Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2007
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2007
Espoo 2008 HUT-TCS-Y2007

ANNUAL REPORT FOR THE YEAR 2007

Harri Haanpää (Ed.)

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2007
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2007
Espoo 2008 HUT-TCS-Y2007

ANNUAL REPORT FOR THE YEAR 2007

Harri Haanpää (Ed.)

Helsinki University of Technology
Department of Computer Science and Engineering
Laboratory for Theoretical Computer Science

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietojenkäsittelyteorian laboratorio

Distribution:
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O.Box 5400
FI-02015 TKK, FINLAND
Tel. +358 9 451 1
Fax. +358 9 451 3369
E-mail: lab@tcs.tkk.fi
URL: http://www.tcs.tkk.fi/

Multiprint Oy
Espoo 2008

ABSTRACT: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2007.

KEYWORDS: personnel, teaching, research, activities, publications

CONTENTS

1 INTRODUCTION

Helsinki University of Technology (TKK) re-organized its internal structure as of January 1, 2008. TKK's twelve departments consisting of laboratories were re-arranged into four faculties that consist of departments. The Laboratory for Theoretical Computer Science joined together with the former Laboratory of Computer and Information Science to form the Department of Information and Computer Science in the Faculty of Information and Natural Sciences. Hence, this is the last annual report of the Laboratory for Theoretical Computer Science.

In 2007 the international publication record of the laboratory stayed relatively strong (26 papers in international conferences and 7 articles in peer-reviewed international journals) although a major change took place in the staff: Prof. Hannu H. Kari left TKK and started as the Research Director of the National Defence University as of April 1, 2007. A new professorship in distributed computation was opened and it received 11 applicants but the final decisions on the nomination are made in 2008.

This change caused some variation in the personnel. While the number of other permanent academic staff (three professors and two teaching researchers) and technical personnel (secretaries and systems support) remained stable, the number of researchers and research assistants decreased slightly in the other half of the year. Out of the almost 2 M€ total budget of the laboratory in 2007, just over 0.6 M€ were operational funds provided by the university and the rest was procured by individual research proposals. The amount of external funding indicates that the laboratory is an attractive partner for research investment. However, high dependence on external funding takes up a considerable amount of time and effort that could more profitably be used in actual research work.

In 2007 the Academy of Finland commissioned an international evaluation of computer science research in Finland 2000–2006 (Publications of the Academy of Finland 8/07). The results of the evaluation give an opportunity to recap the main activities of the laboratory during recent years. The strategy of the laboratory emphasizing doctoral education and high quality research has been very successful especially when considering the low number of permanent academic staff and the humble level of basic funding. During the evaluation period 2000–2006 16 doctoral dissertations were completed in the laboratory and, for example, 72 international journal articles and 220 international conference papers were published. The evaluation report concludes that "the impact of their research is outstanding both in scientific communities and industries". These kinds of results are possible only with an enormous commitment of the staff and students in the laboratory and their passion for high level research.

More detailed information on the personnel, education, research, visits, and publications in the laboratory in 2007 can be found in the following sections.

2 PERSONNEL

The personnel of the Laboratory for Theoretical Computer Science in 2007 is listed in this section. The personnel are grouped into a number of categories. With the exception of Section 2.2 (Docents), whose contents overlap the other categories to some extent, no person appears in two categories.

2.1 Professors

Kari, Hannu H.; D.Sc. (Tech.), until March

Niemelä, Ilkka; D.Sc. (Tech.), Head of Laboratory

Nyberg, Kaisa; D.Phil., on partial leave

Orponen, Pekka; D.Phil.

Pastor-Satorras, Romualdo; Visiting professor, in August

2.2 Docents

Heljanko, Keijo; D.Sc. (Tech.), Docent in Model Checking

Husberg, Nisse; D.Sc. (Tech.), Docent in Verification

Janhunen, Tomi; D.Sc. (Tech.), Docent in Computational Logic

Kari, Hannu H.; D.Sc. (Tech.), Docent in Mobility Management in Computer Networks, from July 2007

Lipmaa, Helger; Ph.D., Docent in Cryptology

Ukkonen, Esko; D.Phil., Docent in Theoretical Computer Science, Academy Professor, Professor in Computer Science, University of Helsinki

Varpaaniemi, Kimmo; D.Sc. (Tech.), Docent in Formal Verification Methods for Parallel and Distributed Systems

2.3 Staff

Haanpää, Harri; D.Sc. (Tech.), Teaching researcher

Huhtala, Anttoni; Stud. (Tech.), System administrator, from June

Janhunen, Tomi; D.Sc. (Tech.), Teaching researcher

Kauppila, Minna; Secretary

Kotimäki, Jaakko; Stud. (Tech.), System administrator

Lassila, Eero; Lic.Sc. (Tech.), Laboratory manager, on leave from September

Lemmilä, Ulla; Secretary, part-time

Valkonen, Jukka; M.Sc. (Tech.), Researcher until August, laboratory manager from September

2.4 Researchers

Brumley, Billy Bob; M.Sc. (Tech.), Researcher

Dubrovin, Jori; M.Sc. (Tech.), Researcher

Heljanko, Keijo; D.Sc. (Tech.), Academy Research Fellow

Hermelin, Miia; Lic.Sc. (Tech.), Researcher

Hietalahti, Maarit; Lic.Sc. (Tech.), until July

Hyvärinen, Antti; M.Sc. (Tech.), Researcher

Junttila, Tommi; D.Sc. (Tech.), Project manager

Järvisalo, Matti; Lic.Sc. (Tech.), Researcher

Kullberg, Tuulia; M.Sc. (Tech.), Researcher, on leave from 30 May

Lagutin, Dmitrij; M.Sc. (Tech.), Researcher

Laur, Sven; M.Sc., Researcher

Lundberg, Janne; D.Sc. (Tech.), Researcher, until 14 August

Oikarinen, Emilia; Lic.Sc. (Tech.), Researcher

Schumacher, André; Dipl.-Inf., Researcher

Syrjänen, Tommi; Lic.Sc. (Tech.), Researcher

Tauriainen, Heikki; D.Sc. (Tech.), Researcher

Wieringa, Siert; B.Sc., Researcher, from October

2.5 Research Assistants

Brunčák, Radovan; from June until August

Ellonen, Sakari; Stud. (Tech.), from June

Hakala, Risto; M.Sc. (Tech.)

Hänninen, Aleksi; Stud. (Tech.)

Koskimies, Matti; Stud. (Tech.), from 26 February until 1 April and from May

Kylmälä, Lea; Stud. (Tech.), from June until August and from October

Kähkönen, Kari; Stud. (Tech.), from June

Lahtinen, Jussi; Stud. (Tech.), from June

Lampinen, Jani; Stud. (Tech.), from June

Launiainen, Tuomas; Stud. (Tech.), from 27 April

Liedes, Sami; Stud. (Tech.), from February until March and from June until August

Nuorvala, Ville; Stud. (Tech.), until March

Ojala, Vesa; Stud. (Tech.)

Peltonen, Juhana; Stud. (Tech.), from June until August

Rusanen, Antti; Stud. (Tech.), until July

Saarela, Aleksi; Stud. (Tech.), from June until August

Savola, Petri; Stud. (Tech.), from June until August

Suvilehto, Jyry; Stud. (Tech.), from June until August

Thaler, Thorn; from June until August

Tuominen, Antti; Stud. (Tech.), until 4 January

2.6 Teachers

Teachers who are not professors, docents, staff, researchers, or research assistants at the Laboratory for Theoretical Computer Science are listed in this section along with the course with which they have been involved.

Hartmann, Alexander; Professor, T–79.7003

Herttua, Ilkka; Stud. (Tech.), T–79.5303

Oza, Nilay; D.Sc. (Tech.), T–0.7050

Tynjälä, Teemu; Lic.Sc. (Tech.), T–79.5303

Östergård, Patric; Professor, D.Sc. (Tech.) T–79.5203

3 EDUCATIONAL ACTIVITIES

The aim of the education at the undergraduate level is to give the students basic insight into theoretical computer science as well as into applying theoretical results to practice. At the postgraduate level the aim is to deepen the understanding, often in context of some particular theoretical questions.

3.1 Courses Arranged in 2007

In 2007, the following courses were arranged.

Below, the code, English name, number of credits, season, lecturer(s), teaching assistants, and a description of each course are given. The teaching assistants are listed in parentheses.

