Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2005
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2005
Espoo 2006 HUT-TCS-Y2005

ANNUAL REPORT FOR THE YEAR 2005

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 2005
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosikertomus 2005
Espoo 2006 HUT-TCS-Y2005

ANNUAL REPORT FOR THE YEAR 2005

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
Helsinki 2006

ABSTRACT: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2005.

KEYWORDS: personnel, teaching, research, activities, publications

CONTENTS

1 INTRODUCTION

By all indicators of academic performance, the year 2005 of the Laboratory for Theoretical Computer Science was an outstanding success. A record number of five doctoral theses were defended (Petteri Kaski, Timo Latvala, Toni Jussila, Catharina Candolin, Antti Autere), complemented by two licentiate's theses and nine master's theses. The exceptionally high quality of graduate work at the laboratory was acknowledged by several awards: Petteri Kaski's doctoral thesis was selected as TKK's Outstanding Dissertation for 2005, Emilia Oikarinen received one of TKK's highly competitive Master's Thesis awards, and Johan Wallén the national prize awarded by the Finnish Society for Computer Science for the best Master's Thesis in 2004.

The laboratory's publication profile continued its healthy trend towards archival series: in addition to 27 papers in international conferences with printed proceeedings, a total of 12 articles were published in peer-reviewed journals in 2005, up from 9 in 2003 and 10 in 2004.

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 National Technology Agency TEKES, and graduate student positions at the Helsinki Graduate School in Computer Science and Engineering HeCSE. In February 2005, Kaisa Nyberg started as the new professor of cryptology at the laboratory. Also two new docents were appointed in 2005: Helger Lipmaa in cryptology, starting from April 2005, and Keijo Heljanko in model checking, starting from January 2006.

Out of the 1.8 M€ total budget of the laboratory in 2005, only about 0.6 M€ were operational funds provided by the university; the rest was procured by individual research proposals. While this balance shows that the laboratory is an attractive partner for research investment, maintaining such a funding structure is arduous: presently available research grants are typically small, short-term and volatile, and high dependence on them, while inevitable, induces uncertainty and 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 2005 can be found in the following sections.

2 PERSONNEL

The personnel of the Laboratory for Theoretical Computer Science in 2005 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.), Teaching researcher until July; Professor (pro tem) from August

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

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

Nyberg, Kaisa; D.Phil., Professor; on leave in January 2005, on partial leave from February to November

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

Orponen, Pekka; D.Phil., Professor; Head of the Laboratory from August

2.2 Docents

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.), Researcher until October; Teaching researcher from November

Kangasniemi, Ulla; Secretary

Klaus, Katja; Secretary, on leave from March 2005 to February 2006

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

Lassila, Eero; Lic.Sc. (Tech.) Laboratory manager, on partial leave until August

Lipmaa, Helger; PhD, Teaching researcher from January to March

Nikander, Marianne; Secretary from March 2005

Varpaaniemi, Kimmo; D.Sc. (Tech.), Teaching researcher in January and from August to 16 October; researcher from February to July and from 17 October

2.4 Researchers

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

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

Hietalahti, Maarit; M.Sc. (Tech.), on leave from November

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

Jussila, Toni; D.Sc. (Tech.)

Järvisalo, Matti; M.Sc. (Tech.)

Kaski, Petteri; D.Sc. (Tech.), until December

Keinänen, Misa; Lic.Sc. (Tech.)

Kiviluoto, Lasse; Stud. (Tech.), in April

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

Kullberg, Tuulia; M.Sc. (Tech.), on leave from 10 October

Latvala, Timo; D.Sc. (Tech.), until October

Laur, Sven; M.Sc.,

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

Marinoni, Stefano; M.Sc., on leave from 8 July to 7 August

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

Petander, Henrik; M.Sc. (Tech.)

Schaeffer, Satu Elisa; Lic.Sc. (Tech.)

Schumacher, André; Dipl.-Inf., from December

Syrjänen, Tommi; Lic.Sc. (Tech.)

Särelä, Mikko; M.Sc. (Tech.), Researcher

Tauriainen, Heikki; Lic.Sc. (Tech.), until 9 January and from August

Wallén, Johan; Lic.Sc. (Tech.)

2.5 Research Assistants

Brumley, Billy; from January to June

Červenka, Miroslav; IAESTE trainee from June to July

Dubrovin, Jori; Stud. (Tech.), from April

Hyvärinen, Antti; M.Sc. (Tech.)

Kaitala, Annukka; from September to December

Käsper, Emilia; B.Sc., until November

Laine, Jaakko; M.Sc., part time

Nuorvala, Ville; Stud. (Tech.)

Nykopp, Janne; Stud. (Tech.) part time from March to April; full time from May to October

Paukkeri, Mari-Anne; from 17 May until December

Rusanen, Antti; Stud. (Tech.) from June to August

Taheri, Amir; from 4 March

Tuominen, Antti; Stud. (Tech.)

