Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2006
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2006
Espoo 2007 HUT-TCS-Y2006

ANNUAL REPORT FOR THE YEAR 2006

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 2006
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2006
Espoo 2007 HUT-TCS-Y2006

ANNUAL REPORT FOR THE YEAR 2006

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 2007

Abstract: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2006.

Keywords: personnel, teaching, research, activities, publications

CONTENTS

1 INTRODUCTION

After a record year in 2005 with five doctoral thesis completed the academic performance of the Laboratory for Theoretical Computer Science remained on a very high level also in 2006. Four doctoral theses were finished (Misa Keinänen, Janne Lundberg, Satu Elisa Schaeffer, Heikki Tauriainen) in addition to a licentiate's thesis and seven master's theses. The laboratory's publication record stayed also strong: 30 papers in international conferences with printed proceedings (27 in 2005) and 10 articles in peer-reviewed journals in 2006 (12 in 2005).

The personnel volume at the laboratory has been relatively stable over the past couple of years, consisting of six permanent academic staff (four professors and two teaching researchers), technical personnel (secretaries and systems support), plus about thirty researchers supported by external competitive funding, mainly grants from the Academy of Finland and the Finnish Funding Agency for Technology and Innovation (TEKES), and graduate student positions at the Helsinki Graduate School in Computer Science and Engineering (HeCSE).

Out of the almost 1.8 M€ total budget of the laboratory in 2006, less than 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, maintaining such a funding structure is arduous: presently available research grants are typically small, short-term and volatile, and high dependence on them takes up a considerable amount of time and effort that could more profitably be used in actual research work.

More detailed information on the personnel, education, research, visits, and publications in the laboratory in 2006 can be found in the following sections.

2 PERSONNEL

The personnel of the Laboratory for Theoretical Computer Science in 2006 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

Janhunen, Tomi; D.Sc. (Tech.), Professor (pro tem) until July; Teaching researcher from August

Kari, Hannu H.; D.Sc. (Tech.), Professor

Niemelä, Ilkka; D.Sc. (Tech.), Senior Academy Researcher until July; Professor and Head of the Laboratory from August

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

Ojala, Leo; Lic.Sc. (Tech.), Professor Emeritus

Orponen, Pekka; D.Phil., Professor; Head of the Laboratory until July

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

Lilius, Johan; D.Sc. (Tech.), Docent in Reactive Systems, Professor in Computer Science and Engineering, Åbo Akademi University

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

Kangasniemi, Ulla; Secretary, part-time

Kauppila, Minna; Secretary, from March

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

Lassila, Eero; Lic.Sc. (Tech.) Laboratory manager

Nikander, Marianne; Secretary until January

2.4 Researchers

Candolin, Catharina; D.Sc. (Tech.), until June

Ekberg, Jan-Erik; M.Sc. (Tech.), from 14 August until 15 October

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

Hermelin, Miia; Lic.Sc. (Tech.), from 16 August

Hietalahti, Maarit; M.Sc. (Tech.), on leave until 15 June

Hyvärinen, Antti; M.Sc. (Tech.)

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

Jussila, Toni; D.Sc. (Tech.) until 14 February

Järvisalo, Matti; M.Sc. (Tech.)

Keinänen, Misa; D.Sc. (Tech.) until 28 May

Kortesniemi, Yki; Lic.Sc. (Tech.) until July

Kullberg, Tuulia; M.Sc. (Tech.), on leave

Lagutin, Dmitrij; M.Sc. (Tech.) part-time, full-time from June to August

Laine, Jaakko; M.Sc., part time, until June

Laur, Sven; M.Sc.

Lundberg, Janne; D.Sc. (Tech.)

Marinoni, Stefano; M.Sc., part-time from February

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

Schaeffer, Satu Elisa; D.Sc. (Tech.), until July
Schumacher, André; Dipl.-Inf.
Syrjänen, Tommi; Lic.Sc. (Tech.)
Särelä, Mikko; M.Sc. (Tech.)
Tauriainen, Heikki; D.Sc. (Tech.)
Valkonen, Jukka; M.Sc. (Tech.), on leave from October to December
Varpaaniemi, Kimmo; D.Sc. (Tech.), until June
Wallén, Johan; Lic.Sc. (Tech.)

2.5 Research Assistants

Brumley, Billy; M.Sc. (Tech.),
Dubrovin, Jori; M.Sc. (Tech.),
Hakala, Risto-Matti; Stud. (Tech.), from June, part-time from September
Hakulinen, Lasse; Stud. (Tech.), from June until August
Hänninen, Aleksi; Stud. (Tech.), from June, part-time from September
Kaitala, Annukka; until January
Liedes, Sami; Stud. (Tech.), from June, part-time from September
Nuorvala, Ville; Stud. (Tech.) part-time from October
Ojala, Vesa; Stud. (Tech.) from June, part-time from September
Prasad, Shreyas; from 23 June until 15 August
Rusanen, Antti; Stud. (Tech.) from August
Savola, Petri; Stud. (Tech.), from June until August
Toivonen, Aleksi; Stud. (Tech.), from 16 October
Tuominen, Antti; Stud. (Tech.)

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.

Herttua, Ilkka; Stud. (Tech.) T–79.5303
Huima, Antti; M.Sc. (Tech.) T–79.5304
Launiainen, Tuomas; Stud. (Tech.) T–79.1001 / T–79.1002
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 2006

In 2006, 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 2006

T–79.1001 Introduction to theoretical computer science T (4 cr)
Pekka Orponen (Tommi Syrjänen; Antti Hyvärinen, Matti Järvisalo, Vesa Ojala)

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

T–79.1002 Introduction to theoretical computer science Y (2 cr)
Pekka Orponen (Tommi Syrjänen; Antti Hyvärinen, Matti Järvisalo, Vesa Ojala)

Finite automata and regular languages. Context-free grammars and pushdown automata.

T–79.3001 Logic in computer science: foundations (4 cr)
Tomi Janhunen (Antti Hyvärinen, Emilia Oikarinen)

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)
Hannu H. Kari

Current research topics in theoretical computer science. In year 2006, focus was on ad hoc network performance analysis.

T–79.4201 Search problems and algorithms (4 cr)
Ilkka Niemelä, Pekka Orponen (Antti Rusanen)

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–79.4301 Parallel and Distributed Systems (4 cr)
Keijo Heljanko (Heikki Tauriainen)

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

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

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. Password based authentication. Kerberos, IKE, UMTS AKA. Other examples of cryptographic protocols.

T–79.5101 Logic in Computer Science: Special Topics I (4 cr)
Tomi Janhunen (Matti Järvisalo)

Basics of modal logic. Current applications in computer science.

T–79.5202 Combinatorial Algorithms (4 cr)
Harri Haanpää

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–79.5301 Reactive systems (4 cr)
Misa Keinänen

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

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

Special problems of mobility management in wireless networks.

T–79.7001 Postgraduate course in theoretical computer science (2–10 cr)
Pekka Orponen

Current research problems in theoretical computer science. In spring, the topic was spectral graph theory. (see also autumn 2006)

3.3 Autumn 2006

T–79.1001 Introduction to theoretical computer science T (4 cr)
Harri Haanpää (Tommi Syrjänen; 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; 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 (Antti Rusanen)

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, Jukka Valkonen)

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 (Vesa Ojala)

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. The course in Autumn 2006 will be concerned with enumerative combinatorics, i.e. the counting of combinatorial objects by means of their complex-valued generating functions.

T–79.5304 Formal conformance testing (4 cr)
Antti Huima

Introduction to conformance testing. Formal conformance testing and its automatization. On testing timed and infinite-state systems. Estimation of testing coverage.

T–79.5305 Formal methods (4 cr)
Tommi Junttila (Keijo Heljanko, Ilkka Niemelä, Heikki Tauriainen)

Software model checking. Data and predicate abstraction.

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

Special problems of mobility management in wireless networks.

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

Cryptographic security models and provable security.