3.2 Spring 2007

T–0.7050 Introduction to Postgraduate Studies in Computer Science (2 cr)

Harri Haanpää, Tomi Janhunen, and Nilay Oza

Introduction to the facilities and research skills required for successful postgraduate studies in the Department of Computer Science and Engineering.

T–79.3001 Logic in computer science: foundations (4 cr)

Tomi Janhunen (Emilia Oikarinen; Antti Hyvärinen, Matti Järvisalo)

Propositional and predicate logic, their syntax, semantics and proof theory. Applications of logic in computer science.

T–79.4001 Seminar on theoretical computer science (3 cr)

Pekka Orponen

Annually varying topics of current interest in the field. In Spring 2007, fundamental techniques in the design and analysis of algorithms for distributed computation.

T–79.4301 Parallel and Distributed Systems (4 cr)
Keijo Heljanko (Tuomas Launiainen)

Modelling of parallel and distributed systems. Computer aided verification of properties of systems.

T–79.5101 Advanced Course in Computational Logic (4 cr)
Ilkka Niemelä (Matti Järvisalo)

Basics of modal logic. Current applications in computer science.

T–79.5202 Combinatorial Algorithms (4 cr)
Harri Haanpää (Aleksi Hänninen)

Basic algorithms and computational methods for combinatorial problems. Combinatorial structure generation (e.g. permutations). Search methods. Graph algorithms and combinatorial optimization. Symmetries of combinatorial structures.

T–79.5203 Graph Theory (5 cr)
Patric Östergård and Petteri Kaski (Jori Dubrovin)

Introduction to graph theory. Trees, planar graphs and digraphs. Graph coloring. Random graphs. Algorithms for central graph problems. Applications. Also with code S–72.2420.

T–79.5204 Combinatorial Models and Stochastic Algorithms (6 cr)
Pekka Orponen

Stochastic methods such as MCMC sampling, simulated annealing and genetic algorithms are currently at the forefront of approximate techniques for dealing with computationally demanding problems. This course presents these algorithms and their underlying theory, with the goal of learning to apply the methods to novel problems and achieving a broad understanding of their common foundations.

T–79.5301 Reactive systems (4 cr)
Heikki Tauriainen

Specification and verification of reactive systems with temporal logic. Basics of computer-aided verification methods and their algorithms.

T–79.5303 Safety Critical Systems (4 cr)
Ilkka Herttua and Teemu Tynjälä

A basic course on Safety Critical Systems and the use of Formal Methods to verify and validate safety systems. Subjects covered this year are: Requirement Engineering, Hazard/Risk Analysis Methods, System Reliability, Safety Critical Hardware/Software and Verification/Validation Tools.

T–79.5401 Special course in mobility management (2–10 cr)
Hannu H. Kari

Special problems of mobility management in wireless networks. In Spring 2007, arranged in conjunction with T–79.7001.

T–79.5501 Cryptology (5 cr)
Kaisa Nyberg (Miia Hermelin)

The course deals with the mathematical basis of modern cryptographic algorithms. It can be taken as a special course in advanced level undergraduate and graduate studies of computer science and mathematics.

T–79.7001 Postgraduate course in theoretical computer science (2-10 cr)
Hannu H. Kari (Dmitri Lagutin)

Current research problems in theoretical computer science. In Spring 2007, arranged in conjunction with T–79.5401.

T–79.7002 Individual studies (1–10 cr)
T–79 professors

The contents and extent of the course are to be agreed with a professor before commencing the course.

3.3 Autumn 2007

T–79.1001 Introduction to theoretical computer science T (4 cr)
Harri Haanpää (Tommi Syrjänen; Lea Kylmälä, Tuomas Launiainen, Emilia Oikarinen, Petri Savola)

Finite automata and regular languages. Context-free grammars and pushdown automata. Context-sensitive and unrestricted grammars. Turing machines and computability.

T–79.1002 Introduction to theoretical computer science Y (2 cr)
Harri Haanpää (Tommi Syrjänen; Lea Kylmälä; Tuomas Launiainen, Emilia Oikarinen, Petri Savola)

Finite automata and regular languages. Context-free grammars.

T–79.4201 Search problems and algoritms (4 cr)
Ilkka Niemelä and Pekka Orponen (André Schumacher)

Search spaces and search methods. Backtracking, local and heuristic search. Representing and solving search problems using propositional satisfiability, constraint programming and integer programming techniques.

T–79.4501 Cryptography and data security (4 cr)
Kaisa Nyberg (Billy Brumley, Risto Hakala)

Data and communications security. Principles of cryptographic security. Symmetric cryptosystems. Stream ciphers. Block ciphers: DES, IDEA, AES. Modes of operation. Asymmetric cryptosystems. Digital signatures. Authentication and key agreement. Applications of cryptography: SSL, TLS, IPSec, GSM, Bluetooth.

T–79.5001 Student project in theoretical computer science (5 cr)
T–79 professors and teaching research scientists

Independent student project on a subject from the field of theoretical computer science.

T–79.5102 Special course in computational logic (4 cr)
Tomi Janhunen (Antti Hyvärinen)

Knowledge representation, reasoning and decision-making. Automated reasoning.

T–79.5103 Computational complexity theory (5 cr)
Ilkka Niemelä (Matti Järvisalo)

NP-completeness. Randomized algorithms. Cryptography. Approximation algorithms. Parallel algorithms. Polynomial hierarchy. PSPACE-completeness.

T–79.5201 Discrete structures (4 cr)
Pekka Orponen

Annually varying topics concerned with the basic structures and methods of computer science theory. In Autumn 2007, probabilistic combinatorics, i.e., the characteristics of random ensembles of combinatorial structures such as graphs, set systems, codes, geometric arrangements etc.

T–79.5302 Symbolic model checking (4 cr)
Tommi Junttila

Model checking is a method for analyzing whether the dynamic behavior of a hardware or software system meets its specification. The course T–79.5302 considers two famous techniques for symbolic model checking: binary decision diagram manipulation and bounded model checking.

T–79.5502 Advanced course in cryptology (5 cr)
Kaisa Nyberg (Sven Laur)

Cryptographic security models and provable security.

T–79.7001 Postgraduate course in theoretical computer science (2-10 cr)
Ilkka Niemelä

Varying subjects in theoretical computer science; in Autumn 2007, Propositional Proof Complexity. Propositional proof complexity studies the lengths of proofs in propositional logic. It is an area that is related to major open questions of computational complexity theory and to practical properties of automated theorem provers such as satisfiability checkers.

T–79.7002 Individual studies (1–10 cr)
T–79 professors

The contents and extent of the course are to be agreed with a professor before commencing the course.

T–79.7003 Research course in Theoretical Computer Science (6 cr)
Prof. Alexander Hartmann (University of Oldenburg)

The course gives an introduction to studying the typical behavior of algorithms for solving NP-complete problems over ensembles of random

instances, similar to the way phase transitions are studied in statistical physics. The new statistical physics approach to computational complexity has helped to understand the behavior of NP-complete systems better and has led to the design of new efficient algorithms.

4 RESEARCH ACTIVITIES

The research activities of Laboratory for Theoretical Computer Science in 2007 are summarized in this section. A major part of the research has been funded by the Academy of Finland with substantial support from Helsinki Graduate School in Computer Science and Engineering (HeCSE). Particularly the more applied research has also been funded by non-academic partners, often in conjunction with the Finnish Funding Agency for Technology and Innovation (TEKES). Table 1 lists the externally funded projects in the laboratory that were ongoing in 2007.

4.1 Computational Logic

The work in the computational logic group involves a number of interacting research themes described below in more detail. In addition to basic research the activities involve more applied research done mainly in the TEKES and industrially funded MODSAFE, LIME, and SMUML projects.

Extensions and Tool Development for Rule-Based Constraint Programming
Tomi Janhunen, Ilkka Niemelä, and Tommi Syrjänen

The development of declarative semantics, in particular the stable model semantics, for logic programming type rules has led to an interesting new approach to solving computationally challenging problems. In the novel answer set programming paradigm (ASP) a problem is solved by devising a logic program whose answer sets correspond to the solutions of the problem and then using an efficient answer set solver to find answer sets of the program. The research group has developed an efficient ASP system called SMODELS[1] which is used in dozens of research groups worldwide. The on-going work includes the development of extensions of rule-based constraint language, tools for program development in ASP, and applications of such extended rule languages. In 2007, we have developed a number of auxiliary tools[2] for ASP [51], e.g., for managing ASP program modules. These tools exploit the internal file format of the SMODELS system. There are also other similar file formats and the development of an unified *intermediate language* for ASP was initiated by the survey in [14].