Balakrishna Pillai, Unnikrishnan; part time from 4 to 30 April, full-time from May

Valkonen, Jukka; Stud. (Tech.) from June to August, part time from September

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–79.232

Honkola, Jukka; Stud. (Tech.) T–79.179

Ojala, Vesa; Stud. (Tech.) T–79.1001/2

Riihimäki, Vesa; M.Sc. (Tech.) T–79.165

Tynjälä, Teemu; Lic.Sc. (Tech.) T–79.232

Östergård, Patric; Professor, D.Sc. (Tech.) T–79.165

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.

In 2005, Helsinki University of Technology changed to a wholly new study structure. In the old study structure there was no B.Sc. level degree and courses were measured in study weeks, each of which represents 40 hours of work by the student. A M.Sc. degree was 180 study weeks, including 20 study weeks for the thesis.

In the study structure of 2005, many things changed. A three-year B.Sc. degree was introduced, while a M.Sc. degree is expected to take five. Courses are now measured in ECTS (European Credit Transfer System) points, and students are expected to earn 60 of them in a year. Thus, a B.Sc. is 180 credits, including 10 for the candidate thesis seminar, and a M.Sc. is an additional 120 credits, including 20 for the master's thesis.

Not only the units in which the degrees are measured, but also the structure of the degree program changed considerably. In most major and minor subjects three modules of 20 credits each are available; for a master's (candidate) degree a student must take three (two) modules in his chosen major and two (one) modules in the minor.

At the department level, the transition to the new study structure was coordinated by a workgroup chaired by Ilkka Niemelä, who was also a member of the university-level degree structure committee. At the TCS laboratory, the work required of students taking each course was systematically evaluated and used as a basis for the new credit point values. There were some changes to the selection of courses offered, mostly due to adjusting to the module structure and removing unnecessary special courses, but for most old courses there is a new very similar course with the same name.

The old course codes were of the form T–79.XXX, with each X representing a digit. The new course codes are of the form T–79.XYZZ, where X represents the level of the course (1=general studies, 2=programme studies, 3=level 1, 4=level 2, 5=level 3, 6=special, 7=post-graduate); Y represents the subfield within theoretical computer science (0=general, 1=computational logic, 2=computational complexity, 3=verification, 4=mobility management, and 5=cryptology); and ZZ is a running number in the range 00-99.

3.1 Courses Arranged in 2005

In 2005, 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 2005

The courses given in spring 2005 were still given according to the degree regulations of 1995 and measured in study weeks.

T–79.146 Logic in Computer Science: Special Topics I (2 sw)
spring, Ilkka Niemelä (Misa Keinänen)

Basics of modal logic. Current applications in computer science.

T–79.148 Introduction to Theoretical Computer Science (2 sw)
spring, Timo Latvala (Tommi Syrjänen; Antti Hyvärinen, Matti Järvisalo, Emilia Oikarinen)

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

T–79.159 Cryptography and Data Security (3 sw)
spring, Kaisa Nyberg (Johan Wallén)

Unconditional and computational security. Symmetric and asymmetric cryptography. Block ciphers, stream ciphers, public key cryptosystems, digital signatures, key distribution, secret sharing and other algorithms and protocols. Securityproofs and definitions. Modern cryptography (zero-knowledge, proofs of knowledge). New directions in cryptography. Practical applications.

T–79.161 Combinatorial Algorithms (2 sw)
spring, Harri Haanpää (Emilia Oikarinen)

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–79.165 Graph Theory (3 sw)
spring, Patric Östergård and Petteri Kaski (Vesa Riihimäki)

Introduction to graph theory. Trees, planar graphs and digraphs. Graph coloring. Random graphs. Algorithms for central graph problems. Applications. Also with code S–72.343.

T–79.179 Parallel and Distributed Digital Systems (3 sw)
spring, Kimmo Varpaaniemi (Jukka Honkola, Misa Keinänen)

Modelling digital systems. Concurrency. Basics of Petri nets and process algebra. Using computer aided methods.

T–79.186 Reactive Systems (2 sw)
spring, Keijo Heljanko (Misa Keinänen)

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

T–79.189 Student Project in Theoretical Computer Science (3 sw)
all TCS professors and senior lecturers; Kimmo Varpaaniemi acts as a contact person

Independent student project on a subject from the field of theoretical computer science. The project can be done ingroups of up to three people.

T–79.194 Seminar on Theoretical Computer Science (2 sw)
spring, Pekka Orponen

Current research topics in theoretical computer science. The seminar in Spring 2005 will be concerned with algorithmic and computation theoretic issues in distributed sensor networks.

T–79.230 Foundations of Agent-Based Computing (3 sw)
spring, Tomi Janhunen (Toni Jussila)

Decison-making on the basis of uncertain information. Theory, architectures, and applications for agent-based computing. As a project assignment, one is supposed to implement a soccer playing software agent.

T–79.232 Safety-Critical Systems (2 sw)
spring, Ilkka Herttua and Teemu Tynjälä

Safety-critical systems. The use of formal methods in the specification, modelling and verification of systems.

