Report on the Dagstuhl Seminar 00181 on

Probabilistic Methods in Verification

The established methodology of engineering computer systems, both hardware and software, involves first building a *model* of the system, and then its detailed *analysis*, before implementation takes place. The motivation for this is to increase the engineers' confidence in the design of the system, with respect to desirable characteristics such as functional correctness and performance requirements. Two related disciplines which are instances of this methodology are *verification* and *performance evaluation*:

- The first of these, **verification** through *model checking*, employs algorithmic methods to provide "Yes/No" answers to qualitative correctness requirements, primarily concerned with *system behaviour over time* (for example, ensuring the delivery of a message or safety of a particular activity). A model of the system is formulated using an appropriate formalism, and then supplied as input to a software tool which automatically checks if a given specification is satisfied. Such model checking tools are used widely in practical applications, particularly for analysing hardware and communication protocols. The term **probabilistic verification** refers to methods in which "Yes/No" answers are replaced with estimates of the *likelihood* of the system satisfying a specification. Two prevailing views of probabilistic verification exist. The first concerns probabilistic models of the system (for example, discrete-time Markov chains or Markov decision processes), and aims to model check these against probabilistic variants of temporal logics. The second is applied in the context of non-probabilistic systems, but those of a size which makes exhaustive model checking impractical or infeasible. The aim is then to establish that the required properties hold with high probability.
- The field of **performance evaluation** involves building a probabilistic model of a system, followed by analysis focused on the calculation of *performance measures*. Typically, the underlying model of system description formalisms in this field is a continuous-time Markov chain, with the desired system requirements (throughput, mean time to failure, etc.) expressed in terms of steady-state probabilities. This relies heavily on the use of numerical methods and tools when analysing the models. Performance evaluation tools have been successfully used to predict the impact of changes to load and arrival characteristics of computer networks.

Though the fields of verification and performance evaluation have historically concentrated on analysing different aspects of the system (*qualitative* correctness requirements versus *quantitative* performance issues), they are complementary and have much in common. For example, both aim to build a representation of the model in the computer memory, and in fact the difficulties and challenges posed by representing very large models have been recognised in both communities (the verification community calls this the 'state explosion problem', whereas to performance evaluation practitioners it is known as 'largeness'). Therefore, the appeal of integration and cross-fertilisation of techniques between the two fields is immediate. The goal of this Dagstuhl meeting was to bring together researchers representing the different communities, who would not necessarily meet at other conferences or workshops, in order to provoke debate and to facilitate exchange of expertise. In all, 48 researchers from 11 countries participated in the meeting.

In an effort to bring the two distinct, yet closely related, fields together four keynote speakers were invited to give overview lectures. **Luca de Alfaro** gave an introductory talk on the algorithmic verification of probabilistic systems. **Rajeev Alur** then spoke about modular specification and simulation of hybrid systems. An introduction to the field of performance evaluation was presented by **Boudewijn Haverkort**. This was complemented by a talk from **Martin Reiser** giving an overview of performance evaluation of computer and communication systems over the past thirty years.

The remaining 31 presentations given by participants of the meeting covered a range of topics from probabilistic verification and performance evaluation. Some centred on the development of **modelling formalisms** for probabilistic systems, including stochastic variants of process algebras and the π-calculus, real-time extensions to probabilistic and stochastic systems, and continuous space Markov processes.

Other talks concerned **methods of analysis** for such systems: model checking algorithms for probabilistic and stochastic temporal logics; and equivalences on probabilistic systems and their corresponding decision procedures.

A third group of talks centred on the **implementation** of probabilistic verification, describing recent or ongoing work on the development of efficient tools and techniques. These included symbolic, BDD-based, model checking of probabilistic algorithms and stochastic Petri net tools employing Kronecker-based techniques. While the former focuses on verification and the latter on performance evaluation, what they have in common is the use of BDDs and Kronecker, which should lead to fruitful exchange of ideas. A group of talks introduced BDD-based methods for representing and verifying logical circuits with high probability.

A number of interesting **application areas** were also highlighted, including security and fault-tolerant systems.

The selection of presentations was accompanied by a **panel discussion** chaired by **Moshe Vardi** held towards the end of the meeting. Six prominent researchers (**Boudewijn Haverkort**, **Ulrich Herzog**, **Radha Jagadeesan**, **Joost-Pieter Katoen**, **Marta Kwiatkowska** and **Frits Vandraager**) were invited to answer questions on the present and future relationship between the fields of probabilistic verification and performance evaluation, prompting lively, interesting and productive discussion summarised at `http://www.cs.bham.ac.uk/~mzk/Dagstuhl/`. The optimism for future cooperation was evident not only here, but in the numerous stimulating discussions between participants during the week.

Of course, the success of the event was only made possible by the excellent facilities and working environment of the venue. On behalf of everyone who attended the seminar, the organisers would like to thank the staff at Schloß Dagstuhl for all their hard work.

Marta Kwiatkowska
Ulrich Herzog
Christoph Meinel
Moshe Vardi