Translation-Based Techniques for Knowledge Representation
Tomi Janhunen and Emilia Oikarinen

The research in this area concentrates on various knowledge representation formalisms and transformations between them. As part of this research, we

[1] http://www.tcs.hut.fi/Software/smodels/
[2] http://www.tcs.hut.fi/Software/asptools/

Table 1: Ongoing projects in 2007

Project name Head Duration Funding source Researchers (in 2007)
Advanced Constraint Programming Techniques for Large Structured Problems (ACPT) Niemelä 1.1.2005–31.12.2007 Academy of Finland Tomi Janhunen, Antti Hyvärinen, Matti Järvisalo, Lea Kylmälä, Emilia Oikarinen, Tommi Syrjänen
Testing, Verification, and Synthesis of Distributed Systems Heljanko 1.1.2006–31.12.2008 Academy of Finland Keijo Heljanko
Cryptology and data-mining (CRYDAMI) Nyberg 1.1.2004–31.12.2007 Academy of Finland Sven Laur
Symbolic Methods for UML Behavioural Diagrams (SMUML) Niemelä 1.1.2006–31.12.2007 TEKES Tommi Junttila, Heikki Tauriainen, Jori Dubrovin, Sami Liedes, Vesa Ojala, Juhani Peltonen
Securing IP-based network infrastructures using Packet Level Authentication technique (PLA) Kari 1.1.2006–31.12.2007 TEKES Billy Brumley, Dmitri Lagutin, Janne Lundberg
Interconnected Broadband Home Networks (INHONETS) Nyberg 1.1.2006–31.12.2007 TEKES Billy Brumley, Aleksi Toivonen, Jukka Valkonen
Lightweight formal Methods for distributed component-based Embedded systems (LIME) Niemelä 1.10.2007–30.9.2009 TEKES Keijo Heljanko, Jori Dubrovin, Kari Kähkönen, Jani Lampinen
Stream cipher cryptanalysis Nyberg 1.6.2006–31.12.2008 MATINE Risto Hakala, Miia Hermelin
Ad Hoc Networks Nyberg 1.1.2006–31.12.2007 The Finnish Defence Forces Risto Hakala, Maarit Hietalahti, Aleksi Hänninen
Model-Based Safety Evaluation of Automation Systems (MODSAFE) Niemelä 1.1.2007–30.9.2009 VYR Keijo Heljanko, Matti Koskimies, Jussi Lahtinen
CAV Heljanko 1.1.2007–31.12.2009 Teknologiateollisuuden 100-vuotissäätiö Matti Koskimies, Kari Kähkönen, Jani Lampinen, Tuomas Launiainen

have earlier developed a linear and faithful but *non-modular* translation from Lifschitz' parallel circumscription into disjunctive logic programs. On one hand, this enables the use of disjunctive ASP solvers for computing minimal models. On the other hand, varying and fixed atoms can be advisedly used in disjunctive logic programs in order to obtain more concise problem encodings. In 2007, the linear translation was generalized for *prioritized circumscription* [30] and the respective priority classes were integrated to the implementation, i.e., the translator CIRC2DLP[3] for disjunctive logic programs [56]. As regards experimental evaluation, we use *model-based diagnosis* of digital circuits as the main benchmark problem.

Modularity in Answer Set Programming
Tomi Janhunen and Emilia Oikarinen

The overall goal of this research is to bring good software engineering practise, such as modular program development, to the realm of ASP. To this end, we have previously developed a module architecture for logic programs. The architecture is fully compatible with answer set semantics and the respective notion of *modular equivalence* enables substitutions of equivalent modules. In 2007, we generalized the module architecture for further classes of logic programs, namely SMODELS programs [29] and disjunctive logic programs [15]. Moreover, we took our translation-based verification technique [3] into reconsideration and tailored it to the case of modular equivalence [31]. Capabilities to deal with program modules were also integrated to LPEQ [52] which implements the translation for comparing of two programs. This research [27,28] will be part of Emilia Oikarinen's doctoral dissertation.

Boolean Satisfiability Checking
Matti Järvisalo, Tommi Junttila, and Ilkka Niemelä

The Davis–Putnam–Logemann–Loveland (DPLL) method is the basis of typical state–of–the-art solvers aimed at solving real–world instances of the propositional satisfiability problem (SAT). Most DPLL based SAT solvers incorporate clause learning, which has proven to increase the efficiency of DPLL. The techniques for making decisions, i.e., branching, play a central role in complete methods, such as DPLL, for solving structured SAT instances. In practice, there are cases when DPLL solvers benefit from limiting the set of variables the solver is allowed to branch on to so called input variables. Theoretically, however, we have previously shown that restricting branching to input variables implies a super-polynomial increase in the length of the optimal proofs for DPLL (without clause learning), and thus input-restricted DPLL cannot polynomially simulate DPLL. Extending this previous work on the proof complexity theoretic effect of restricting branching, in 2007 we settled the case of DPLL with clause learning: even with unlimited restarts, input-restricted branching clause learning DPLL cannot simulate DPLL (even without clause learning) [16, 17, 21]. The effects of structure-based restrictions on branching was also evaluated experimentally [20]. A selection of small hard SAT instances used in the experimental evaluation were submitted to the SAT Competition 2007 [63]. Additionally,

[3] http://www.tcs.hut.fi/Software/circ2dlp/

based on the theoretical and experimental results, M.J. finished his Licentiate's thesis [39, 43] in 2007.

As an application of the underlying ideas used in the theoretical work on branching restrictions, in collaboration with Emilia Oikarinen, M.J. introduced the Extended ASP Tableaux tableau method for normal logic programs as a counter part for the well-known Tseitin's Extended Resolution proof system for SAT. The resulting publication [18] received the ICLP 2007 Best Student Paper Award at the 23rd International Conference on Logic Programming.

Grid-Based Search Techniques

Antti Hyvärinen, Tommi Junttila, and Ilkka Niemelä

Computing grids differ in many aspects from traditional distributed environments. For example, the communication delays, failure rates and heterogeneity of the computing elements rise challenges which are not experienced elsewhere. The research concentrates currently on solving difficult instances of the propositional satisfiability problem (SAT). We have studied the suitability of newly developed methods for distributed SAT solving by developing an implementation for a realistic setting[4]. In 2007, our research has also extended to simulated environments. The related experiments have deepened the understanding of the different approaches. For example, statistical analysis has directed the implementation towards a more robust approaches while at the same time helped to understand some observations made from the grid environment. Our fruitful cooperation with NorduGrid, the Finnish IT Center for Science (CSC), and Globus has continued and the first-hand experience obtained from these sources and our own computing infrastructure has helped to guide the research in practically interesting areas.

Computer Aided Verification Theory

Keijo Heljanko, Sakari Ellonen, Matti Koskimies, Kari Kähkönen, Jani Lampinen, Tuomas Launiainen, and Siert Wieringa

The aim of research on this topic is to develop methods to support the design of complex concurrent and reactive software systems such as embedded systems, data-communications protocol software, and server software for reactive web based services. The main goal is to develop verification theory and tools for software systems built from software components.

The approach involves solving a number of issues that require basic research in theory of computer aided verification. The long term goal is to create computer aided verification tools, which are applicable to a wide class of engineering problems on embedded software and communication protocols. These in turn will aid the development of distributed systems with less bugs in them and created with a smaller development effort than with traditional methods.

The main achievement in 2007 was the book manuscript created together with Prof. Javier Esparza from TU München Germany on model checking theory. The book is expected to be available in March 2008. Also this project has contributed to the technical report [37] on model checking of UML state

[4] http://www.tcs.hut.fi/Software/satu/

machines. The research group has extended quite significantly with many new recruits in 2007. The group has done research on the use of SAT and SMT solvers to solve various problems in verification, more efficient symbolic model checking methods for safety properties, as well as on finding minimal unsatisfiable cores of SAT formulas. The results of these studies will be published in the year 2008.

