Theoretical Computer Science

The theory group specializes in logic in computer science, automata theory and formal languages, verification, computational complexity, cryptographic protocols, and computing education.

Results

Information flow security. As the internet has become one of the major means of communication and interaction in our society, it is most important to ensure that communication over it is carried out in a secure fashion. This calls for: (1) mechanisms for secure communication, and (2) methods for proving systems using these mechanisms securely. Unfortunately, standard methods for (2) are not really modular: they do not support hierarchical approaches, and neither do they work well with abstraction, which means complex systems can hardly be proved secure at all. According to Rushby, a solution may be to analyze the information flow between individual components of a system. In fact, the notion of „information flow security" tries to capture this idea formally and may be a good starting point in this regard. One of the main results of the theory group in 2011 was a complete classification of different notions of information flow security proposed in the literature, in terms of their computational complexity.

Cryptography. In recent years, the theory group has built up expertise on cryptography, both in research and teaching. One of the major objectives in teaching is to convey that IT systems need not only be designed so as to ensure security but also rigorously proved to be secure (see above). There had been no textbook in German advocating this view until last year, when the theory group, together with a group at Trier University, concluded its work on the first, entitled „Moderne Kryptographie" .

Automata theory. Automata, basic models of computation, are applied in many areas of computer science. One particular automaton model, often used in verification of non-terminating computation processes, is a finite-state device called „Büchi automaton" . Over the last years, the theory group has contributed regularly to the study of Büchi automata. In 2011, in joint work with colleagues from the US and Israel, a result was obtained regarding complementation of Büchi automata, one of the major technical problems when dealing with such automata.

Propositional Logic. Continuing the research about constraint-related problems from propositional logic, the theory group studied the minimization problem for propositional formulas. In addition to its relevance for complexity theory (a variant of this problem led to the definition of the polynomial hierarchy), this problem has highly practical relevance in artificial intelligence, for example in the „compression" of knowledge bases. The group, in joint work with a colleague from the US, obtained very broad classification results showing in which cases formulas can be minimized efficiently. Unlike similar problems in the literature, the complexity of the minimization problem is not determined by the usual algebraic characterizations.

Modal Logic. In joint work with a colleague from the US, the theory group continued their research on complexity of the modal satisfiability problem. This year the main result is that there is a very „simple" modal logic that is undecidable, namely one which is obtained by restricting the allowed models to those satisfying a universal first-order formula (without equality). This result complements earlier work of the group about the complexity of the modal satisfiability problem where the class of allowed models was restricted to universal Horn formulas.

Computing education. In 2011, the theory group continued its work on the „Scratch project" . Its objective is to find out to which extent it is possible to convey basic programming and algorithmic skills, by (simply) using a specifically designed tool for designing computer animations and computer games in art courses. The tool used is Scratch, which was developed at MIT. First findings had shown that, in contrast to our assumptions, it is easier for children to use message passing (for structuring a distributed program) than to use loops (as a means of abstraction). In a new project, the theory group is investigating why the Annual „Software Challenge" , a programming contest for high school students organized by the group lead by Professor Schimmler and aimed at attracting talented students, has been such a success in recent years.

Personnel

Head of the group: Prof. Dr. Th. Wilke; Secretary: H. Capell (15 percent), F. Lorenz, D. Patz (15 percent)
Technical Staff: Th. Heß (50%)

Scientific Staff:

Dipl.-Math. S. Eggert	01.01.-31.12.2011		CAU
M.Sc. I. Khan	01.01.-31.07.2011		DAAD
Dr. rer. nat. K. O. Kürtz	01.01.-31.03.2011		CAU
Dipl.-Math. S. Preugschat	01.01.-31.12.2011	(50%)	CAU
Dipl.-Math. T. Radtke (75 percent)	01.01.-31.12.2011		ISH
Dr. H. Schnoor	01.01.-31.12.2011		CAU
StR S. Schulmeister	01.01.-31.12.2011	(50%)	CAU

Lectures, Seminars, and Laboratory Course Offers

Summer 2011

Inf-LogInf: Logik in der Informatik, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ S. Preugschat)

MS0101: Kryptographie, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke, H. Schnoor (+ H. Schnoor, S. Eggert)

Inf-PP: Programmierpraktikum, 3 hrs Exercise/Week,
Th. Slawig (+ H. Schnoor, S. Schulmeister)

Inf-FortProg: Fortgeschrittene Programmierung, 3 (+ 2) hrs Exercise (+ Exercises)/Week,
F. Huch (+ Th. Wilke, F. Reck, B. Peemöller)

Winter 2011/2012

Inf-EinfPP: Einführendes Programmierpraktikum, 2 hrs Exercise/Week,
H. Schnoor (+ O. Fleischmann, S. Schulmeister, M. Spönemann)

Inf-TGI: Theoretische Grundlagen der Informatik, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ S. Eggert, Th. Wilke)

MS0102: Automaten, Logiken, Spiele, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ S. Preugschat)