T–79.7001 Postgraduate course in theoretical computer science (2–10 cr)
Kaisa Nyberg, N. Asokan

In Autumn 2006 the course is arranged in cooperation with the course T–110.7290 Research seminar on network security, with Prof Asokan. The topic is Authenticated Key Establishment. (see also spring 2006)

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.

3.4 Pedagogical education

In 2005–2006, Keijo Heljanko completed a 15 study week Program on Higher Education Pedagogy (YOOP), arranged by the Teaching and Learning Development unit and intended for the teaching staff of Helsinki University of Technology.

4 RESEARCH ACTIVITIES

The research activities of Laboratory for Theoretical Computer Science in 2006 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).

4.1 Computational Logic

Extensions of Rule-Based Constraint Programming
Ilkka Niemelä and Tommi Syrjänen

The development of declarative semantics, such as the stable model semantics, for logic programming type rules has led to an interesting new paradigm for solving computationally challenging problems. In the novel answer set programming (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 [41, 42]. The

Project name Head Duration Funding source Researchers
Advanced Constraint Programming Techniques for Large Structured Problems (ACPT) Niemelä 1.1.2005–31.12.2007 Academy of Finland Antti Hyvärinen, Matti Järvisalo, Misa Keinänen, 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
Algorithms for Nonuniform Networks (ANNE) Orponen 1.1.2004–31.12.2006 Academy of Finland Satu Elisa Schaeffer
Algorithms and Combinatorics for Sensor Networks (ACSENT) Orponen 1.8.2004–31.12.2006 Academy of Finland Antti Rusanen, André Schumacher
Security and Mobility in Hierarchical Ad Hoc Networks (SAMOYED) Orponen 1.9.2003–31.12.2006 TEKES Maarit Hietalahti, Mikko Särelä, Antti Tuominen
Symbolic Methods for UML Behavioural Diagrams (SMUML) Niemelä 1.1.2006–31.12.2007 TEKES Jori Dubrovin, Tommi Junttila, Toni Jussila, Kari Kähkönen, Sami Liedes, Vesa Ojala, Heikki Tauriainen
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, Stefano Marinoni, Johan Wallén
Interconnected Broadband Home Networks (INHONETS) Nyberg 1.1.2006–31.12.2007 TEKES Billy Brumley, Jan-Erik Ekberg, Aleksi Toivonen, Jukka Valkonen
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 Maarit Hietalahti, Aleksi Hänninen

Table 1: Ongoing projects in 2006

project has developed an efficient ASP system called SMODELS[1] which is used in dozens of research groups world wide.

The current ASP systems are research tools and they lack most of the standard programming tools that are present in more established languages. The declarative nature of ASP makes it difficult to apply the standard methodology directly so we have studied how the existing concepts can be translated into ASP. We have developed a prototype ASP debugger that is based on meta-programming: the core of the debugger is an ASP program that gets as an input the program that is debugged [52].

We have investigated the proof theory of programs with monotone cardinality atoms (mca-programs) and demonstrated that the operational concept of the one-step provability operator used in normal logic programs can be extended to mca-programs but this extension involves nondeterminism. The resulting proof theory is shown to generalize the corresponding concepts in normal logic programs and in disjunctive logic programs with the possible-model semantics of Sakama and Inoue.

Translation-Based Techniques for Knowledge Representation
Tomi Janhunen

The research in this area concentrates on various formalisms for knowledge representation and transformations between them. As part of this research, we have been developing translations from normal logic programs to sets of classical clauses. Here the objective is to utilize efficient Boolean satisfiability (SAT) solvers when computing answer sets for normal logic programs. Our translation technique is based on a characterization of answer sets in terms of *level numberings*. The advantages of this approach are (i) a bijective relationship between answer sets and satisfying assignments, (ii) a fixed translation for each program, and (iii) low (sub-quadratic) time complexity. In 2006, we published the journal version of the translation [5] which includes an evaluation of an implementation of the translation that consists of two translators named as LP2ATOMIC and LP2SAT.[2] New versions of these translations were simultaneously published [79] and submitted to first answer set solver contest to be organised in conjunction with the 9th International Conference on Logic Programming and Nonmonotonic Reasoning (LPNMR'07).

Disjunctive Logic Programming
Tomi Janhunen and Ilkka Niemelä

Since 2000, we have been developing a inference engine GNT[3] for the computation of answer sets for disjunctive logic programs. The system is based on two cooperating SMODELS engines: the first generates model candidates for the disjunctive logic program given as input whereas the second is responsible for checking the minimality of the candidates. In 2006, the journal version of the technical paper describing the GNT system was published [6]. Moreover, the system was also submitted to the first answer set

[1] `http://www.tcs.hut.fi/Software/smodels/`
[2] `http://www.tcs.hut.fi/Software/lp2sat/`
[3] `http://www.tcs.hut.fi/Software/gnt/`

solver competition mentioned above.

Modularity in Answer Set Programming
Tomi Janhunen and Emilia Oikarinen

Answer set programming (ASP) is a constraint programming paradigm that combines the rule-based syntax of logic programs with a declarative semantics based on *answer sets*. The overall goal of our modularity research is to bring good software engineering practise to the realm of ASP and, in particular, to exploit modules in order to ease program development in ASP. In 2006, we introduced a Gaifman-Shapiro-style module architecture for normal logic programs [45, 46]. In this architecture, modules interact through a well-defined input/output interface. The main result is a *module theorem* which gives the interconnection between the answer sets of individual modules and the answer sets of entire programs obtained as suitable combinations of modules. This result is a proper strengthening of Lifschitz and Turner's *splitting set theorem* in the case of normal programs. Moreover, the respective notion of equivalence between modules, viz. *modular equivalence*, proves to be a congruence for program composition. This research is part of Emilia Oikarinen's Licentiate's thesis project [59, 64].

SAT-based Planning
Keijo Heljanko and Ilkka Niemelä

Together with Jussi Rintanen (NICTA Limited, Canberra, Australia) we have studied a number of semantics for plans with parallel operator application. The standard semantics used most often in earlier work requires that parallel operators are independent and can therefore be executed in any order. We have considered a more relaxed definition of parallel plans, first proposed by Dimopoulos et al., as well as normal forms for parallel plans that require every operator to be executed as early as possible. We have formalized the semantics of parallel plans emerging in this setting, and proposed effective translations of these semantics into the propositional logic. And finally we have shown that one of the semantics yields an approach to classical planning that is sometimes much more efficient than the existing SAT-based planners. In 2006 these results were published in a journal paper [9].

Boolean Satisfiability Checking
Tommi Junttila, Matti Järvisalo, 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). We have previously studied the proof complexity theoretic effect of restricting branching in the DPLL method. Today, most solvers incorporate clause learning, which has proven to increase the efficiency of DPLL. Continuing this line of research on branching restrictions, in 2006 we have experimented on clause learning DPLL with various branching restrictions based on structural aspects of non–clausal (Boolean circuit) encodings of real–world problems.

In collaboration with Harri Haanpää (TCS Computational Complexity and Combinatorics Group) and Petteri Kaski (Helsinki Institute for Informa-

tion Technology HIIT) M.J. and I.N. have studied the problem of generating hard satisfiable SAT instances for clausal SAT solvers. In particular, we have introduced the Regular XORSAT model based on transforming a random regular graph into a system of linear equations followed by clausification. Additionally, we have developed schemes for introducing nonlinearity to the model, making the instances suitable for benchmarking clausal solvers with equivalence reasoning techniques. Compared with other well-known families of satisfiable instances, our model generates instances that are among the hardest. Articles published in 2006 related to this research are [4,20]. Additionally, a software generator for the Regular *d*-XORSAT model was published [80].