T–79.250 Combinatorial Models and Stochastic Algorithms (4 sw)
spring, Pekka Orponen

Combinatorial system models: random graphs, spinglasses, NK-systems. Fitness landscapes of combinatorial optimisation problems. Markov chains and MCMC sampling. Stochastic algorithms: MCMC-based approximation algorithms, simulated annealing, evolutionary algorithms. Special topics: structure of fitness landscapes, combinatorial phase transitions.

T–79.295 Individual Studies (1–10 sw)
TCS professors

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

T–79.300 Postgraduate Course in Theoretical Computer Science (2–10 sw)

spring, Hannu H. Kari

Current research problems in theoretical computer science. The course in Spring 2005 was concerned with simulating ad hoc network using NS2 simulator.

T–79.515 Cryptology: Special Topics (2–6 sw)

spring, Helger Lipmaa

This is a graduate level course that every semester concentrates on one concrete area of cryptology.

3.3 Autumn 2005

Starting in autumn 2005, the courses given by the Laboratory for Theoretical Computer Science follow the degree regulations of 2005, and they are measured in ECTS units.

T–79.1001 Introduction to theoretical computer science T (4 cr)

autumn, Pekka Orponen (Tommi Syrjänen; Antti Hyvärinen, Vesa Ojala, Antti Rusanen)

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)

autumn, Pekka Orponen (Tommi Syrjänen; Antti Hyvärinen, Vesa Ojala, Antti Rusanen)

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

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)

autumn, Tomi Janhunen (Emilia Oikarinen)

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

T–79.5103 Computational complexity theory (5 cr)

autumn, Tomi Janhunen (Matti Järvisalo)

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

T–79.5201 Discrete structures (4 cr)
autumn, Pekka Orponen

Annually varying topics concerned with the basic structures and methods of computer science theory. The course in Autumn 2005 will be concerned with Boolean circuit complexity.

T–79.5302 Symbolic model checking (4 cr)
autumn, Tommi Junttila and Kimmo Varpaaniemi

Symbolic methods for efficient qualitative analysis of parallel and distributed systems. Binary decision diagrams. Bounded model checking.

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

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

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

Current research problems in mobility management area. The course in Autumn 2005 was concerned with hand-off algorithms in wireless networks.

T–79.5501 Cryptology (5 cr)
autumn, Kaisa Nyberg (Emilia Käsper)

Mathematical properties of modern cryptographic methods. Information theory of encryption. Basic building blocks for stream ciphers and block ciphers and their analysis. Hash-functions. Information theory of authentication. Message authentication. Public key cryptosystems.

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

Current research problems in theoretical computer science. The contents of the course vary from term to term.

T–79.7002 Individual studies (1–10 cr)
autumn, 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 2004–2005, Tomi Janhunen and Matti Järvisalo completed a 15-study week Program ond 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 2005 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. The project has developed an efficient ASP system called `smodels` 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.

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.

We have studied a flexible framework to specify problem solutions (outcomes) and preferences among them [17]. The proposal combines ideas from answer-set programming (ASP), answer-set optimization (ASO) and CP-nets. The problem domain is structured into components. ASP techniques are used to specify values of components, as well as global (inter-component) constraints among these values. ASO methods are used to describe preferences among the values of a component and CP-net techniques to represent inter-component dependencies and corresponding preferences.

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

The research in this area concentrates on various formalisms for knowledge representation and transformations between them. This year we mainly concentrated on implementing Lifschitz' parallel circumscription using a linear and faithful but *non-modular* translation into disjunctive logic programs [34]. The implementation, a translator CIRC2DLP[1] for disjunctive logic programs [35, 65], enables the conscious use of varying atoms in disjunctive logic programs — leading to more elegant and concise problem representations in various domains. We have also analyzed ways to integrate prioritized circumscription into CIRC2DLP and model-based diagnosis of digital circuits as its potential application area.

We also continued our research on translating normal logic programs into sets of classical clauses. Here the objective is to utilize efficient Boolean satisfiability (SAT) solvers when computing answer sets for normal logic programs. Since 2003 we have been developing a new translation technique based on a characterization of answer sets in terms of *level numberings*. 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 2005, we continued the development and evaluation of an implementation of the translation that consists of two translators named as LP2ATOMIC and LP2SAT.[2]

Disjunctive Logic Programming

Tomi Janhunen, Ilkka Niemelä, and Tommi Syrjänen

Since 2000, we have been developing a search engine GNT[3] for the computation of answer sets for disjunctive logic programs. This engine can be used as a back-end for CIRC2DLP as described above. The front-end of GNT, i.e. the front-end LPARSE of the SMODELS[4] system, includes support for variables, disjunctions and partial answer sets. In 2005, a new syntax for disjunctions and the respective internal rule type were integrated into LPARSE.

Verifying the Equivalence of Logic Programs

Tomi Janhunen and Emilia Oikarinen

The development of programs in answer set programming resembles that in conventional programming languages: The process yields easily a series of gradually improving programs when optimizing memory consumption and/or the running time elapsed on a particular implementation. This leads to a meta-level problem of ensuring that the different versions of a program are equivalent, i.e. have the same answer sets. To address this problem, we have developed a translation-based technique for the automated verification of equivalence and its implementation LPEQ/DLPEQ[5] for normal and disjunctive logic programs, respectively. The rough idea is to translate any two logic programs of interest into a single logic program whose answer sets (if such exist) yield counter-examples to the equivalence of the two. In 2005, we extended the current implementation for weight constraint programs. The correctness of the method is established using a new notion of *visible equivalence* which enables to hide certain literals of answer sets when compared.

