) in an easy way since the user does not need to be an HLA specialist for designing a Federate. The paper presents the new components added for extending Ptolemy, some semantic issues, application examples and performance analysis.

You Can Program What You Want but You Cannot Compute What You Want

1:20pm to 1:40pm

Christoph Kirsch
University of Salzburg

Computers are the most fascinating machines ever invented. Virtually everyone uses them in one form or another every day. However, most people only have a vague understanding of how computers work, let alone how to program them. Yet computing has become a commodity almost like energy, food, or water. The question is if the general public, for modern society to work properly, needs to understand computing better than what people generally know about, say, producing electricity or clean water. We argue that the intractability and even undecidability of so many important problems in computer science are the reason that computing is indeed different. It is the limits of computability, not just the capabilities of computers, that is the source of unbounded potential in the automation of everything. The challenge is to teach people not just programming but also how programming is the neverending process of overcoming those limits. We have developed a system called selfie that implements a self-referential compiler, emulator, and hypervisor that can compile, execute, and virtualize itself. We use selfie to teach undergraduate and graduate students computer science from first principles. In particular, we show them how self-referentiality in selfie is capability and limitation of computing at the same time. Here, we discuss ongoing early work on integrating verification technology into selfie as yet another way of exploring what computing is.

Power is Overrated, Go for Friendliness!

1:40pm to 2:00pm

Marjan Sirjani
Mlardalen University, Reykjavik University

Expressive power of a language is generally defined as the breadth of ideas that can be represented and communicated in a language. For formal languages we check the expressive power by checking if it is Turing complete. In a modeling process, apart from the modeling language we have two other counterparts, the system being modeled and the modeler. I argue that faithfulness to the system being modeled, and usability for the modeler are at least as important as the expressive power of our modeling language, specially because the modeling languages we use nowadays are highly expressive. I call faithfulness and usability together as friendliness. I show how we used the actor-based language Rebeca in modeling different applications, where it is friendly, and where it is not; and how the features of the language and its friendliness may help in analysis of the model, and synthesis of the system based on the model.

Is Terminological Innovation a Good Idea?

3:30pm to 3:50pm

Dave Messerschmitt
University of California, Berkeley

When a field benefits from many contributors and authors a base of conventional terminology develops over time. This terminology can have problems associated with it, such as inconsistencies or outright contradictions and a lack of thoughtful articulation among related concepts. Particularly in an engineering context that flows from a scientific base, the conventional terminology can lack a logical connection to its eventual context or usage. We argue that it is occasionally valuable to step back and initiate a fresh approach, defining a whole new terminology that obeys a consistent metaphorical model of an application domain. However, this has the obvious disadvantage of perpetuating a disconnect with a large and relevant literature. We illustrate these tensions using a recent initiative of our own to remake relativity in the context of issues of timekeeping in distributed systems. We briefly describe our new relativistic terminology and how it contributes to a consistent and meaningful paradigm describing the effect of motion and gravity on timekeeping. Unfortunately at the same time it renders partially obsolete a relevant, large, and illustrious literature. The reader is left to decide for themselves whether this is a valuable advance or an unwanted distraction.

Interfaces for Stream Processing Systems

3:50pm to 4:10pm

Rajeev Alur
University of Pennsylvania

Efficient processing of input data streams is central to IoT systems, and the goal of this paper is to develop a logical foundation for specifying the computation of such stream processing. In the proposed model, both the input and output of a stream processing system consists of tagged data items with a dependency relation over tags that captures the logical ordering constraints over data items. While a system processes the input data one item at a time incrementally producing output data items, its semantics is a function from input data traces to output data traces, where a data trace is an equivalence class of sequences of data items induced by the dependency relation. This data-trace transduction model generalizes both Kahn process networks and relational query processors, and can specify computations over data streams with a rich variety of ordering and synchronization characteristics. To form complex systems from simpler ones, we define sequential composition and parallel composition operations over data-trace transductions, and show how to define commonly used idioms in stream processing such as sliding windows, key-based partitioning, and map-reduce.

Modeling, Analysis, and Design of Biomolecular Feedback Systems

4:10pm to 4:30pm

Richard Murray

California Institute of Technology

Advances over the past decade have given biological engineers new insights into the role of genetic circuits in nature and the design of biomolecular circuits to implement biological operations in vitro and in vivo. In this talk I will discuss the use of concepts from systems and control engineering as applied to the analysis and design of biological feedback circuits. After a brief survey of relevant concepts from synthetic biology, I will present some recent results that combine modeling, analysis, design and experimental implementation of biological feedback circuits. These results include the role of redundant bioogical pathways for implementing robust decision-making strategies in cells, the use of biomolecular "breadboards" for prototyping and debugging engineered biomolecular circuits, and the implementation of circuits for regulation of gene expression and biomolecular event detection. Using these results as examples, I will discuss some of the open problems and research challenges in the area feedback control using biological circuits.

Modeling Dynamical Phenomena in the Era of Big Data

4:30pm to 4:50pm

Bruno Sinopoli

Carnegie Mellon University

As the world around us gets embedded with widespread sensing, computing, communication and actuation, opportunities to improve the quality of life arise. Smart infrastructures promise to dramatically increase efficiency, safety and quality of life. While data abounds, modeling and understanding complex phenomena such as the interaction of large scale infrastructures, e.g. energy, transportation, communication, water and buildings presents several challenges. Deriving models from first principles via white or grey box modeling is infeasible. Classical black-box modeling is also not practical as model selection is hard, interactions change over time and evolution can be observed passively, without the chance to conduct experiments through data injection or manipulation of the system. Moreover the causality structure of such systems is largely unknown. We contend that determining data-driven, minimalistic models capable of explaining dynamical phenomena and tracking their validity over time is an essential step toward building dependable systems. In this work we will outline challenges, review existing work and propose future research directions.


Ringer I.
Bassoon L.
24b
24b, a
43b
18
17