Model-Based Safety Evaluation of Automation Systems (MODSAFE)

Ilkka Niemelä, Keijo Heljanko, Matti Koskimies, and Jussi Lahtinen

The assurance of automation systems and devices for use in critical applications requires careful safety assessment. In this project methods based on model checking are developed and applied in the safety analysis of nuclear power plant (NPP) safety automation. The general objectives of the project are: development of methods and procedures for model based safety evaluation of NPP automation; application of the methods in selected case studies; evaluation of suitability of model checking methods for NPP automation analysis; operationalization of model based safety evaluation as part of safety cases of safety automation systems; and development of recommendations for the practical application of the methods. This research project is part of the SAFIR 2010 program and is done in cooperation with VTT.

Lightweight Formal Methods for Distributed Component-Based Embedded Systems (LIME)

Ilkka Niemelä, Keijo Heljanko, Kari Kähkönen, and Jani Lampinen

Embedded software is already employed in a large range of applications and its use is increasing rapidly. Interesting areas include home electronics from set-top boxes to intelligent homes of the future equipped with sensor networks. Typically embedded software is to some degree safety critical (e.g. satellites, cars, health care) and often it should work relatively autonomously without supervision by an administrator. In the future systems are becoming larger and more complicated and are likely to be composed out of components that need to be inter-operable and are potentially provided by different subcontractors. All of the above means a fully new level of quality of software needs to be achieved. For this new software development and validation methods are needed for designing sufficiently robust software cost-efficiently.

The main objective of the project is to simplify the adoption of new design and validation methods for distributed embedded software components in practice. The project proposes a stepwise introduction of lightweight formal methods that act as a key enabling methodology for creating embedded software out of components. Interface specifications and design models (e.g., using a UML state machine notation) of the software can act as specifications according to which the software component suppliers will design requested components in a real programming language. In addition, the design model can act as an environment model in which the real implementation of the embedded software component can be simulated, tested, and validated even before the rest of the system's implementation is available.

This Tekes Ubicom program project has started in October 2007, with initial two years of funding granted.

Symbolic Methods for UML Behavioural Diagrams (SMUML)

Ilkka Niemelä, Tommi Junttila, Heikki Tauriainen, Jori Dubrovin, Vesa Ojala, Juhani Peltonen, and Sami Liedes

The increasing size and level of concurrency of software systems poses new challenges for obtaining reliable software and cost effectiveness in the software process. Especially the analysis of the dynamic (behavioral) aspects of a software system in its various development phases is gaining more importance. The sooner the incorrect behaviors of a software system can be detected, the cheaper it is to correct them.

This project studies the analysis of dynamic aspects of software system models described in the Unified Modelling Language (UML). In UML such aspects are described with so-called behavioral diagrams, e.g. state machine and message sequence diagrams. Important properties to be analyzed include e.g. that systems do not deadlock, violate assertions, or perform unwanted implicit consumption of messages. In 2007, we have (i) developed a translation from UML models to the input language of the symbolic model checker NuSMV [36, 50], (ii) extended the symbolic step encoding technique for exploiting the concurrency of systems to work with the object-oriented and message passing aspects of UML models [37], and (iii) generalized the symbolic translation to exploit non-Boolean constraints available in modern satisfiability modulo theories (SMT) solvers [49, 53].

To make UML models more amenable to analysis, we have also designed and implemented model reduction techniques based on UML state machine slicing [40, 58], data abstraction using user-defined type libraries, and automatic counterexample-guided refinement of abstract UML models generated by abstracting concrete integers with integer intervals [57, 59, 60]. We have also implemented a tool to assist in the design of user-defined abstract type libraries [61].

Graph Isomorphism and Canonical Labeling of Graphs

Tommi Junttila

The problem of deciding whether two graphs are isomorphic, as well as its generalization of transforming a graph into a canonical form (i.e. canonically labeling the vertices of a graph in a way that two graphs are isomorphic if and only if their canonical forms are identical), are central problems when classifying combinatorial objects up to isomorphism. They are also applied in approaches for reducing the space and time requirements of explicit state model checking algorithms by pruning out symmetric (isomorphic) state configurations. Together with Petteri Kaski (University of Helsinki), we have developed new data structures and search space pruning techniques for solving the canonical labeling problem for large and sparse graphs [19].

4.2 Computational Complexity and Combinatorics

Work in the area of computational complexity and combinatorics at the laboratory is structured in three research groups, *Computational Models and Mechanics*, *Coding Theory and Optimisation*, and *Distributed Algorithmics*.

Computational Models and Mechanics

Petri Savola, Sakari Seitz and Pekka Orponen

The group studies methods for the analysis and solution of computational problems in structurally complex state spaces, such as large nonuniform networks, spin glass models, and energy landscapes arising from combinatorial optimisation problems.

The main focus of this work in 2007 continued to be the theory and applications of stochastic search methods. This work was pursued in collaboration with Mr. Sakari Seitz, Doc. Mikko Alava from the TKK Laboratory of Physics, Dr. Petteri Kaski from the Helsinki Institute for Information Technology (former graduate of the TCS laboratory), and the group of Prof. Erik Aurell at KTH Royal Institute of Technology, including Dr. Supriya Krishnamurthy and Mr. John Ardelius. Some results of this work are presented in the technical report [35], which discusses the unexpected efficiency on generically solvable random K-SAT instances of a simple local search technique that never goes "uphill" in the energy landscape. The presented experimental results go against widely-accepted conjectures on the structure of the K-SAT energy landscape near the satisfiability transition threshold.

In June thru August, the group was joined by Mr. Petri Savola, who continued his work from the previous summer on combinatorial methods for probing the structure of spin glass energy landscapes.

In August, the group hosted a visit by Prof. Romualdo Pastor-Satorras from the Universitat Politècnica de Catalunya, who gave a series of lectures providing an *Introduction to Complex Networks*, and for August thru October the group was visited by Prof. Alexander Hartmann from the Universität Oldenburg who taught a joint computer science/physics graduate course on *Phase Transitions in Optimisation Problems*.

Also in 2007, a major survey article on graph clustering methods [7] by former group member Satu Elisa Schaeffer was published. The article, which is based on Dr. Schaeffer's doctoral dissertation work, was largely written in 2006 before Dr. Schaeffer took up a permanent position at the Universidad Autónoma de Nuevo León, Mexico.

Coding Theory and Optimisation

Harri Haanpää

The group works on computational methods for solving problems in combinatorics. A typical approach is to use a computer to generate, up to isomorphism, all possible candidate solutions. Coding theory and graph theory are a rich source of problems of this type.

In 2007, Harri Haanpää kept working on computational methods for finding full-rank tilings of small primary Abelian groups in co-operation with Prof. Patric Östergård of the EE department and Dr. Sándor Szabó of the University of Pécs.

This group has contributed to the journal articles [2, 4].

Distributed Algorithmics

Harri Haanpää, Antti Rusanen, André Schumacher, Thorn Thaler and Pekka Orponen

The group applies combinatorial and complexity-theoretic methods to the solution of algorithmic problems in distributed systems.

In the first part of 2007, the group's work was focused on distributed graph-theoretic approaches to the problem of lifetime maximisation in data-gathering sensor networks. Two methods were developed for this task: one based on a distributed breadth-first search for minmax transmission power paths connecting sensor nodes to the given base station node, and another one based on a distributed binary search over the range of feasible transmission power levels in the network. Both methods were implemented on the widely used ns-2 network simulator and compared experimentally against previously published methods, with excellent results. This work was pursued collaboratively by Harri Haanpää, André Schumacher and Pekka Orponen, and the group was also joined from June thru August by Mr. Thorn Thaler, a visiting M.Sc. student from the Technische Universität Graz. The report on the first method was presented in a conference paper [11] in late 2007, and the report on the second method in a consequent paper in early 2008 (forthcoming).

Later in 2007, focus of the group's work turned towards distributed approximation methods for the so called Network Utility Maximisation model, and their application to problems in sensor networks. Reports on this work are forthcoming in 2008.

Former group member Maarit Hietalahti completed her Lic.Sc. thesis [42] on security and trust relations in mobile networks in the spring of 2007. This work was published as part of the technical report [38]. Also in 2007, the group's M.Sc. student Antti Rusanen obtained a number of promising NP-completeness results on the problem of wireless network localisation via 3-fold visibility coverings of polygons.

4.3 Cryptography

The research on cryptography, led by Prof. Kaisa Nyberg, is divided into three research directions described below.

Cryptanalysis of symmetric primitives
Risto Hakala, Miia Hermelin, Aleksi Hänninen and Kaisa Nyberg

This group develops and implements cryptanalytic methods for different symmetric cryptographic primitives. In 2007 the main focus was on cryptanalysis of stream ciphers.