[1] http://www.tcs.hut.fi/Software/circ2dlp/
[2] http://www.tcs.hut.fi/Software/lp2sat/
[3] http://www.tcs.hut.fi/Software/gnt/
[4] http://www.tcs.hut.fi/Software/smodels/
[5] http://www.tcs.hut.fi/Software/lpeq/

SAT-based Planning

Keijo Heljanko and Ilkka Niemelä

Together with Jussi Rintanen (Albert-Ludwigs-Universität Freiburg, Germany) we have studied a number of semantics for plans with parallel operator application [43]. The standard semantics used most often in earlier work requires that parallel operators are independent and can therefore be executed in any order. We consider 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 formalize the semantics of parallel plans emerging in this setting, and propose effective translations of these semantics into the propositional logic. And finally we show that one of the semantics yields an approach to classical planning that is sometimes much more efficient than the existing SAT-based planners.

Boolean Satisfiability Checking

Tommi Junttila, Matti Järvisalo, and Ilkka Niemelä

A variety of interesting propositional satisfiability problem (SAT) instances stem from areas such as planning and model checking of finite state systems. Most current state-of-the-art SAT checkers assume that the input formulas are in conjunctive normal form (CNF). Direct modeling with CNF is typically cumbersome. Moreover, CNF often hides information about the structure of the original domain. Boolean circuits provide a compact and structure-preserving presentation for problems in many domains. A non-clausal generalization of the Davis-Putnam-Logemann-Loveland (DPLL) procedure to Boolean circuits has been developed and implemented by Junttila and Niemelä during recent years. We have studied the relative efficiency of variations of this method. The variations are obtained by restricting the use of the cut (splitting) rule in several natural, locality based ways. It is shown that the more restricted variations cannot polynomially simulate the less restricted ones. The results also apply to DPLL. Thus, for example, DPLL with splitting (branching) restricted to the variables corresponding to the input gates cannot polynomially simulate standard DPLL. A journal article presenting these results appeared during 2005 [6].

In collaboration with Harri Haanpää and Petteri Kaski (TCS Computational Complexity and Combinatorics Group) we have studied the problem of generating hard satisfiable SAT instances for clausal SAT solvers. In particular, we introduce the Regular XORSAT model based on transforming a random regular graph into a system of linear equations followed by clausification. Additionally, we develop 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. During 2005, this work resulted in a benchmark description [66] (with instances submitted to the 2005 SAT competition) and benchmark generator software [63].

Satisfiability Modulo Theories Checking

Tommi Junttila

In cooperation with the ITC-IRST research institute (Trento, Italy), we have done research on extending satisfiability checking beyond the propositional case in the so-called satisfiability modulo theories (SMT) framework. New 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 [14, 15, 16] and implemented in the MathSAT system (`http://mathsat.itc.it/`).

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, see e.g. [27]. In addition, in [28] we have applied answer set programming techniques to solve general systems of Boolean equations. Keinänen has written his Licentiate's Thesis [52] on these topics which has been reported in [40].

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. In 2005, we have made progress in the areas of distributed answer set programming (ASP) and grid-based satisfiability checking in this respect.

We have cooperated with Prof Schaub's group at the University of Potsdam in the development of a platform for distributed answer set solving called PLATYPUS[6] [22]. The current system supports a variety of software and hardware architectures and provides basic coordination mechanisms for the distributed computation of answer sets. This cooperation is part of the Working Group on Answer Set Programming (WASP) funded by the European Commission.

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 [55]. 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. We have developed a novel distribution method for solving SAT problem instances, called scattering. The key advantages of scattering are that it can be used in conjunction with any sequential SAT solver (including industrial black box solvers), the distribution heuristic is strictly separated from the heuristic used in sequential solving, and it requires no communication between processes solving subproblems but still allows co-

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

ordination of such processes. An implementation of the method has been developed for NorduGrid, a large widely distributed production-level grid running in Scandinavia. The implementation has been benchmarked with test cases including random 3SAT and challenging industrial benchmarks used in previous SAT competitions.

Bounded Model Checking

Keijo Heljanko, Tommi Junttila, Toni Jussila, Timo Latvala, 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 main result in encoding temporal logics is the efficient encoding of linear temporal logic with past (PLTL) properties [29], whose implementation was reported already in the year 2004. The approach has been further extended in [23] to incorporate incremental bounded model checking methods to obtain a significant boost in performance for bounded model checking of PLTL properties. The approach provides also a complete model checking procedure and it has been implemented in a prototype bounded model checker [64] built on top of the state-of-the-art NuSMV 2.2.3 model checker. The algorithms of the prototype tool will be included in the next official version of NuSMV, due to be released in 2006. The two papers mentioned above also appeared as part of Timo Latvala's Doctoral dissertation.