Satisfiability Modulo Theories Checking
Tommi Junttila

In cooperation with the ITC-IRST research institute (Trento, Italy), during the previous years we have done research on extending satisfiability checking beyond the propositional case in the so-called satisfiability modulo theories (SMT) framework. Results concerning (i) solving techniques for the satisfiability problem of propositional logic with linear arithmetic and equality logic constraints, and (ii) how to combine decision procedures for multiple theories in the SMT framework, have been achieved and implemented in the MathSAT system (`http://mathsat.itc.it/`). In 2006, a journal article [2] describing some of the results has been published.

Techniques for Solving Boolean Equation Systems
Misa Keinänen and Ilkka Niemelä

Boolean equation systems provide a useful framework to study verification problems of finite state concurrent systems. For instance, many model checking problems and behavioral equivalences can be encoded as Boolean equation systems. We have studied techniques for solving Boolean equation systems and their applications in formal verification. We have developed algorithms for various classes of Boolean equation systems. In addition, we have applied answer set programming techniques to solve general systems of Boolean equations. In 2006 the results of this research were published in the Doctoral dissertation of Misa Keinänen [60].

Distributed and Grid-Based Techniques for Constraint-Based Search
Antti Hyvärinen, Tomi Janhunen, Tommi Junttila, and Ilkka Niemelä

The overall goal of this research is to distribute the search tasks involved in constraint programming on multiple machines in order to boost the search. We have ongoing activities in the areas of distributed answer set programming (ASP) and grid-based satisfiability checking in this respect.

We have continued our cooperation with Prof Schaub's group at the University of Potsdam in the development of a platform for distributed answer set solving called PLATYPUS[4]. The current system supports a variety of software and hardware architectures and provides basic coordination mechanisms for

[4] `http://www.cs.uni-potsdam.de/platypus/`

the distributed computation of answer sets. In 2006, we completed an extended experimental evaluation of the new PLATYPUS version [15, 16] that supports multi-threading and a special search technique called *probing*. A special Platypus Workshop was organized at the University of Potsdam in December 2006 in order to exchange ideas among developers and to design future extensions to PLATYPUS.

The emerging large-scale computational grid infrastructure is providing an interesting platform for massive distributed computations. We have studied the problem of exploiting such computational grids for solving challenging propositional satisfiability problem (SAT) instances [56], and the results have further been compared against a direct method of distributed solving in [18, 19]. When designing a distributed algorithm for a large loosely coupled computational grid, a number of grid specific problems need to be tackled including the heterogeneity of the resources, inherent communication delays, and high failure probabilities of grid jobs. The computing infrastructure has been greatly enhanced with respect to response time, reliability and size, in cooperation with the Nordugrid and globus communities and the Finnish CSC.

Bounded Model Checking

Keijo Heljanko, Tommi Junttila, Toni Jussila, Misa Keinänen, and Ilkka Niemelä

Bounded model checking (BMC) is a memory efficient method for locating design errors in reactive systems. The basic idea is to look for counterexample executions to a property required from the system of a bounded length by mapping the problem to, e.g., a propositional satisfiability problem and then using propositional satisfiability solvers to solve the problem at hand. The progress on bounded model checking techniques has been quite significant during the reporting period. The focus has been on ways to more efficiently encode more expressive temporal logics and on how to exploit the concurrency in bounded model checking of asynchronous systems.

The journal paper [1] sums up and extends the groups encoding methods for bounded model checking of linear temporal logic (LTL) and its extension to past time temporal modalities (PLTL). An advanced full day tutorial on bounded model checking was given on the 26th of June by Keijo Heljanko and Tommi Junttila in the joint conference on Applications of Concurrency to System Design (ACSD 2006) / Application and Theory of Petri Nets and Other Models of Concurrency (ATPN 2006). In addition, Ilkka Niemelä gave an invited talk on bounded model checking in the Bounded Model Checking workshop (BMC'06) affiliated with the Federated Logic Conference (FLOC'06) [43].

The bounded model checking approach discussed above has been extended further from LTL expressible properties to all ω-regular properties in [17]. The approach of this paper has been implemented in a new bounded model checking tool built on top of the open source NuSMV model checker [83].

Automata-Theoretic Methods for Linear Time Temporal Logic Model Checking

Heikki Tauriainen

This research has explored techniques for improving automata-based model checking of propositional linear time temporal logic (LTL) by making use of alternating and nondeterministic generalized Büchi automata with transition-based acceptance and on-the-fly explicit state exploration techniques. In the year 2006, the results of this research were published in the journal article [10] as well as in Heikki Tauriainen's Doctoral dissertation [63].

Symbolic Methods for UML Behavioural Diagrams

Ilkka Niemelä, Tommi Junttila, Toni Jussila, Heikki Tauriainen, Jori Dubrovin, Vesa Ojala, 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 (behavioural) aspects of a software system in its various development phases is gaining more importance. The sooner the incorrect behaviours 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 behavioural diagrams, e.g. state machine and message sequence diagrams. Important properties to be analysed include e.g. that systems do not deadlock, violate assertions, or perform unwanted implicit consumption of messages. We have developed a Java-like action description language for UML state machines [67] and done research on (i) translating UML models to the input language of the Spin model checker [22], (ii) defining a translation from UML models to the input language of the symbolic model checker NuSMV, and (iii) applying slicing and data abstraction techniques to UML state machines in order to make them more amenable to analysis.

The STRATUM System

Janne Nykopp, Tomi Janhunen, and Pekka Orponen

Since year 2000, our laboratory has been developing a web-based learning environment which is exploited in teaching to automate home assignments organized on basic courses in (theoretical) computer science. In the environment, (i) personalized home assignments are automatically created for (hundreds of) students, (ii) home assignments are put available for download in the web, (iii) students are provided automated tools for doing their assignments, (iv) the tools deliver the answers of students for approval using electronic mail, and (v) the answers of the students are checked either immediately or at specific points of time using assignment-specific automatic verifiers. In 2006, we completed the reconstruction of the common infrastructure, i.e., the STRATUM system. The revision of the system formed the technical part of Janne Nykopp's Master's thesis project [69]. The new STRATUM version was then taken into production use at our web server.

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, Satu Elisa Schaeffer, Sakari Seitz, and Pekka Orponen

The group studies methods for the solution of computational problems in structurally complex state spaces, focusing on techniques that are algorithmically relatively simple, but which adapt effectively to the characteristics of the problem instance at hand.

In April, Satu Elisa Schaeffer defended her doctoral thesis [62] on algorithmic issues in the modelling, analysis and management of large nonuniform networks. Topics discussed in the thesis cover efficient online clustering and sampling of large graphs with applications to routing and topology control in telecommunication networks, efficient storage for large graphs for improving neighbourhood and path queries, approximate pattern search in graphs, and computational complexity of clustering measures. In 2006, two articles based on the dissertation material were published. Article [51] presents a number of results on the complexity of optimising measures of graph clustering quality. Article [49] discusses a simple protocol for self-organising distributed cluster formation in ad hoc networks. This method, which is based on the general graph clustering principles introduced in the thesis, was first validated using ns-2 network simulations in [49], and later developed into an actual Linux prototype implementation by Mr. Antti Tuominen.

Satu Elisa Schaeffer's work was supported by the project *Algorithms for Nonuniform Networks (ANNE)* from the Academy of Finland. After her graduation, she took up in August a tenure-track position as a Teaching Researcher at the Universidad Autónoma de Nuevo León, Mexico.

In the area of theory and applications of stochastic search methods, Sakari Seitz and Pekka Orponen continued to investigate the structure of combinatorial optimisation landscapes and the surprising effectiveness of focused local search algorithms on such landscapes. This research was pursued in collaboration with the group of Doc. Mikko Alava from the TKK Laboratory of Physics and Dr. Petteri Kaski, who graduated from the TCS laboratory in 2005 and moved in January 2006 to a postdoctoral position at the Helsinki Institute for Information Technology. In June thru August, the group was joined by Mr. Petri Savola, who developed combinatorial methods for the uniform sampling of local minima in specific types of spin glass landscapes.

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 2006, Harri Haanpää worked 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.