Kaisa Nyberg attended the Dagstuhl workshop on Symmetric Cryptography and gave a presentation on a linear attack on SOBER-128, which was joint work with Risto Hakala [24], and is a key recovery attack using linear distinguishers. The main observation was that the sign and absolute value of the bias of a linear approximation over the filter function depend on the value of the constant. In the same workshop, a new stream cipher called Shannon was presented. The multidimensional linear cryptanalysis method was applied to Shannon, and the result will be presented at ACISP 2008. A detailed account on this work is given in the Master's thesis by Risto Hakala [44].

A second Master's thesis project in 2007 was done by Aleksi Hänninen. The topic of this work was to use methods from logic programming, such as

SAT solvers, in cryptanalysis of a contemporary stream cipher Trivium. The manuscript was almost completed by the end of the year.

Risto Hakala's and Aleksi Hänninen's work was funded by the Ad Hoc Networks project of the Finnish Defence Forces.

Miia Hermelin continued working on her Ph.D project on the topic of multidimensional linear cryptanalysis. A new tool, called Multi-Walsh transform was presented which allows analysis of linearity properties of multidimensional distributions [25]. Also statistical methods used in multidimensional linear attacks, in particular, extensions of Matsui's Algorithms 1 and 2, were studied and extended. The work of Miia Hermelin was funded by the Scientific Advisory Board for Defence.

Concrete cryptographic security and secure data mining

Sven Laur

The main aim of the CRYDAMI project, funded by Academy of is to study possibility of privacy-preserving techniques in data-mining. Such techniques can be divided into two major research fields: privacy-preserving micro-data publishing and privacy-preserving data aggregation.

Privacy-preserving data aggregation can benefit from cryptographic methods. The problem can be formalized as a secure two- or multiparty computation. Secure computation allows to compute the desired end result (e.g. discover more disease patterns) without revealing no other information. It is possible to distribute the data among several institutions so that no institution can recover any information unless majority of them collude.

Many protocols that are based on homomorphic encryption are private only if a client submits inputs from a limited range. Conditional disclosure of secrets (CDS) helps to overcome this restriction. In a CDS protocol for a set of inputs S, the client obtains server's secret if and only if the client's inputs belong to S and thus the server can guard itself against malformed queries. In [23] Sven Laur and Helger Lipmaa extend the existing CDS protocols to work over additively homomorphic cryptosystems for every set from NP/poly. The new construction is modular and easy to apply. As an example, a new oblivious transfer protocol with log-squared communication and a millionaire's protocol with logarithmic communication is derived. Also a private, universally verifiable and robust multi-candidate electronic voting is presented, where all voters only transmit an encryption of their vote.

Important supporting infrastructure for security is time-stamping that allows to undeniably date digital documents. For example, time-stamping makes possible to audit complex computer systems. Time-stamping can be used to discover and prove existence inside and outside attacks that might compromise secure multiparty computations. In particular, we have refined what is exactly needed for secure time-stamping [10].

Sven Laur submitted the manuscript of his Ph.D. Thesis, "Cryptographic Protocol Design" for pre-examination in October 2007. The pre-examiners are Prof. Phil Rogaway, UCLA Davis, USA, and Prof. Berry Schoenmakers, TU Eindhoven, The Netherlands.

Applications of cryptography in secure networking

Billy Brumley, Maarit Hietalahti, Kaisa Nyberg, Aleksi Saarela, Jukka Valkonen

This topic covers work done by different group members in three different projects: PLA (Billy Brumley, Dmitri Lagutin and Kaisa Nyberg), InHoNets (Billy Brumley and Jukka Valkonen), and Ad Hoc Networks (Maarit Hietalahti and Kaisa Nyberg).

In the PLA project, the Cryptology group contributes in two areas: first, design of efficient certification scheme and, secondly, efficient implementation of elliptic curve cryptography. Also, a brief description of the PLA work completed by the researchers Dmitri Lagutin and Janne Lundberg, from the former Mobility Group led by Prof. Hannu Kari, is included below.

Within the first task the security properties of the PLA certification scheme were analyzed. It was observed that certain canonical mappings on elliptic curves are differentially uniform. On the other hand, the impersonation attack against the implicit certificate scheme of Ateniese and de Medeiros does not work if a differentially uniform mapping is used in the scheme. In the paper written by Billy Brumley and Kaisa Nyberg this phenomenon is analyzed in the slightly more general context of a partially blind signature scheme, which is a new cryptographic primitive that seems to gain security properties from differentially uniform mappings [9].

Billy Brumley also continued collaboration with Kimmo Järvinen from the Signal Processing Laboratory of the EE Department of the TKK, with the goal to improve efficiency of hardware implementation of elliptic curve cryptography [8].

Dmitrij Lagutin and Janne Lundberg from the former Mobility Group worked on designing overall PLA architecture and creating a proof of concept software implementation of PLA for Linux. In addition, other possible uses of PLA were researched. A method for utilizing PLA for controlling incoming connections in the network is described in [22].

A proof of concept software implementation of PLA is available from [1]. It supports both software and hardware based implementations of elliptic curve cryptography.

Within the InHoNets project the researchers of the Cryptology Group continued working on the secure association models in 2007. A comparative survey paper analyzing secure pairing protocols was published [32]. The applicability of the multiparty pairing protocol developed in 2007 to the existing MAC layer radio standards was investigated in [26].

Also efficient implementation of the emerging Bluetooth Simple Pairing standard was investigated by Billy Brumley. Especially the efficiency of the implementation was improved for standard NIST curves. In the paper "Fast Point Decompression for Standard Elliptic Curves" to be published in 2008 (EuroPKI'08), Billy Brumley presents improved algorithms for point decompression which make use of the specialized form of the prime field over which the elliptic curve is defined. The algorithm is applied to 25 standard elliptic curves, including P-192 used in Bluetooth Simple Pairing, in this case resulting in a speedup of 41.7 percent over textbook methods. Software and hardware results are presented.

In addition, the research included methods for establishing joint random-

ness for a group of devices investigated by Aleksi Saarela in collaboration with Nokia Research Center. A draft paper was written including the results from simulations performed in the subtask. The motivation for this work originates from the privacy system of Wibree, but can be applied to improve efficiency of private addresses and session key generation in general.

In the Ad Hoc Networks -project, Maarit Hietalahti developed a key management protocol that handles an arbitrary ad hoc network in two layers. The lower layer is formed by separate clusters. In each cluster, the nodes are at one hop distance from each other. In each cluster, one node acts as a cluster head. The higher layer connects all clusters together by connecting the cluster heads together. The protocol scales very well to large networks where it can be assumed that devices can be grouped in clusters. It was shown that the time taken by this algorithm is proportional to the number of vertices in the spanning tree for the network, which in the average is square root of the number of nodes. In comparison, the time taken by the straightforward algorithm, where one device connects all other devices to distribute a group key is almost the same as the number of nodes [12].

Maarit Hietalahti completed her Licentiate thesis in July [42].

5 CONFERENCES, VISITS, AND GUESTS

5.1 Conferences

This section summarizes the activities of the personnel of the Laboratory for Theoretical Computer Science in conferences and international meetings in 2007. The events are ordered chronologically.