In the Doctoral dissertation of Toni Jussila [49] the use of different methods of exploiting concurrency in bounded model checking of asynchronous systems has been studied. The dissertation focuses on the methods using non-standard execution models for speeding up bounded model checking of asynchronous systems. On the topic of the dissertation a journal paper came out [7] discussing two important techniques used, namely, on-the-fly determinization combined with the use of non- standard execution models such as the use of step and process semantics.

Synthesis of Distributed Systems

Keijo Heljanko

In the area of synthesis of distributed systems the idea is to create a distributed implementation of a system specified in a non-distributed manner. Several different setups and notions of synthesis exists and the theoretical complexities of the subproblems of synthesis are not known. The main result on this topic in the reporting period is the conference paper [24] which settles several open problems of computational complexity relating to subproblems of synthesis.

Automata-Theoretic Methods for the Verification of Linear Time Temporal Logic
Heikki Tauriainen

This ongoing research explores 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. In the year 2005, the research has contributed a new on-the-fly explicit state language emptiness checking algorithm for nondeterministic generalized Büchi automata [45], improving previous results from 2004 and a journal article accepted for publication.

Symbolic Methods for UML Behavioural Diagrams
Ilkka Niemelä, Tommi Junttila, Jori Dubrovin, Toni Jussila, Timo Latvala

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 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. (i) that some expected behaviours ("use cases") are indeed possible in the system, (ii) the correspondence between the behaviours of different development versions of the system, and (iii) the correctness of testing behaviour of the system.

4.2 Automated Home Assignments

The STRATUM System
Janne Nykopp, Tomi Janhunen, and Pekka Orponen

In 2000–2005, our laboratory has developed a web-based learning environment which can be used to automate home assignments on basic courses in (theoretical) computer science. In the environment, (i) personal home assignments are automatically generated 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 automatically several times every day using assignment-specific automatic verifiers. In 2005, our goal was to reconstruct and improve the common infrastructure of the system known as STRATUM, which constituted Janne Nykopp's Master's thesis project.

4.3 Verification and State Space Analysis

Model Checking Algorithms
Timo Latvala

Fundamental algorithmic problems in model checking have been studied. The research has addressed different models of concurrency, different ways to specify properties, and also the use of symbolic model checking techniques. During 2005 we have contributed to research in bounded model checking (see page 13) and the results of the previous years have been collected and published as Timo Latvala's Doctoral dissertation [51].

On Stubborn Sets in the Verification of Linear Time Temporal Properties
Kimmo Varpaaniemi

The stubborn set method is one of the methods that try to relieve the state space explosion problem that occurs in state space generation. The work published in 2005 [12] concentrated on the verification of nexttime-less LTL (linear time temporal logic) formulas with the aid of the stubborn set method. The essential contribution of [12] is a theorem that gives us a way to utilize the structure of the checked formula when the stubborn set method is used and there is no fairness assumption. The theorem also applies to verification under fairness assumptions, including those which allow a predefined subset of actions to be treated unfairly.

4.4 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
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.

Satu Elisa Schaeffer completed her doctoral work on algorithmic issues in the modelling, analysis and management of large nonuniform networks. The thesis was submitted for review at the end of January 2006, and the eventual defense is expected to take place in April 2006. 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 2005, articles [36, 38] based on this material were published. In addition, the technical report [44] was accepted for publication in 2006. Satu Elisa Schaeffer's work has been supported by the project *Algorithms for Nonuniform Networks (ANNE)* from the Academy of Finland, and much of it was in 2005 done during an extended visit (Mar–Dec) to the University of Chile in Santiago.

In the area of theory and applications of stochastic search methods, the work of Sakari Seitz and Pekka Orponen on randomly generated 3-SAT instances and the surprising effectiveness of focused local search algorithms such as WalkSAT and Focused Metropolis Search was presented at the SAT05 conference [39] and later expanded to a journal paper [11].

In the related area of structure of optimisation landscapes, Pekka Orponen's joint paper with Evan Griffiths on a combinatorial characterisation of "No Free Lunch" landscapes was published in 2005 [3].

Coding Theory and Optimisation

Harri Haanpää and Petteri Kaski

In 2005 the group continued their work on classification algorithms. With algorithms of this type, computational classification results have been obtained for various structures, including Steiner triple and quadruple systems, near resolvable 2-designs, conference matrices, one-factorizations of regular graphs, sum packings of Abelian groups, etc. Structures for which other (algebraic, combinatorial, and computational) methods have been applied include point codes of Steiner triple systems of order 19 and whist tournaments. Many of the computational results have been obtained with very CPU-intensive computations, some of which have been distributed using the distributed batch system `autoson` over the computer network of the laboratory. In 2005, Petteri Kaski and Patric Östergård finished their book Classification Algorithms for Codes and Designs, available from Springer in early 2006. One joint topic of interest has been using expander graphs to generate satisfiability instances that are hard for current solvers [66] in cooperation with Matti Järvisalo and Ilkka Niemelä.