The book Classification Algorithms for Codes and Designs [54] by Petteri Kaski and Patric Östergård was published by Springer in early 2006. Group members have contributed to the journal articles [3, 4, 7] and to [87].

Distributed Algorithmics

Harri Haanpää, Maarit Hietalahti, Annukka Kaitala, Shreyas Prasad, Antti Rusanen, André Schumacher, Mikko Särelä, Antti Tuominen, and Pekka Orponen

The group applies combinatorial and complexity-theoretic methods to the solution of algorithmic problems in distributed systems. Work in this area in 2006 was supported by the project *Algorithms and Combinatorics for Sensor Networks (ACSENT)* from the Academy of Finland and a related industrial project *Security and Mobility in Hierarchical Ad Hoc Networks (SAMOYED)* from the National Technology Agency TEKES.

Within the ACSENT collaboration, work in 2006 concentrated on the application of distributed approximation algorithms to typical optimisation problems arising in ad hoc networks. In particular, balancing of packet routing using a linear programming approximation algorithm by Young (1995) was considered. This work was pursued collaboratively by Harri Haanpää, André Schumacher, Satu Elisa Schaeffer and Pekka Orponen, and the group was also joined in July and August by Mr. Shreyas Prasad from the University of California at Santa Barbara (now at the University of Illinois at Urbana-Champaign).

The designed distributed algorithm was implemented on the widely used ns-2 network simulator, as an extension to its DSR routing protocol [50]. The resulting Balanced Multipath Source routing (BMSR) protocol was then evaluated by means of ns-2 runs. The first simulations presented in [50] showed a gain in network throughput of 14% to 69% compared to the basic DSR protocol. Further evaluations of the BMSR protocol, submitted for publication, considered the effect of different network topologies and multiple source-destination traffic flows on its performance.

Within the SAMOYED project, researcher Mikko Särelä completed an extended (December 2005 – July 2006) visit to the University of California at San Diego, where he was working on security and mobility issues in wireless emergency response systems. His publications from this period include [37, 48]. Researcher Maarit Hietalahti was on maternity leave until June. During this time she was substituted by Antti Tuominen, who developed a Linux-based prototype implementation of the network clustering method mentioned earlier, and also a compatible cluster-based routing protocol. After her return, Maarit Hietalahti continued to work on her Lic.Sc. thesis on security and trust relations in mobile networks. This work will be completed in 2007.

In addition to these project-specific activities, Ms. Annukka Kaitala from the Royal Institute of Technology KTH was visiting the group until January,

working on her M.Sc. thesis on energy-aware dynamic source routing,[5] and starting in August, Mr. Antti Rusanen joined the group to prepare his M.Sc. thesis on wireless network localisation via 3-fold visibility coverings of polygons.

4.3 Mobility management

Catharina Candolin, Hannu H. Kari, Yki Kortesniemi, Tuulia Kullberg, Dmitrij Lagutin, Jaakko Laine, Janne Lundberg, Stefano Marinoni, Ville Nuorvala and Antti Tuominen

In 2006, the research on mobility management, led by Prof. Hannu H. Kari, resulted in the publications [8,23–36,40,47,61,65,68,70,72–77,84,85].

4.4 Cryptography

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

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

This group develops and implements cryptanalytic methods for different symmetric cryptographic primitives. In 2006 the main focus was on cryptanalysis of stream ciphers.

Kaisa Nyberg and Johan Wallén attended the FSE 2006 workshop in Austria and Johan Wallén presented the paper containing the results obtained by the group previously [44]. Distinguishing attacks using linear cryptanalysis (linear masking) were previously applied to SNOW 2.0 by Watanabe, et al. The main contribution of the crypto group was that the estimates of the efficiency of the linear maskings were significantly improved using previous results by Johan Wallén on linear approximation of addition modulo 2^n and correlation theorems by Kaisa Nyberg. The extensive heuristic mask searches were designed by Kaisa Nyberg and implemented by Jukka Valkonen.

In 2006 the work continued. Risto Hakala and Kaisa Nyberg investigated a linear attack on SOBER-128. Now the goal was not only a distinguishing attack, but also key recovery attack. SOBER-128 contains a key dependent constant in the filter function. 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. The results of this work were presented by Kaisa Nyberg at the Dagstuhl workshop in January 2007.

In August, Miia Hermelin started her Ph.D project on using multiple linear approximations in linear cryptanalysis under supervision of Kaisa Nyberg. The work of Risto Hakala and Miia Hermelin was funded by the Scientific Advisory Board for Defence.

August 30 to September 8, Dr. Alexander Maximov, University of Luxembourg, visited the group and helped Risto Hakala to develop and install tools

[5] A. Kaitala: An Energy Aware Dynamic Source Routing Protocol. Examensarbete, Magisterutbildning Datornätverk, KTH Syd, 2007 (40 pp).

for linear cryptanalysis.

A second important class of cryptanalytic methods on stream ciphers is algebraic cryptanalysis, which aims at establishing systems of equations or logical constraints on the algebraic or Boolean variables involved in the input, output and the key of the cipher. Aleksi Hänninen started looking at the Trivium stream cipher and investigated the applicability of constrained logic programming tools, such as SAT solvers, on the cipher.

Concrete cryptographic security and secure data mining

Sven Laur and Kaisa Nyberg

The main aim of the CRYDAMI project 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.

The main emphasis of CRYDAMI project has been on developing methodology and tools to construct cryptographically secure data mining algorithms. This research has taken place with Dr. Taneli Mielikäinen from Helsinki Institute for Information Technology (HIIT). In 2006, secure implementations of complex classification algorithms have been devised [38].

We have also worked on issues how to provide authentic communication [39] when there is no public key infrastructure available. In many cases, data is gathered from users via internet and no public keys are sent ahead. Therefore, such low-weight authentication protocols can significantly diminish the success of domain-spoofing and other similar attacks.

Another similar but important supporting infrastructure 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 [14].

Sven Laur is also cooperating with University of Tartu in order to design a fast prototyping tool for secure multi-party computations. The main aim of this project is to develop fast but secure algorithms for basic computational operations. This should significantly increase the prototyping speed and allow to construct privacy-preserving algorithms without specific cryptographic knowledge.

Applications of cryptography in secure networking

Billy Brumley, Jan-Erik Ekberg, Maarit Hietalahti, Kaisa Nyberg, Aleksi Toivonen, Johan Wallén, and Jukka Valkonen

This topic covers work done by different group members in three different projects: PLA (Billy Brumley, Kaisa Nyberg and Johan Wallén), InHoNets

(Billy Brumley, Jan-Erik Ekberg, Kaisa Nyberg, Aleksi Toivonen and Jukka Valkonen), and Ad Hoc Networks (Maarit Hietalahti and Kaisa Nyberg).

In the PLA project the task was two-fold. First a secure and efficient signature scheme and certification scheme was designed. This was accomplished by Kaisa Nyberg and Johan Wallén. Secondly, an efficient software implementation had to be created. Billy Brumley developed a few enhancements to the existing elliptic curve implementation methods [12], [13]. He also started 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. Billy Brumley completed his Master's thesis in December on this topic [66].

Within the InHoNets project the researchers of the Crypto Group worked on following topics:

- Ad-Hoc Security Associations for Wireless Devices. This was a Master's thesis project by Jukka Valkonen completed in September [71].

- Design of a manually authenticated group key agreement method published in [53] (Kaisa Nyberg and Jukka Valkonen in collaboration with N. Asokan).

- Design of a lightweight security system for the Wibree radio. This was a licenciate thesis project by Jan-Erik Ekberg. The licenciate thesis is expected to be completed in 2007.

- Usability testing of different pairing methods for personal devices in home environment (Jukka Valkonen and Aleksi Toivonen in collaboration with Kristiina Karvonen from the TML laboratory). A set of tests were perfomed and a report will be published in September 2007 in IWSSI 2007 -workshop. The tests were implemeted using a framework developed at Nokia Research Center. Jukka Valkonen spent a three-month internship at NRC with the task to study the tool, learn to use it, and customize it for this particular test setting.