January

Symmetric Cryptography, Dagstuhl Seminar 07021, Schloss Dagstuhl, Germany, January 7-12. Participant: Kaisa Nyberg

33rd International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2007), Harrachov, Czech Republic, January 20-26. Member of programme committee: Pekka Orponen

International Conference on Information Networking 2007 (ICOIN), Estoril, Portugal, January 22-26. Participant: André Schumacher

SASC 2007 Workshop, Bochum, Germany, January 30 - February 2. Participant: Risto Hakala

February

Winter School Artist2 - Motives, Trento, Italy, February 18-24. Participant: Jori Dubrovin

NorduGrid Technical Meeting of ARC Developers, Lund, Denmark, February 18-21. Participant: Antti Hyvärinen

March

The 12th Estonian Winter School on Computer Science 2007 (EWSCS), Tallinn, Estonia, March 4-9. Participants: Antti Hyvärinen and Sven Laur

Fast Software Encryption (FSE 2007), Luxembourg, March 25-28. Member of programme committee and session chair: Kaisa Nyberg

April

Public Key Cryptography Conference (PKC 2007), Beijing, China, April 15-21. Participant: Sven Laur

Software and Services Variability Management Workshop, Espoo, Finland, April 19-20. Member of programme committee: Ilkka Niemelä

Ecrypt PhD Summer School, Samos, Greece, April 29 - May 5. Participants: Risto Hakala, Miia Hermelin

May

The 9th International Conference on Logic Programming and Nonmonotonic Reasoning (LPNMR 2007), Tempe, Arizona, USA, May 14-17. Poster: Emilia Oikarinen. Member of programme committee: Ilkka Niemelä, Tomi Janhunen. Session chair: Tomi Janhunen

Workshop on Correspondence and Equivalence for Nonmonotonic Theories (CENT 2007), Tempe, Arizona, USA, May 14. Member of programme committee: Emilia Oikarinen. Session chair: Tomi Janhunen

1st International Workshop on Software Engineering for Answer Set Programming (SEA 2007), Tempe, Arizona, USA, May 14. Participants: Tomi Janhunen, Emilia Oikarinen

PedaForum 2007, Tampere, Finland, May 24-25. Participant: Harri Haanpää

Google Europe Anita Borg Scholarship 2007 meeting, Zurich, Switzerland, May 31 - June 2. Google Europe Anita Borg Memorial Scholarship 2007 finalist: Emilia Oikarinen

Summer School on Algorithmic Data Analysis (SADA 2007), Helsinki, Finland, May 28 to June 1. Poster: Jori Dubrovin, Antti Hyvärinen, Matti Järvisalo, Emilia Oikarinen, André Schumacher

June

Wireless Mobile and Multimedia Networks Conference (WoWMoM 2007), Espoo, Finland, June 18-21. Participant: Jukka Valkonen

Workshop on Unfoldings and Partial Order Techniques (UFO'07), Siedlce, Poland, June 26. Member of programme committee: Keijo Heljanko

14th International Symposium on Temporal Representation and Reasoning (TIME 2007), Alicante, Spain, June 28-30. Member of programme committee: Keijo Heljanko

July

14th International SPIN Workshop on Model Checking Software (SPIN 2007), Berlin, Germany, July 1-3. Participant: Keijo Heljanko

Computer Aided Verification (CAV) Conference 2007, Berlin, Germany, July 3-7. Participants: Tommi Junttila and Keijo Heljanko

Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007), Cambridge, Great Britain, July 1-4. Participant: Jukka Valkonen

IEEE Information Theory Workshop (ITW 2007), Bergen, Norway, July 2-5. Member of programme committee, invited speaker: Kaisa Nyberg

4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007), Cambridge, United Kingdom, July 2-3. Member of programme committee: Kaisa Nyberg

International Conference on Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX 2007), Aix en Provence, France, July 3-6. Member of programme committee: Ilkka Niemelä

14th RCRA Workshop on Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion, Rome, Italy, July 4-7. Participant: Matti Järvisalo. Member of programme committee: Ilkka Niemelä

3rd Workshop on Cryptography for Ad-Hoc Networks (WCAN 2007), Wroclaw, Poland, July 8. Member of programme committee: Kaisa Nyberg. Participant: Maarit Hietalahti

GOCP Workshop, Wroclaw, Poland, July 7-10. Participant: Maarit Hietalahti

Summer School on Dependable Computer Systems, Lugano, Switzerland, July 8-14. Participant: Antti Hyvärinen

COSIC Course: State of the Art and Evolution of Computer Security and Industrial Cryptography, Leuven, Belgium, July 9-13. Participant: Jukka Valkonen

The 7th International Conference on Application of Concurrency in System Design (ACSD 2007), Bratislava, Slovak Republic, July 10-13. Member of programme committee: Keijo Heljanko

3rd International Workshop on Algorithmic Aspects of Sensor Networks (ALGOSENSORS 2007), Wroclaw, Poland, July 14. Member of programme committee: Pekka Orponen

Workshop on Statistical Mechanics of Distributed Information Systems, Mariehamn, Åland, July 16-18. Participant: Pekka Orponen and Petri Savola

22nd Conference on Artificial Intelligence (AAAI-07), Vancouver, British Columbia, Canada, July 22-26. Member of programme committee: Tomi Janhunen

August

SAC 2007 Conference, Ottawa, Canada, August 15-18. Participant: Billy Brumley

ACAI 2007 Summer School, Leuven, Belgium, August 19-29. Participants: Matti Järvisalo, Emilia Oikarinen. Poster: Matti Järvisalo, Emilia Oikarinen

JSS17 Summer School, Jyväskylä, Finland, August 20-24. Participant: Aleksi Hänninen

September

The 23rd International Conference on Logic Programming (ICLP07), Porto, Portugal, September 7-14. Participants: Ilkka Niemelä, Tomi Janhunen, Matti Järvisalo, Emilia Oikarinen. Chairman of programme committee: Ilkka Niemelä. Member of programme committee: Tomi Janhunen. Session chairs: Ilkka Niemelä, Tomi Janhunen. Poster: Emilia Oikarinen. Best student paper award awarded to Matti Järvisalo and Emilia Oikarinen.

LASER Summer School on Software Engineering Applied Software Verification, Elba, Italy, September 7-17. Participant: Jori Dubrovin

4th International Workshop on Answer Set Programming: Advances in Theory and Implementation (ASP'07), Porto, Portugal, September 8 and 13. Participants: Tomi Janhunen, Matti Järvisalo, Ilkka Niemelä, Emilia Oikarinen. Member of programme committee and session chair: Emilia Oikarinen

NEW2AN Conference, Saint Petersburg, Russia, September 10-14. Participant: Dmitrij Lagutin

International Workshop on Secure Spontaneous Interaction (IWWSI), Innsbruck, Austria, September 15-17. Participants: Kaisa Nyberg (also chairperson of programme committee) and Jukka Valkonen

The 13th International Conference on Principles and Practice of Constraint Programming, Providence, Rhode Island, USA, September 22-28. Participant: Matti Järvisalo

4th International Workshop on Local Search Techniques in Constraint Satisfaction, Providence, Rhode Island, USA, September 23. Participant: Matti Järvisalo

7th International Workshop on Symmetry and Constraint Satisfaction Problems, Providence, Rhode Island, USA, September 23. Participant: Matti Järvisalo

Nordugrid Conference 2007, Copenhagen, Denmark, September 24-28. Participant: Antti Hyvärinen

Dagstuhl Seminar on Deduction and Decision Procedures, Dagstuhl, Germany, September 30 - October 5. Participant: Ilkka Niemelä

October

International Conference on Applications of Declarative Programming and Knowledge Management, Würzburg, Germany, October 4-6. Member of programme committee: Ilkka Niemelä

Information Security Conference (ISC 2007), Valparaiso, Chile, October 9-12. Member of programme committee and session chair: Kaisa Nyberg

International Conference on Sensor Technologies and Applications, Valencia, Spain, October 14-20. Member of programme committee: Pekka Orponen

International RuleML Symposium on Rule Interchange and Applications, Orlando, Florida, USA, October 25-26. Member of programme com-

mittee: Ilkka Niemelä

November

NWERC Programming Contest, Utrecht, The Netherlands, November 16-18. Participant: Harri Haanpää (Team Leader). The TKK team (Markus Ojala, Veli Peltola and Ville Pettersson) placed 3rd among 52 teams and qualified for the World Finals of the ICPC.

December

The Third International Conference on Mobile and Ad-Hoc Sensor Networks (MSN 2007), Beijing, China, December 8-15. Participant: Harri Haanpää (Session chair)

Workshop Automata and Logic, History and Perspectives, WAL07, Aachen, Germany, December 13-16. Participants: Keijo Heljanko and Heikki Tauriainen

5.2 Visits

Ilkka Niemelä visited Griffith University in Brisbane, Australia on 9.-20.4.2007.

Keijo Heljanko visited University of Aarhus in Denmark on 17.-21.4.2007.

Keijo Heljanko visited TU Munchen on 23.-30.9.2007.

Tomi Janhunen visited Vienna University of Technology in Austria on 12-17.11.2007.

Matti Järvisalo and **Emilia Oikarinen** visited University of Potsdam in Germany on 18.-24.11.2007.

Kaisa Nyberg was opponent for Håkan Englund in Lunds Universitet in Sweden on 13.-15.12.2007.

5.3 Guests

In this section the various academic visits to the Laboratory for Theoretical Computer Science in 2007 are summarized. The host is given at the end of each entry.