Petteri Kaski defended his doctoral thesis [50] in June 2005. In 2005, the group contributed to the journal articles [4, 5, 8, 9].

Distributed Algorithmics

Antti Autere, Harri Haanpää, Maarit Hietalahti, Annukka Kaitala, Petteri Kaski, Stefano Marinoni, André Schumacher, Mikko Särelä and Pekka Orponen

The group applies combinatorial and complexity-theoretic methods to the solution of algorithmic problems in distributed systems. Much of the work in 2005 was done in close collaboration with researchers from the University of Helsinki Department of Computer Science and the TKK Networking Laboratory, as part of the consortium *Networking and Architecture for Proactive Systems (NAPS)* (`http://www.cs.helsinki.fi/hiit_bru/projects/naps/`), funded by the Academy of Finland as part of its *Proactive Computing (PROACT)* research programme. Other work in this area has been supported by the projects *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 NAPS/ACSENT collaboration, work in 2005 continued in the area of energy-efficient and fault-tolerant data gathering techniques in wireless sensor networks. Towards the end of the year, also new joint work with the TKK Networking Laboratory was initiated on the topic of optimal allocation of communication network transmission modes. During the year, two journal articles [1, 2] describing earlier work of the group were published: the former considers the problem of maximising the lifetime of a multicast connection in an energy-constrained radio network, and the latter the problem of optimally balanced data gathering in a similarly energy-constrained network of sensors. During the Autumn term of 2005, Ms. Annukka Kaitala visited the group from the Royal Institute of Technology KTH to work on her M.Sc. thesis on power-aware dynamic source routing, and in December Dipl.-Inf. André Schumacher joined the group from TU Darmstadt to pursue doctoral studies in the applications of optimisation techniques to the management of communication networks.

Within the SAMOYED project, Maarit Hietalahti continued to work on her Lic.Sc. thesis on security and trust relations in mobile networks until going away on maternity leave in November. During the leave, she was substituted first by Stefano Marinoni and then by Antti Tuominen, who is working on a Linux-based prototype implementation of the clustering and cluster-based routing methods developed earlier in the project. Simulation studies of these methods using the ns2 simulation tool were performed in Autumn 2005 by Mikko Särelä and Stefano Marinoni. In December, Mikko Särelä departed for a seven-month visit to the University of California, San Diego, where he will be working on security and mobility issues in wireless emergency response systems.

Supported by a personal grant from TKK, Antti Autere completed his doctoral work on the theory and applications of the A^* search algorithm, and defended his dissertation [47] in December 2005. Among other results, the thesis presents an application of the A^* methodology to energy-efficient routing in ad hoc networks.

4.5 Mobility management

Work in the area of mobility management led by Prof. Hannu H. Kari is structured in four research projects CAN, Brocom, GO-CORE and UbiComp which are described below.

CAN: core ad hoc networks
Hannu H. Kari and Catharina Candolin

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to establish and maintain communications. Naturally, if such an infrastructure exists, the nodes will take advantage of it for better performance, security, and quality of service. In most cases the ad hoc network will have access to at least some kind of fixed infrastructure, which also may have been established dynamically and for temporary usage only. Such an infrastructure can be called a core ad hoc network, as it functions as a core network for more mobile ad hoc networks, but it is also established in an ad hoc fashion, i.e. on demand.

Ad hoc networks have been seen as a solution for military and disaster recovery networking in the future. Wireless networks have already now been successfully deployed on the battlefields around the world, and research is going on to improve the capabilities of the systems to allow more flexibility and better survivability. In this project, survivability is enhanced by allowing nodes to reconfigure their tasks in the network as the environment changes.

Nodes are reconfigured by relying on an architecture for context aware management. The main criteria considered in this project are security, reliability, and performance.

The development of better networking solutions support the network-centric approach that many armed forces around the world are deploying. The purpose of network-centric warfare (NCW) is to connect sensors, shooters, and decision makers in order to achieve information superiority. NCW recognizes three domains: the physical domain, which is the traditional domain of warfare and where the networks reside, the information domain, which is ground zero in this new concept of warfare, and the cognitive domain. The main asset is information. The networks are merely a tool for distributing information in a timely fashion to all needing entities regardless of their location. However, for the NCW concept to function, the underlying networks must be robust and secure. The same applies for the networks of armed forces that do not directly deploy NCW, but still rely on technical solutions to distribute information between entities.

As a conclusion of this project, Catharina Candolin defended her dissertation [48] in December 2005.

The Mobility/Multicast subproject of Brocom

Hannu H. Kari and Janne Lundberg

Multicast enables sending data efficiently from one or more senders to a group of receivers. The size of the group of receivers has virtually no upper limit, and in the Internet, it can potentially be as large as millions.

The Mobility/Multicast subproject of the Brocom (Broadcast communication) project administered by IDC (Institute of Digital Communications in Helsinki University of Technology) develops new ways of distributing data to mobile clients using multicast delivery. The clients can be connected to the Internet through some wireless or wireline technology. The subproject is designing and implementing a prototype of a multicast system that can utilize any current or future wireless technology that can transmit IP-packets. The focus of the subproject is on developing multicast caching and on the efficient use of the radio interface. The subproject is building the necessary multicast and mobility related software that will allow other Brocom subprojects to build applications that support multicast as well as to test new radio access technologies.