In the Ad Hoc Networks -project, Maarit Hietalahti and Kaisa Nyberg reviewed the security architecture document that had been created earlier in the project by other partners. Significant improvements were suggested. Also a solution for secure delivery of data to a legitimate but possibly revoked recipient was proposed.

In Autumn 2006 the post graduate course T-79.7001 was organised in cooperation with prof. N. Asokan from the TML laboratory. The topic was authenticated key agreement. In total four papers, written and presented in this seminar, have subsequently been published in workshops and conferences in 2007, and three of them were (co-)authored by researchers of the TSC Crypto group.

5 CONFERENCES, VISITS, AND GUESTS

5.1 Conferences

This section summarizes the conference participation of the personnel of the Laboratory for Theoretical Computer Science in 2006. The conferences are ordered chronologically.

January

The Finnish Mathematical Days 2006, Tampere, Finland. January 4–6. Participant: Sven Laur

5th Nordic Grid Neighbourhood workshop, Uppsala, Sweden. January 18–20. Participant: Antti Hyvärinen

The 32nd International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 06), Merin, Czech Republic, January 20–28. Participant: Satu Elisa Schaeffer

March

Estonian Winter School in Computer Science, Palmse, Estonia. March 5–10. Participants: Jukka Valkonen and Sven Laur

Fast Software Encryption 2006, FSE 2006, Graz, Austria. March 15–17. Participants: Kaisa Nyberg and Johan Wallen

April

5th International Conference on Networking (ICN06), Mauritius, April 23–29. Participant: Stefano Marinoni

May

Helsinki–Rutgers Ph.D. Student Workshop on Spontaneous Networking, Piscataway, New Jersey, USA, May 8–12. Participant: Satu Elisa Schaeffer

MEAs and Mceas, ISCRAM2006, Newark, New Jersey, USA, May 14–17. Participant: Mikko Särelä

6th International School on Formal Methods for the Design of Computer, Communication and Software Systems, Bertinoro, Italy, May 21–28. Participant: Matti Järvisalo

The 25th International Cryptology Conference, Eurocrypt 2006, Saint Petersburg, Russia, May 28–June 1. Participants: Sven Laur and Johan Wallén

11th International Workshop on Non-Monotonic Reasoning, NMR'06, (NMR'06), Lake District, Great Britain, May 29–June 2. Participants: Emilia Oikarinen, Ilkka Niemelä, Tomi Janhunen and Tommi Syrjänen

June

10th International Conference on Principles of Knowledge Representation and Reasoning, KR 2006, Lake District, Great Britain, June 2–5. Participant: Emilia Oikarinen

Tietojenkäsittelytieteen päivät 2006, Kumpula, Helsinki, June 5–6. Participant: Antti Hyvärinen

13th International Symposium on Temporal Representation and Reasoning (TIME 2006), Budapest, Hungary, June 14–17. Participant: Keijo Heljanko

PARA '06 Workshop on state-of-the-art in scientific and parallel computing, Umeå, Sweden, June 18–21. Participant: Antti Hyvärinen

6th International Conference on Application of Concurrency to System Design (ACSD06) 26th International Conference on Application and Theory of Petri Nets (Petri Nets06) Advanced tutorial on Bounded Model Checking, Turku, June 25–30. Participants: Keijo Heljanko and Tommi Junttila

Petri Net Markup Language Forum 26.6., Workshop on Modelling of Objects, Components and Agents; Advanced tutorial on Petri Net Modelling of Business Processes; International Conference on Application of Concurrency to System Design; International Conference on Application and Theory of Petri Nets and Other Models of Concurrency; Turku, June 26–30. Participant: Kimmo Varpaaniemi

July

IWWAN workshop, New York, USA, June 28–30. MiNEMA workshop, Lisbon, Portugal, July 2–3. Participant: Mikko Särelä

ICALP 2006 (International Colloquium on Automata, Languages and Programming) and Workshop AlgoSensors 2006 (Algorithmic Aspects of Wireless Sensor Networks), Venice, Italy, July 9–16. Participant: Pekka Orponen

International Summer School on Grid Computing 2006, Ischia, Italy, July 9–21. Participant: Antti Hyvärinen

21st National Conference on Artificial Intelligence (AAAI-06), Boston, USA, July 15–20. Participant: Matti Järvisalo

August

Summer School on "Software System Reliability and Security", Marktoberdorf, Germany, August 1–13. Participant: Jori Dubrovin

Fedarated logic conference (FLOC 2006), Seattle, USA, August 9–22. Participants: Ilkka Niemelä, Keijo Heljanko and Antti Hyvärinen

Summer School in Wireless Sensor Networks, and 5th International Conference on AD-HOC Networks & Wireless, Ottawa, Canada, August 14–19. Participant: André Schumacher

The twelfth annual international conference on Knowledge Discovery and Data mining, Philadelphia, USA, August 19–25. Participant: Sven Laur

Crypto Santa Barbara, NIST Hash Workshop, Santa Barbara, USA, August 20–24. Participant: Kaisa Nyberg

The 17th European Conference on Artificial Intelligence (ECAI-06), Riva del Garda, Italy, August 28–September 1. Participants: Ilkka Niemelä, Tomi Janhunen and Emilia Oikarinen

"Towards a Science of Networks Workshop: Communication Networks

and Complexity", Greece, August 30–September 2. Participant: Hannu Kari

September

Optimal Discrete Structures and Algorithms (ODSA 2006), Rostock, Germany, September 3–6. Participant: Harri Haanpää

Reasoning Web 2006 Summer School, Lisbon, Portugal, September 4–8. Participant: Emilia Oikarinen

The 10th European Conference on Logics in Artificial Intelligence (JELIA '06), Liverpool, Great Britain, September 12–15. Participants: Ilkka Niemelä and Tomi Janhunen

Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2006), Hamburg, Germany, September 18–21. Participant: Jukka Valkonen

20th International Symposium on Distributed Computing, Stockholm, Sweden, September 18–20. Participant: Pekka Orponen

Twelfth International Conference on Principles and Practice of Constraint Programming, Nantes, France, September 25–30. Participant: Matti Järvisalo

October

NordSec 2006, Linköping, Sweden, October 18–22. Participant: Billy Brumley

EU DELIS-CompNet Workshop on Theoretical Aspects & Models of Large, Complex & Open Information Networks, Barcelona, Spain, October 17–21. Participant: Pekka Orponen

November

EU/US Summit, Dublin, Ireland, November 15–16. Participant: Mikko Särelä.

IST 2006 – Information Society Technologies Conference, Helsinki, November 21–23. Participants: Keijo Heljanko, Tommi Junttila and Kaisa Nyberg

December

ICICS'06 Conference in Raleigh, North Carolina, USA, December 4–7. Participant: Billy Brumley

eScience Conference in Amsterdam, The Netherlands, December 4–8. Participant: Ilkka Niemelä

Conferences Asiacrypt and CANS, Suzhou, China, December 3–10. Participant: Sven Laur

The 2nd International Conference on Mobile Ad-Hoc and Sensor Networks (MSN 2006), Hong Kong, December 11–17. Participant: André Schumacher

5.2 Visits

January

Ilkka Niemelä visited National ICT Australia (NICTA). Australia's Information and Communications Technology centre of excellence on 29 November 2005 to 21 January 2006.
Mikko Särelä made research visit to University of California, San Diego, CALIT2 Institute. He worked in a WIISARD project on 4 December 2005 to 31 July 2006.

February

Eurocrypt 2006 Program Committee Meeting in Lausanne, Switzerland, February 3–6. Participant: Kaisa Nyberg

April

Kaisa Nyberg was opponent for Hansang Kim in Sofia Antipolis on 27 to 29 April.

May

Ilkka Niemelä visited University of Texas at Austin and University of Kentucky on 1 to 12 May.