Erik Aurell, Prof., Kungliga Tekniska Högskolan, Ruotsi, 1 days, reason of visit: Research. (Orponen)

Alexander K. Hartmann, Prof., Universität Oldenburg, Saksa, 2 months, reason of visit: Teaching and research. (Orponen)

Romualdo Pastor-Satorras, Prof., Universitat Politecnica de Catalunya, Espanja, 1 months, reason of visit: Teaching and research. (Orponen)

Satu Elisa Schaeffer, Prof. inv., Universidad Autonoma de Nuevo Leon, Meksiko, 3 weeks, reason of visit: Research. (Orponen)

Viktor Schuppan, Dr., ETH Zurich, Switzerland, 5 days, reason of visit: Research. (Heljanko)

Siert Wieringa, B.Sc., TU Delft, Netherlands, 3 days, reason of visit: Research. (Heljanko)

6 SCIENTIFIC EXPERT TASKS

This section summarizes the scientific expert tasks carried out by the personnel of Laboratory for Theoretical Computer Science in 2007. Tasks related to conferences are summarized in Section 5.1. Tasks internal to Helsinki University of Technology are not reported.

6.1 Positions of trust

Ilkka Niemelä, member of the executive committee of the Association for Logic Programming

Kaisa Nyberg, member of the board of Finnish Mathematical Society; member of evaluation board of VERDIKT research programme in Norges forsknigsråd, Norway; member of the Scientific Advisory Board for Defence (MATINE)

6.2 Memberships in editorial boards

Ilkka Niemelä, member of the editorial board of Theory and Practice of Logic Programming; member of the editorial board of Journal of Artificial Intelligence Research

Leo Ojala, member of the editorial board of Journal of Universal Computer Science

Pekka Orponen, member of the editorial board of Theoretical Computer Science C and of Neural Computing Surveys.

Kaisa Nyberg, member of the editorial board of International Journal of Security and Networks (IJSN).

6.3 Scientific expert duties

Keijo Heljanko, pre-examiner and official opponent of Henri Hansen at Tampere University of Technology, Tampere, Finland

Kaisa Nyberg, statement concerning filling a professor position in VTT, Finland; official opponent of Håkan Englund at Lunds Universitet, Sweden

7 PUBLICATIONS

7.1 Journal Articles

[1] Philippe Dumas, Helger Lipmaa, and Johan Wallén. Asymptotic behaviour of a non-commutative rational series with a nonnegative linear representation. *Discrete Mathematics and Theoretical Computer Science*, 9(1):247–274, 2007.

[2] Harri Haanpää and Patric Östergård. Sets in abelian groups with distinct sums of pairs. *Journal of Number Theory*, 123(1):144–153, 2007.

[3] Tomi Janhunen and Emilia Oikarinen. Automated verification of weak equivalence within the smodels system. *Theory and Practice of Logic Programming*, 7(6):697–744, 2007.

[4] Petteri Kaski and Patric Östergård. There exists no symmetric configuration with 33 points and line size 6. *Australasian Journal of Combinatorics*, 38:273–277, 2007.

[5] Kaisa Nyberg. Kryptologia - tiedon turvaamisen tiede. *Tietojenkäsittelytiede*, 26:32–53, 2007.

[6] Pekka Orponen. "P = NP" -ongelma ja laskennan vaativuusteoria. *Tietojenkäsittelytiede*, 26:54–67, 2007.

[7] Satu Elisa Schaeffer. Graph clustering. *Computer Science Review*, 1(1):27–64, 2007.

7.2 Conference Papers

[8] Billy Bob Brumley and Kimmo Järvinen. Koblitz curves and integer equivalents of Frobenius expansions. In *Selected Areas in Cryptography, 14th International Workshop—SAC '07*, volume 4876 of *Lecture Notes in Computer Science*, pages 126–137. Springer-Verlag, 2007.

[9] Billy Bob Brumley and Kaisa Nyberg. Differential properties of elliptic curves and blind signatures. In *Information Security, 10th International Conference—ISC '07*, volume 4779 of *Lecture Notes in Computer Science*, pages 376–389. Springer-Verlag, 2007.

[10] Ahto Buldas and Sven Laur. Knowledge-binding commitments with applications in time-stamping. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*, volume 4450 of *Lecture Notes in Computer Science*, pages 150–165. Springer, 2007.

[11] Harri Haanpää, André Schumacher, Thorn Thaler, and Pekka Orponen. Distributed computation of maximum lifetime spanning subgraphs in sensor networks. In Hongke Zhang, Stephan Olariu, Jiannong Cao, and David B. Johnson, editors, *Proceedings of The 3rd International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2007)*, volume 4864 of *Lecture Notes in Computer Science*, pages 445–456, Berlin / Heidelberg, 2007. Springer-Verlag.

[12] Maarit Hietalahti. A clustering-based group key agreement protocol for ad-hoc networks. In *3rd Workshop on Cryptography for Ad hoc Networks (WCAN 2007), July 8th, 2007, Wroclaw, Poland*, 2007.

[13] Jukka Honkola, Sari Leppänen, Pasi Rinne-Rahkola, Martti Söderlund, Markku Turunen, and Kimmo Varpaaniemi. A case study: Applying Lyra in modeling S60 camera functionality. In John Leaney, Jerzy W. Rozenblit, and Jianfeng (Eds.) Peng, editors, *Proceedings of the 14th*

Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems, ECBS 2007, Raising Expectations of Computer-Based Systems, pages 25–36, Los Alamitos, CA, USA, 2007. IEEE Computer Society Press.

[14] Tomi Janhunen. Intermediate languages of ASP systems and tools. In Marina De Vos and Torsten Schaub, editors, *Proceedings of the 1st International Workshop on Software Engineering for Answer Set Programming*, number CSBU-2007-05 in Deparment of Computer Science, University of Bath, Technical Report Series, pages 12–25, Tempe, Arizona, USA, May 2007.

[15] Tomi Janhunen, Emilia Oikarinen, Hans Tompits, and Stefan Woltran. Modularity aspects of disjunctive stable models. In Chitta Baral, Gerhard Brewka, and John Schlipf, editors, *Logic Programming and Nonmonotonic Reasoning 2007*, volume 4483 of *Lecture Notes in Artificial Intelligence*, pages 175–187. Springer-Verlag, 2007.

[16] Matti Järvisalo. Industrial-strength SAT solving and restricted branching. In Veli Mäkinen, Greger Lindén, and Hannu Toivonen, editors, *Summer School on Algorithmic Data Analysis (SADA 2007) and Annual Hecse Poster Session. Abstract proceedings*, Series of Publications B, Report B-2007-4, page 39. Helsinki University Printing House, 2007.

[17] Matti Järvisalo and Tommi Junttila. Limitations of restricted branching in clause learning. In Christian Bessiere, editor, *Proceedings of the 13th International Conference on Principles and Practice of Constraint Programming (CP 2007)*, volume 4741 of *Lecture Notes in Computer Science*, pages 348–363. Springer, 2007.

[18] Matti Järvisalo and Emilia Oikarinen. Extended ASP tableaux and rule redundancy in normal logic programs. In Verónica Dahl and Ilkka Niemelä, editors, *Proceedings of the 23rd International Conference on Logic Programming (ICLP 2007)*, volume 4670 of *Lecture Notes in Computer Science*, pages 134–148. Springer, 2007. Received ICLP 2007 Best Student Paper Award.

[19] Tommi Junttila and Petteri Kaski. Engineering an efficient canonical labeling tool for large and sparse graphs. In David Applegate, Gerth Stølting Brodat, Daniel Panario, and Robert Sedgewick, editors, *Proceedings of the Ninth Workshop on Algorithm Engineering and Experiments and the Fourth Workshop on Analytic Algorithms and Combinatorics*, 2007.

[20] Matti Järvisalo. The effect of structural branching on the efficiency of clause learning SAT solving. In *14th RCRA Workshop: Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion 2007*. AI*IA RCRA, 2007.

[21] Matti Järvisalo. Restricted branching in clause learning DPLL. In Brahim Hnich and Kostas Stergiou, editors, *Proceedings of the CP 2007 Doctoral Programme*, pages 55–60, 2007.

[22] Dmitrij Lagutin and Hannu H. Kari. Controlling incoming connections using certificates and distributed hash tables. In *Proceedins of The 7th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2007)*, volume 4712 of *Lecture Notes in Computer Science*, pages 455–467, St. Petersburg, Russia, Sep 2007. Springer-Verlag.