As a conclusion of this project, Janne Lundberg will defend his dissertation in May 2006.

GO-CORE – a mobility architecture for heterogeneous wireless networks

Hannu H. Kari, Jaakko Laine, Ville Nuorvala, Henrik Petander, Antti Tuominen, Stefano Marinoni, and Tuulia Kullberg

Ubiquitous access to services, potentially tailored for mobile users, is the main driver of wireless data networking. Short range wireless communications technologies allow users to access these services locally at high speeds and potentially at low price. However, due to the short range, these networks often have limited coverage. Use of IP based mobility management protocols makes it possible to bind these short range networks together and join them to wide area networks providing broader coverage.

The GO-CORE project administered by IDC (Institute of Digital Communications in Helsinki University of Technology) develops a mobility architecture with the aim of providing users with seamless communications in a heterogeneous networking environment. The architecture brings together mobile networks and use of multiple wireless interfaces in mobile nodes. GO-CORE has developed a prototype of the Mobile IPv6 mobility management protocol for use in the mobility architecture. The prototype supports three major categories of mobility management protocols: Mobile IP (MIPLv6), network mobility (NIPLv6), and ad hoc networking (AODVv6). This prototype is used for managing mobility in heterogeneous wireless IPv6 networks and is also used as a basis for further work in the field of node and network mobility.

UbiComp: Privacy issues in wireless world

Hannu H. Kari, Mari-Sanna Paukkeri, Amir Taheri, Unnikrishan Pillai

Wireless communication reveals alot of information of the communication devices. Even in the case, where communication is secured with end-to-end encryption, outsiders can easily detect, who is communicating with whom, where they are located and when the communication happens. These additional pieces of information are as crucial as the actual content of the messages. Thus, it is important to study new methods to protect various categories of the privacy of users and computers in modern wireless and wired data networks.

In this research project, funded by the Academy of Finland, we have studied the privacy issues of persons that are using wireless networks. This project has worked together with CAN-project and has utilized the six level privacy categorization developed earlier in CAN-project. In this UbiComp-project, we have also evaluated the impacts of legistlation to the privacy issues. In principle, our legistlation protects our privicy by criminating acts of persons or organizations that are obtaining and using without a proper justification any kind of information of our communication. However, the laws do not prevent prevent the breach of information but only punishes the wrongdoers. Hence, we need to have technical means that minimizes the risks of information leakage. Hence, this work has produced technical means to protect individual persons privacy but also at the same time discussed the means how criminals could be indentified.

4.6 Cryptology

Cryptanalysis of symmetric primitives

Lasse Kiviluoto, Emilia Käsper, Kaisa Nyberg, Jukka Valkonen, Johan Wallén

This group develops and implements cryptanalytic methods for different symmetric cryptographic primitives. In 2005 the main focus was on cryptanalysis of stream ciphers.

In her master's thesis work Emilia Käsper investigated the existing cryptanalytic attacks on the stream cipher A5/1 which is the main and most widely used encryption algorithm for protecting confidentiality over the air interface in GSM networks.

The most extensive work in 2005 was carried on the SNOW 2.0 stream cipher. SNOW 2.0 was proposed by P. Ekdahl and T. Johansson in 2002 as a strengthened version of its earlier version SNOW 1.0, which was shown to be vulnerabile against a distinguishing attack using linear cryptanalysis by D. Coppersmith et al., in 2001. SNOW 2.0 can be considered as one of the most interesting new stream ciphers. Its importance is emphasized by the fact that it is used for performance benchmarking the eSTREAM project of the EU Network of Excellence ECRYPT. SNOW 2.0 has also been taken as a starting point for the ETSI project on a design of a new UMTS encryption algorithm.

Distinguishing attacks using linear cryptanalysis (linear masking) were previously applied to SNOW 2.0 by Watanabe et al. The main part of such attack is to search for efficient linear maskings. The group extended the previous searches on linear maskings. However, the main contribution of the 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. The results will appear in the proceedings of the 13th International Workshop on Fast Software Encryption (FSE 2006).

A second important class of cryptanalytic methods on stream ciphers is algebraic cryptanalysis. Resistance of a cipher component against algebraic attacks is measured by a quantity called *algebraic immunity* which is the lowest degree a system of equation describing the component can have. Lasse Kiviluoto implemented the algorithm to computing the algebraic immunity for an S-box. This algorithm was used to evaluate the algebraic immunity of a number of modifications of SNOW 2.0, and reported in an internal report by Emilia Käsper.