June

Ilkka Niemelä visited Universität Potsdam and Universität Leipzig, TU Clausthal on 26 June to 5 July.
Kaisa Nyberg was opponent for Alexander Maximov in Lund, Sweden, on 15 to 17 June.

October

Keijo Heljanko visited University of Newcastle, School of Computing Science on 30 October to 4 November.

November

Pekka Orponen, Mikko Särelä and Antti Tuominen visited Ericsson in Kista, Sweden on 14 November.
Sven Laur visited University of EPFL in Lausanne, Switzerland on 19 to 25 November.

December

Ilkka Niemelä visited University of Bremen, Germany on 7 December.
Kaisa Nyberg was opponent for Panu Hämäläinen in Tampere on 8 December.

Kaisa Nyberg was opponent for Mårten Trolin in Stockholm on 15 December.

Tomi Janhunen visited University of Potsdam and participated in the Platypus Workshop on 16 to 19 December.

5.3 Guests

In this section the various academic visits to the Laboratory for Theoretical Computer Science in 2006 are summarized. The host is given at the end of each entry.

April

Prof. **Josep Diaz,** Universitat Politecnica de Catalunya, Spain, 28 to 30 April, opponent of Satu Elisa Schaeffer (Orponen)

May

Prof. **Gerald Maguire,** Kungliga Tekniska Högskolan, Kista, Sweden, 15 May, opponent of Janne Lundberg (Kari)

June

M.Sc. **Shreyas Prasad,** University of California, Santa Barbara, USA, 23 June to 15 August, IAESTE summer trainee (Orponen)

September

Alexander Maximov, University of Luxembourg, 30 August to 8 September; talk at TCS Forum on 1 September (Nyberg)

Henrik Petander, National ICT Australia, 8 September, talk at TCS Forum (Kari)

Dr. **Paul B. Losiewicz,** European Office of Aerospace Research and Development, Great-Britain, 12 September (Kari)

Prof. **Hans Tompits,** Technical University of Vienna, 20 September (Janhunen)

Dr. **Stefan Woltran,** Technical University of Vienna, 20 September, talk at TCS Forum (Janhunen)

Alexandre Duret-Lutz, Laboratoire d'Informatique de Paris 6, France, 22 September, talk at TCS Forum (Heljanko)

October

Prof. **Elias Koutsoupias** University of Athens, Greece and Prof. **Christian Scheideler** Technische Universität Munchen, Germany, 25 to 29 October (Orponen)

Prof. **Thomas Wilke,** Christian-Albrechts-Universität zu Kiel, Germany, 26 to 28 October, opponent of Heikki Tauriainen (Niemelä)

November

Prof. **Bart Preneel,** Katholieke Universiteit Leuven, Germany, 23 November, talk at TCS Forum (Nyberg)
Prof. **Fabio Massacci,** Università di Trento, Italy, 23 November, talk at TCS Forum (Niemelä)
M.Sc. **Orkunt Sabuncu,** Middle East Technical University, Turkey, 23 November (Niemelä)

December

Prof. **Rance Cleaveland,** University of Maryland, USA, 14 to 17 December, opponent of Misa Keinänen (Niemelä)
Prof. **Gerard Ang,** Dr. **Mun Kew Leong,** Dr. **Feng Bao,** Dr. **Shen Tat Goh,** and Dr. **How Lung Eng,** Agency for Science, Technology and Research, Singapore, 15 December (Kari)
Prof. **Satu Elisa Schaeffer,** Universidad Autonoma de Nuevo Leon, Mexico, 22 December to 18 January, research (Orponen)

6 SCIENTIFIC EXPERT TASKS

This section summarizes the scientific expert tasks carried out by the personnel of Laboratory for Theoretical Computer Science in 2006. 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

Hannu H. Kari, Finnish delegate on behalf of National Emergency Service Agency at EU CI2RCO project dealing with Critical Information Infrastructure Research Co-ordination
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 the board of Maanpuolustuksen tieteellinen neuvottelukunta (MATINE, Scientific Advisory Board for Defence)

6.2 Memberships in editorial boards

Hannu H. Kari, member of the editorial board of Journal of Security, Information and Society
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) and of International Journal of Information Security (IJIS).

6.3 Scientific expert duties

Hannu H. Kari, pre-examiner of Ville Saarikoski at University of Oulu; pre-examiner of Justin Pierce at Deakin University, Geelong, Australia
Kaisa Nyberg, statement concerning filling a professor position in Cryptology at University College London, U.K.; official opponent of Kim Hahn-sang at L'Institut National des communications and l'Universit d'Evry-Val d'Essonne, France; official opponent of Alexander Maximov at Lund University, Sweden; official opponent of Panu Hämäläinen at Tampere University of Technology; official opponent of Mårten Trolin at Kungliga Tekniska Högskolan, Sweden
Pekka Orponen, statement concerning filling a professor position in "tietokoneavusteinen matematiikka" (computer-aided mathematics) at University of Helsinki

7 PUBLICATIONS

7.1 Journal Articles

[1] Armin Biere, Keijo Heljanko, Tommi Junttila, Timo Latvala, and Viktor Schuppan. Linear encodings of bounded LTL model checking. *Logical Methods in Computer Science*, 2(5:5), 2006. (doi: 10.2168/LMCS-2(5:5)2006).

[2] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Silvio Ranise, Peter van Rossum, and Roberto Sebastiani. Efficient theory combination via boolean search. *Information and Computation*, 204(10):1493–1525, October 2006.

[3] Malcolm Greig, Harri Haanpää, and Petteri Kaski. On the coexistence of conference matrices and near resolvable 2-(2k+1, k, k-1) designs. *Journal of Combinatorial Theory, Series A*, 113(3):703–711, May 2006.

[4] Harri Haanpää, Matti Järvisalo, Petteri Kaski, and Ilkka Niemelä. Hard satisfiable clause sets for benchmarking equivalence reasoning techniques. *Journal on Satisfiability, Boolean Modeling and Computation*, 2(1-4):27–46, 2006.

[5] Tomi Janhunen. Some (in)translatability results for normal logic programs and propositional theories. *Journal of Applied Non-Classical Logics*, 16(1–2):35–86, June 2006. Special issue on implementation of logics.

[6] Tomi Janhunen, Ilkka Niemelä, Dietmar Seipel, Patrik Simons, and Jia-Huai You. Unfolding partiality and disjunctions in stable model seman-

tics. *ACM Transactions on Computational Logic*, 7(1):1–37, January 2006.

[7] Petteri Kaski, Patric R.J. Östergård, and Olli Pottonen. The steiner quadruple systems of order 16. *Journal of Combinatorial Theory. Series A*, 113(8):1764–1770, 2006.

[8] Stefano Marinoni and Hannu Kari. Ad hoc routing protocol's performance: a realistic simulation based study. *Telecommunication Systems*, 33(1-3):269–289, 2006.

[9] Jussi Rintanen, Keijo Heljanko, and Ilkka Niemelä. Planning as satisfiability: parallel plans and algorithms for plan search. *Artificial Intelligence*, 170(12-13):1031–1080, 2006.

[10] Heikki Tauriainen. Nested emptiness search for generalized Büchi automata. *Fundamenta Informaticae*, 70(1-2):127–154, 2006.

7.2 Conference Papers

[11] Christian Anger, Martin Gebser, Tomi Janhunen, and Torsten Schaub. What's a head without a body? In Gerhard Brewka, Silvia Coradeschi, Anna Perini, and Paolo Traverso, editors, *Proceedings of the 17th European Conference on Artificial Intelligence*, pages 769–770, Riva del Garda, Italy, August 2006. IOS Press.

[12] Billy Bob Brumley. Efficient three-term simultaneous elliptic scalar multiplication with applications. In Viiveke Fåk, editor, *Proceedings of the 11th Nordic Workshop on Secure IT Systems (NordSec 2006)*, pages 105–116, Linköping, Sweden, October 2006.