[23] Sven Laur and Helger Lipmaa. A new protocol for conditional disclosure of secrets and its applications. In Jonathan Katz and Moti Yung, editors, *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*, volume 4521 of *Lecture Notes in Computer Science*, pages 207–225. Springer, 2007.

[24] Kaisa Nyberg and Risto Hakala. A key-recovery attack on SOBER-128. In Eli Biham, Helena Handschuh, Stefan Lucks, and Vincent Rijmen, editors, *Symmetric Cryptography*. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.

[25] Kaisa Nyberg and Miia Hermelin. Multidimensional Walsh transform and a characterization of bent functions. In Tor Helleseth, P. Vijay Kumar, and Oyvind Ytrehus, editors, *Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks*, pages 83–86. IEEE, 2007.

[26] Kaisa Nyberg and Jukka Valkonen. Wireless group security using MAC layer multicast. In *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a*, pages 1–8, 2007.

[27] Emilia Oikarinen. Modular answer set programming. In Veli Mäkinen, Greger Lindén, and Hannu Toivonen, editors, *Summer School on Algorithmic Data Analysis (SADA 2007) and Annual Hecse Poster Session. Poster Abstracts*, Series of Publications B, Report B-2007-4, page 62. Helsinki University Printing House, May 2007.

[28] Emilia Oikarinen. Modular answer set programming. In Verónica Dahl and Ilkka Niemelä, editors, *Proceedings of the 23rd International Conference on Logic Programming (ICLP 2007)*, volume 4670 of *Lecture Notes in Computer Science*, pages 462–463, Porto, Portugal, September 2007. Springer. Doctoral Consortium research summary.

[29] Emilia Oikarinen. Modularity in smodels programs. In Chitta Baral, Gerhard Brewka, and John Schlipf, editors, *Logic Programming and Nonmonotonic Reasoning, 9th International Conference on Logic Programming and Nonmonotonic Reasoning LPNMR 2007, Tempe, AZ, USA, May 2007, Proceedings*, volume 4483 of *Lecture Notes in Artificial Intelligence*, pages 321–326, Tempe, Arizona, USA, May 2007. Springer-Verlag.

[30] Emilia Oikarinen and Tomi Janhunen. A linear transformation from prioritized circumscription to disjunctive logic programming. In Verónica Dahl and Ilkka Niemelä, editors, *Proceedings of the 23rd International Conference on Logic Programming (ICLP 2007)*, volume 4670 of *Lecture Notes in Computer Science*, pages 440–441, Porto, Portugal, September 2007. Springer.

[31] Emilia Oikarinen and Tomi Janhunen. A translation-based approach to the verification of modular equivalence. In Stefania Costantini and Richard Watson, editors, *Proceedings of the 4th Workshop on Answer Set Programming; Advances in Theory and Implementation*, pages 255–269, 2007.

[32] Jani Suomalainen, Jukka Valkonen, and N. Asokan. Security associations in personal networks: A comparative analysis. In *Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks July 2-3 2007, Cambridge, UK*, pages 43–57, 2007.

[33] Jukka Valkonen, Aleksi Toivonen, and Kristiina Karvonen. Usability testing for secure device pairing in home networks. In Anne Bajart, Henrik Muller, and Thomas Strang, editors, *UbiComp 2007 Workshop Proceedings, September 2007, Innsbruck, Austria*, 2007.

7.3 Books

[34] Verónica Dahl and Ilkka Niemelä. *Logic Programming, 23rd International Conference, ICLP 2007, Porto, Portugal, September 8-13, 2007, Proceedings*. Springer, Berlin, 2007.

7.4 Reports

[35] Mikko Alava, John Ardelius, Erik Aurell, Petteri Kaski, Supriya Krishnamurthy, Pekka Orponen, and Sakari Seitz. Circumspect descent prevails in solving random constraint satisfaction problems. Technical Report 0711.4902, arXiv.org, 2007. `http://arxiv.org/abs/0711.4902`.

[36] Jori Dubrovin and Tommi Junttila. Symbolic model checking of hierarchical UML state machines. Technical Report B23, Helsinki University of Technology Laboratory for Theoretical Computer Science, Espoo, 2007.

[37] Jori Dubrovin, Tommi Junttila, and Keijo Heljanko. Symbolic step encodings for object based communicating state machines. Technical Report B24, Helsinki University of Technology Laboratory for Theoretical Computer Science, Espoo, 2007.

[38] Maarit Hietalahti, Mikko Särelä, Antti Tuominen, and Pekka Orponen. Security topics and mobility management in hierarchical ad hoc networks (Samoyed): Final report. Technical Report B22, Helsinki University of Technology Laboratory for Theoretical Computer Science, Espoo, 2007.

[39] Matti Järvisalo. Impact of restricted branching on clause learning SAT solving. Research Report A107, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, 2007.

[40] Vesa Ojala. A slicer for UML state machines. Technical Report B25, Helsinki University of Technology Laboratory for Theoretical Computer Science, Espoo, 2007.

7.5 Doctoral Dissertations

[41] Henrik Petander. A network mobility management architecture for a heterogeneous network environment. Research Report A108, Helsinki University of Technology Laboratory for Theoretical Computer Science, Espoo, 2007. Doctoral dissertation.

7.6 Licentiate's Theses

[42] Maarit Hietalahti. *Requirements for a security architecture for clustered ad-hoc networks.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2007.

[43] Matti Järvisalo. *Impact of Restricted Branching on Clause Learning SAT Solving.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2007.

7.7 Master's Theses

[44] Risto Hakala. Linear cryptanalysis of two stream ciphers. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2007.

[45] Sami Kauppinen. Trust evaluation in component-based software architecture. Master's thesis, Helsinki University of Technology, Department of Computer Scienceand Engineering, Laboratory for Theoretical Computer Science, 2007.

[46] Samuli Larvala. Differential compression for efficient software updating. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2007.

[47] Antti J. Tuominen. Managing global connectivity with IPv6 in heterogeneous mobility scenarios. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2007.

7.8 Patents

[48] Andrei Kustov, Olli Auvinen, Mikko Hamalainen, Hannu Kari, Victor Khachtchanski, Juha Koponen, Hannu Mallat, and Juhana Rasanen.

Methods and arrangements for providing efficient information transfer over a limited speed communications link. First Hop Oy, 2007.

7.9 Software

[49] Jori Dubrovin. SMUML/Suboco 1.10 - an SMT-based UML bounded model checker, 2007.

[50] Jori Dubrovin. SMUML/Uboco 1.10 - a translator from UML models to NuSMV programs, 2007.

[51] Tomi Janhunen. asptools 1.0 - a tool collection for answer set programming, 2007. `http://www.tcs.hut.fi/Software/asptools/`.

[52] Tomi Janhunen. lpeq 1.19 - a tool for testing the modular equivalence of logic programs, 2007. `http://www.tcs.hut.fi/Software/lpeq/`.

[53] Tommi Junttila. PySMT version 0.50 - a Python front-end for satisfiability modulo theories solvers, 2007.

[54] Tommi Junttila. SMUML/proco version 2.00 - a translator from UML models to Promela, 2007.

[55] Janne Lundberg. A proof of concept PLA implementation, 2007. `http://www.tcs.hut.fi/Software/PLA/new/Download.shtml`.

[56] Emilia Oikarinen. circ2dlp 2.1 - a linear translation from prioritized circumscription to disjunctive logic programming, 2007.

[57] Vesa Ojala. SMUML/canal 1.0.0 - a counterexample analysator for analyzing abstract counterexamples from data abstracted UML models, 2007.

[58] Vesa Ojala. SMUML/slicer 1.0.0 - a slicer for slicing UML state machines, 2007.

[59] Heikki Tauriainen. SMUML/abstractor 1.0.0 - data abstraction and abstract type generation tools for abstracting UML state machines, 2007.

[60] Heikki Tauriainen and Vesa Ojala. SMUML/analyze 1.0.0 - front-end to the SMUML tool-set wtih an abstract-check-refine cycle for UML state machines, 2007.

[61] Heikki Tauriainen and Juhani Peltonen. SMUML/abstractor-gui 1.0.0 - a graphical user interface for abstracting UML state machines and editing abstract type libraries, 2007.

7.10 Miscellaneous publications

[62] Harri Haanpää. Annual report for the year 2006. Annual report, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, 2007.

[63] Matti Järvisalo. Equivalence checking hardware multiplier designs (SAT competition 2007 benchmark description), 2007. `http://www.satcompetition.org/2007/contestants.html`.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2007