Third-Party Funds

DAAD, *A/06/90283*, 01.03.-31.07.2011 (4.697,50 EUR)
Innovationsstiftung Schleswig-Holstein, *Wenn Bilder laufen lernen, ist Informatik nicht weit!*, 16.06.2010-30.04.2012 (133080 EUR)
b+m Informatik AG, *Schnupperstudium Informatik*, 17.-21.10.2011 (476,00 EUR)
DiWiSH, *Wenn Bilder laufen lernen, ist Informatik nicht weit!*, 01.01.-31.12.2011 (1.074,85 EUR)
ESN, *Wenn Bilder laufen lernen, ist Informatik nicht weit!*, 01.01.-31.12.2011 (1.190,00 EUR)

Further Cooperation, Consulting, and Technology Transfer

Cooperation with other groups:

Trier (Prof. Dr. Ralf Küsters),

Hannover (Prof. Dr. Heribert Vollmer),

Rochester (Prof. Dr. Edith Hemaspaandra),

Marseille (Prof. Dr. Nadia Creignou),

Paris (Prof. Dr. Arnaud Durand),

Krakow (Prof. Dr. Piotr Faliszewski),

Jerusalem (Prof. Orna Kupferman),

Houston (Prof. Moshe Y. Vardi),

and Sydney (Prof. Dr. Ron van der Meyden).

Diploma, Bachelor and Master Theses

A. Mattal, *Kompakte Darstellung von Spielen,* 20.08.2011
K. Balzer, *Unmöglichkeitsresultate zur Wahlmanipulation in der Praxis,* 30.09.2011
H. Georg, *Fotoverschlüsselung in Browsern,* 30.09.2011
Th. J. Jensen, *Verteilter Abgleich und verteilte Sicherung von Daten,* 28.09.2011
A. Koch, *Ein Mittelsmannangriff auf ein digitales Signiergerät,* 17.09.2011
C. K. Liebchen, *Fuzzing für PDF-Betrachter,* 26.09.2011
S. Pfreundschuh, *Identity-Based Cryptography in Haskell,* 10.10.2011

Publications

Published in 2011

R. Küsters, Th. Wilke, *Moderne Kryptographie. Eine Einführung,* Vieweg + Teubner, (2011)
S. Fogarty, O. Kupferman, M.Y. Vardi, Th. Wilke, *Unifying Büchi Complementation Constructions,* CSL 2011, 248 - 263 (2011)
S. Eggert, R. van der Meyden, H. Schnoor, Th. Wilke, *The Complexity of Intransitive Noninterference,* Security and Privacy 2011, 196 - 2011 (2011)
E. Hemaspaandra, H. Schnoor, *Minimization for Generalized Boolean Formulas,* IJCAI 2011, 566 - 571 (2011)
E. Hemaspaandra, H. Schnoor, *A Universally Defined Undecidable Unimodal Logic,* MFCS 2011, 364 - 375 (2011)
M. Bauland, M. Mundhenk, T. Schneider, H. Schnoor, I. Schnoor, H. Vollmer, *The tractability of model checking for LTL: The good, the bad, and the ugly fragments,* ACM Transactions on Computational Logic, **12**, 1301 - 1328 (2011)

Presentations

Th. Wilke, *Functional Programs for Regular Expression Matching (invited talk),* Developments in Language Theory, Mailand, Italy, 19.-22.07.2011
Th. Wilke, *Prophetic Automata (invited talk),* Games Workshop, Paris, France, 31.08.-03.09.2011
H. Schnoor, *Epistemic, Strategic ATL* with Explicit Strategies,* Dagstuhl-Seminar, Wadern, Deutschland, 06.-11.03.2011

E. Hemaspaandra, H. Schnoor, *Minimization for Generalized Boolean Formulas,* IJCAI 2011, Barcelona, Spanien, 16.-22.07.2011

E. Hemaspaandra, H. Schnoor, *A Universally Defined Undecidable Unimodal Logic,* MFCS 2011, Warschau, Polen, 22.-26.08.2011

S. Eggert, R. van der Meyden, H. Schnoor, Th. Wilke, *The Complexity of Intransitive Noninterference,* Security and Privacy 2011, Oakland, USA, 22.-25.05.2011

Further Activities and Events

» Th. Wilke has been a member of the Council of the European Association for Theoretical Computer Science.

» Th. Wilke has been vice speaker of the division Grundlagen of the Gesellschaft für Informatik .

» Th. Wilke has been a member of the editorial boards of the following journals and series: Fundamenta Informaticae, Formal Methods in System Design, Lecture Notes in Logic.

» Th. Wilke was co-chair of the programme committee of STACS 2012.

» Th. Wilke served on an evaluation panel for the INRIA theme „Programs, Verification and Proofs" .

» Th. Wilke consulted for the curriculum „Kunst und Informatik" .

» Th. Wilke was member of the jury for „Bundeswettbewerb Informatik" .

» Organization of several workshops for computer science and art teachers.

» Organization of one week Schnupperstudium Informatik.

» Organization of a computer animation contest for schools in Schleswig-Holstein.