[13] Billy Bob Brumley. Left-to-right signed-bit τ-adic representations of n integers (short paper). In *International Conference on Information and Communications Security – ICICS'06*, volume 4307 of *Lecture Notes in Computer Science*, pages 469–478, Raleigh, North Carolina, USA, December 2006. Springer-Verlag.

[14] Ahto Buldas and Sven Laur. Do broken hash functions affect the security of time-stamping schemes? In Jianying Zhou, Moti Yung, and Feng Bao, editors, *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*, volume 3989 of *Lecture Notes in Computer Science*, pages 50–65. Springer, 2006.

[15] Jean Gressmann, Tomi Janhunen, Robert Mercer, Torsten Schaub, Sven Thiele, and Richard Tichy. On probing and multi-threading in platypus. In Gerhard Brewka, Silvia Coradeschi, Anna Perini, and Paolo Traverso, editors, *Proceedings of the 17th European Conference on Artificial Intelligence*, pages 392–396, Riva del Garda, Italy, August 2006. IOS Press.

[16] Jean Gressmann, Tomi Janhunen, Robert Mercer, Torsten Schaub, Sven Thiele, and Richard Tichy. On probing and multi-threading in platypus. In Jürgen Dix and Anthony Hunter, editors, *Proceedings of the 11th International Workshop on Nonmonotonic Reasoning*, pages 30–38, Lake District, UK, May 2006. University of Clausthal, Department of Informatics, Technical Report, IfI-06-04.

[17] Keijo Heljanko, Tommi Junttila, Misa Keinänen, Martin Lange, and Timo Latvala. Bounded model checking for weak alternating Büchi automata. In Thomas Ball and Robert B. Jones, editors, *Proceedings of the 18th International Conference on Computer Aided Verification (CAV'2006)*, volume 4144 of *Lecture Notes in Computer Science*, pages 95–108, Seattle, WA, USA, August 2006. Springer-Verlag.

[18] Antti E. J. Hyvärinen. Lauselogiikan toteutuvuusongelman ratkaiseminen laskennallisessa gridissä. In Lea Kutvonen and Päivi Kuuppelomäki, editors, *Tietojenkäsittelytieteen päivät 2006*, volume B-2006-3 of *Tietojenkäsittelytieteen laitoksen julkaisjua sarja B*, pages 37 – 43. Tietojenkäsittelytieteen laitos, 2006.

[19] Antti E. J. Hyvärinen, Tommi Junttila, and Ilkka Niemelä. A distribution method for solving SAT in grids. In Armin Biere and Carla P. Gomes, editors, *SAT 2006*, volume 4121 of *Lecture Notes in Computer Science*, pages 430–435. Springer, 2006.

[20] Matti Järvisalo. Further investigations into regular XORSAT. In *Proceedings of the Twenty-First National Conference on Artificial Intelligence (AAAI-06)*, pages 1873–1874. AAAI Press, 2006.

[21] Matti Järvisalo. Opinions, hopes, and expectations of CS&E students, a case study in academic skills and hidden curriculum. In Tapio Salakoski, Tomi Mäntylä, and Mikko Laakso, editors, *Koli Calling 2005 – Proceedings of the Fifth Finnish / Baltic Sea Conference on Computer Science Education*, volume 41 of *TUCS General Publications*, pages 157–161. Turku Centre for Computer Science, January 2006. ISBN 951-29-3006-4.

[22] Toni Jussila, Jori Dubrovin, Tommi Junttila, Timo Latvala, and Ivan Porres. Model checking dynamic and hierarchical UML state machines. In *MoDeV^{2}a: Model Development, Validation and Verification; 3rd International Workshop, Genova, Italy, October 2006*, pages 94–110, 2006.

[23] Hannu Kari. Dynamic trust management for decision making systems using context aware management/policy manager architecture. Centre for Research and Technology, Hellas, Kreikka, 2006.

[24] Hannu Kari. Dynamic trust management for decision making systems using context aware management/policy manager architecture. 2006.

[25] Hannu Kari. Future of digital communication and internet. 2006.

[26] Hannu Kari. Identification and identities in the digital world. Tieturi, 2006.

[27] Hannu Kari. Infinite bandwidth ...or..future of networks and people. World Transhumanist Association, 2006.

[28] Hannu Kari. Information security. Teknillinen korkeakoulu, 2006.

[29] Hannu Kari. Laajakaistayhteiskunnan haasteet. 2006.

[30] Hannu Kari. Protecting network infrastructures with strong cryptographic algorithms the concept of packet level authentication (pla). www.citris-uc.org, 2006.

[31] Hannu Kari. Tiedonsiirron haasteet. 2006.

[32] Hannu Kari. Turvallinen sähköposti. In *Turvallinen sähköposti*. IIR Finland Oy, 2006.

[33] Hannu Kari. Vapaa internet on kuollut - eläköön turvalliset virtuaaliyhteisöt. Hämeen kesäyliopisto kumppaneinaan Opetusministeriö, Kuntaliitto, Tampereen yliopisto, Helsingin, Hämeenlinnan, Tornion ja Tampereen kaupungit, Suomen rehtorit ry, Opetusalan ammattijärjestö Oaj sekä yrityspartnereina Microsoft, Suomen Messut, TietoEnator, 2006.

[34] Hannu Kari and Sasase Iwao. Evaluation report: Vtt strategic technology theme future communications technologies. Technical report, VTT, 2006.

[35] Hannu H. Kari. Protecting network infrastructures with strong cryptographic algorithms the concept of packet level authentication (pla). 2006.

[36] Hannu H. Kari. Utilizing data networks in stealth attacks. 2006.

[37] Teemu Koponen, Pasi Eronen, and Mikko Särelä. Resilient connections for SSH and TLS. In *Proceedings of the 2006 Usenix Annual Technical Conference*, Boston, MA, USA, Jun 2006. Usenix.

[38] Sven Laur, Helger Lipmaa, and Taneli Mielikäinen. Cryptographically private support vector machines. In *KDD '06: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 618–624, New York, NY, USA, 2006. ACM Press.

[39] Sven Laur and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings. In *The 5th International Conference on Cryptology and Network Security, CANS 2006, Suzhou, Dec. 8 - 10, 2006*, volume 4301 of *Lecture Notes in Computer Science*, pages 90–107. Springer, 2006. A shortened version of ePrint Report 2005/424.

[40] Stefano Marinoni and Hannu H. Kari. Ad hoc routing protocol performance in a realistic environment. In *Proceedings of the Fifth IEEE International Conference on Networking (ICN 2006)*, Le Morne, Mauritius, April 2006. IEEE Press.

[41] Ilkka Niemelä. Answer set programming: A declarative approach to solving search problems. In *Proceedings of the 10th European Conference on Logics in Artificial Intelligence*, volume 4160 of *Lecture Notes in Computer Science*, pages 15–18. Springer, 2006.

[42] Ilkka Niemelä. Answer set programming: Foundations, implementation techniques, and applications. In *Proceedings of the ICLP 2006 Workshop on Search and Logic: Answer Set Programming and SAT*, page 35, 2006. Abstract of an invited talk.

[43] Ilkka Niemelä. Bounded model checking, answer set programming, and fixed points. In *Proceedings of the CAV'06 Workshop on Bounded Model Checking (BMC06)*, page 9, 2006. Abstract of an invited talk.

[44] Kaisa Nyberg and Johan Wallén. Improved linear distinguishers for SNOW 2.0. In *Fast Software Encryption 2006*, Lecture Notes in Computer Science. Springer-Verlag, 2006.

[45] Emilia Oikarinen and Tomi Janhunen. Modular equivalence for normal logic programs. In Jüergen Dix and Anthony Hunter, editors, *Proceedings of the 11th International Workshop on Nonmonotonic Reasoning*, pages 10–18, Lake District, UK, May 2006. University of Clausthal, Department of Informatics, Technical Report, IfI-06-04.

[46] Emilia Oikarinen and Tomi Janhunen. Modular equivalence for normal logic programs. In Gerhard Brewka, Silvia Coradeschi, Anna Perini, and Paolo Traverso, editors, *Proceedings of the 17th European Conference on Artificial Intelligence*, pages 412–416, Riva del Garda, Italy, August 2006. IOS Press.

[47] Kati Rantala, Sirpa Virta, Maija-Riitta Ollila, Janne Kivivuori, Pekka Sulkunen, Hannu Kari, Jarkko Sipilä, and Kari Haavisto. Tieto ja turvallisuus internetissä – mahdollisuuksia ja uhkia. In Kati Rantala and Sirpa Virta, editors, *Tieto - mahdollisuus, uhka vai turva?* Poliisiammattikorkeakoulu, Helsinki, 2006.

[48] Mikko Särelä. Multi-homed internet access in ad hoc networks using host identity protocol. In *Proceedings of the MiNEMA'06 workshop*, Lisbon, Portugal, Jul 2006. MiNEMA.

[49] Satu Elisa Schaeffer, Stefano Marinoni, Mikko Särelä, and Pekka Nikander. Dynamic local clustering for hierarchical ad hoc networks. In *Proceedings of the Third IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'06), International Workshop on Wireless Ad-hoc and Sensor Networks (IWWAN'06) subtrack*, New York, NY, USA, 2006. IEEE Communications Society.

[50] André Schumacher, Harri Haanpää, Satu Elisa Schaeffer, and Pekka Orponen. Load balancing by distributed optimisation in ad hoc networks. In J. Cao, I. Stojmenovic, X. Jia, and S. K. Das, editors, *Mobile Ad-hoc and Sensor Networks*, volume 4325/2006 of *Lecture*

Notes in Computer Science, pages 873–884, Berlin / Heidelberg, 2006. Springer-Verlag.

[51] Jiří Šíma and Satu Elisa Schaeffer. On the NP-completeness of some graph cluster measures. In Jiří Wiedermann, Gerard Tel, Jarslav Pokorný, Mária Bieliková, and Július Štuller, editors, *Proceedings of the Thirty-second International Conference on Current Trends in Theory and Practice of Computer Science (Sofsem 06)*, volume 3831 of *Lecture Notes in Computer Science*, pages 530–537, Berlin/Heidelberg, Germany, 2006. Springer-Verlag GmbH.

[52] Tommi Syrjänen. Debugging inconsistent answer set programs. In *Proceedings of the 11th International Workshop on Nonmonotonic Reasoning*, pages 77–83, Clausthal, Germany, 2006. Clausthal University of Technology, Department of Informatics, Technical Report IfI-06-04.

[53] Jukka Valkonen, N. Asokan, and Kaisa Nyberg. Ad-Hoc Security Associations for Groups. In *Third European Workshop, ESAS 2006, Hamburg, Germany, September 20-21, 2006, Revised Selected Papers*, number 4357 in Lecture Notes in Computer Science, 2006.

7.3 Books

[54] Petteri Kaski and Patric R. J. Östergård. *Classification Algorithms for Codes and Designs*. Number 15 in Algorithms and Computation in Mathematics. Springer-Verlag, Berlin Heidelberg, 2006.

7.4 Reports

[55] Jori Dubrovin. Jumbala — an action language for UML state machines. Research Report A101, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, March 2006.

[56] Antti E. J. Hyvärinen. SATU: A system for distributed propositional satisfiability checking in computational grids. Research Report A100, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, February 2006.

[57] Sven Laur and Helger Lipmaa. Consistent adaptive two-party computations. Cryptology ePrint Archive, Report 2006/088, 2006. Techical report.

[58] Sven Laur and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings: Extended version. Cryptology ePrint Archive, Report 2005/424, 2006. A shorter more compact version was published at CANS 2006.

[59] Emilia Oikarinen. Modular answer set programming. Research Report A106, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, December 2006.

7.5 Doctoral Dissertations

[60] Misa Keinänen. Techniques for solving boolean equation systems. Research Report A105, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, November 2006. Doctoral dissertation. Pre-examiners: H. R. Andersen and M. Jurdzinński. Opponent: Rance Cleaveland.

[61] Janne Lundberg. A wireless multicast delivery architecture for mobile terminals. Research Report A103, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, May 2006. Doctoral dissertation. Pre-examiners: Jarmo Harju and Göran Schultz. Opponent: Gerald Maguire Jr.

[62] Satu Elisa Schaeffer. Algorithms for nonuniform networks. Research Report A102, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, April 2006. Doctoral dissertation. Pre-examiners: Erkki Mäkinen and Sergey Dorogovtsev. Opponent: Josep Diaz.

[63] Heikki Tauriainen. Automata and linear temporal logic: Translations with transition-based acceptance. Research Report A104, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, September 2006. Doctoral dissertation. Pre-examiners: Orna Kupferman and Stephan Merz. Opponent: Thomas Wilke.

7.6 Licentiate's Theses

[64] Emilia Oikarinen. *Modular Answer Set Programming*. Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

7.7 Master's Theses

[65] Antti Ahonen. Radio network optimisation with spatial database tools. Master's thesis, Helsinki University of Technology, Department of Electrical and Communications Engineering, 2006.

[66] Billy Bob Brumley. Efficient elliptic curve algorithms for compact digital signatures. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

[67] Jori Dubrovin. Jumbala — an action language for UML state machines. Master's thesis, Helsinki University of Technology, Department of Engineering Physics and Mathematics, 2006.

[68] Jukka Honkola. Modeling the SpaceWire network architecture with the Lyra method. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

[69] Janne Nykopp. Stratum—yleiskäyttöinen automaattinen koneisharjoitusjärjestelmä. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

[70] Amir Houshang Taheri. An application programming interface for vertical handover enabled applications. Master's thesis, Helsinki University of Technology, Department of Electrical and Communications Engineering, 2006.

[71] Jukka Valkonen. Ad-Hoc Security Associations for Wireless Devices. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2006.

7.8 Patents

[72] Hannu H. Kari. An access control method for a mobile communications system, 2006.

[73] Hannu H. Kari. Data transmission system with sliding-window data flow control, 2006.

[74] Hannu H. Kari. Method and apparatus for the transmission of packets of data, 2006.

[75] Hannu H. Kari. Method and system of providing a service to a subscriber, 2006.

[76] Hannu H. Kari. Method for encryption of information and data communication system, 2006.

[77] Hannu H. Kari. Voice mail server, mobile station and method for voice mail message transmission, 2006.

7.9 Software

[78] Antti E. J. Hyvärinen. Satu (sat ubiquitous), June 2006. Computer program.

[79] Tomi Janhunen. lp2sat 1.10 — translations from normal logic programs into SAT. http://www.tcs.hut.fi/Software/lp2sat/, 2006. Computer Program.

[80] Matti Järvisalo. drgen — regular *d*-XORSAT generator, February 2006. Computer program.

[81] Tommi Junttila. Bc package - tools for constrained boolean circuits, 2006.

[82] Tommi Junttila. bliss- a canonical labeling tool for graphs, 2006.

[83] Timo Latvala and Tommi Junttila. Nusmv-2.3.99-cav2006. Computer program, 2006.

[84] Ville Nuorvala. NEPL NEmo Platform for Linux, version 0.2, 2006.

[85] Ville Nuorvala and Antti Tuominen. MIPL Mobile IPv6 for Linux, version 2.0.2, 2006.

7.10 Miscellaneous publications

[86] Harri Haanpää. *Annual Report for the Year 2005*. Teknillinen korkeakoulu, Tietojenkäsittelyteorian laboratorio (Helsinki University of Technology, Laboratory for Theoretical Computer Science), Espoo, Finland, October 2006.

[87] Harri Haanpää and Patric R. J. Östergård. Steinerin kolmikkojärjestelmistä sudokuun. *Arkhimedes*, 2006(2):18–21, 2006. In Finnish.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2006