Security bounds for symmetric primitives

Johan Wallén

The goal of this project is to investigate provable security of block cipher modes of operation. A mode of operation for block ciphers is a method for turning a block cipher into an encryption scheme that accepts arbitrary length inputs. A security proof for a mode of operation consists of two parts. First, the security model is defined, that is, exact definitions of what it means for an encryption function and a block cipher to be secure are given. The second part consists of the reduction, that is, a transformation is given, which turns any attack that violates the security definition of the encryption scheme into an attack that violates the security definition of the block cipher. A result of the project is a concrete security proof of the cipher feedback (CFB) mode of operation in standard attack models. The proof is accompanied by a matching generic attack. The results have been submitted for publication.

Concrete cryptographic security

Sven Laur, Helger Lipmaa, and Kaisa Nyberg

The main goal of this group is to design and implement cryptographically secure algorithms for privacy-preserving data-mining. One can divide our research activities into two main areas: concrete applications and design of efficient cryptographic primitives.

Data-mining algorithms are usually quite resource demanding and therefore direct application of well known generic cryptographic techniques leads to algorithms that are intractable in practice. Moreover, these two- and multiparty solutions are based on a rather pessimistic assumption that all participants can deviate from the protocol specification. In practice, service providers are often forced to act honestly or otherwise their reputation is compromised. In [42], we studied a relaxed security notion where a service provider is honest but curious and clients can act maliciously.

We developed an efficient generic transformation that provides desired security for all participants, if the protocol is based on homomorphic encryption. More precisely, we devised a novel extension of homomorphic oblivious transfer that can be used together with any homomorphic encryption scheme. Moreover, related techniques allow to implement other cryptographic primitives, e.g. conditional oblivious transfer and solution to millionaire problem.

The second and a more practical publication [30] explores a well known private support counting problem (PISC). Shortly put, a service provider has a private database of patterns and a client wants to retrieve privately the number of occurrences of a certain pattern. An efficient solution to PISC has a wide applicability as many data-mining algorithms use support counting as a subroutine. We presented three different solutions. However, they all have communication linear in the database size that is rather unsatisfactory. Therefore, we showed that finding an efficient PISC protocol with a sublinear communication is highly unlikely, as such protocol gives a rise to a oblivious transfer protocol with similar communication.

The last publication [41], considers a concrete problem that has surfaced in many wireless technologies. Security of wireless network must be based on cryptographic solutions, as it is relatively easy to eavesdrop and spoof wireless communication. Therefore, we need efficient, secure and user-friendly key exchange protocols. If key exchange fails, the security of any wireless network becomes illusory, since malicious parties can mount man-in-the middle attacks. In all such key exchange protocols users have to compare relatively short strings displayed by electronic devices and consequently the deception probability is always non-negligible. In [41], we presented a user-friendly but cryptographically secure protocol that achieves near-optimal security guarantee under standard cryptographic assumptions.

4.7 Generative string rewriting

Eero Lassila

What does one want from a generative string rewriting process? If we were mainly concerned of easy analyzability of the rewriting result, we would be wise to stick to formal language theory and to context-free Chomsky grammars in particular. But here we are not at all interested in such analyzability (which would benefit us only after the generation and only if we for some reason had to parse the output). In contrast, we want to boost the generative process itself: for optimization, we want unbounded context-sensitivity, and for speed, we want optional parallelism. On the other hand, we must take care that our process always remains semantics-preserving. (So while context-free Chomsky grammars closely relate to the front end of a programming language compiler, our work relates to the back end.)

Both synchronously and asynchronously parallel rewriting, in addition to sequential rewriting, should be dealt with. Each of these three rewriting types moreover has several subtypes: for instance, sequential rewriting embraces both Chomsky grammars and macro processors, while Lindenmayer systems constitute a prominent example of synchronous parallelism. We have devised a simple unifying formal framework that tries to capture the three types and their subtypes.

Our goal is to formulate a fairly wide variety of such constraints that if the rewriting rule base as a whole meets one of the constraints, the degree of parallelism in the rewriting process may be selected freely as long as the limits implied by the particular constraint are not exceeded. Adjusting this selection often changes the structure but never the semantics of the output.

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 2005. The conferences are ordered chronologically.

January

VMCAI 2005: Sixth International Conference on Verification, Model Checking and Abstract Interpretation, Paris, France, 17 to 19 January. Participants: Timo Latvala and Keijo Heljanko.

February

Estonian Theory Days, Koke, Estonia, 4 to 6 February. Programme committee member and session chair: Helger Lipmaa.

IASTED International Conference on Artificial Intelligence and Applications (AIA2005), Innsbruck, Austria, 12 to 15 February. Keynote speaker: Ilkka Niemelä.

European Grid Conference 2005, Amsterdam, Holland, 13 to 17 February. Participant: Hyvärinen Antti.

FSE 2005, Fast Software Encryption 2005, Paris,France, 21 to 23 February. Participants: Kaisa Nyberg, Helger Lipmaa, Johan Wallén. Programme committee member and session chair: Kaisa Nyberg.

22nd Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, 24 to 26 February. Participant: Keijo Heljanko.

Connectathon 2005, San Jose, USA, 24 February to 4 March. Participants:Ville Nuorvala and Antti Tuominen.

EWSCS, 10th Estonian Winter School in Computer Science, Palmse Es-

tonia, 27 February to 4 March. Participants: Helger Lipmaa and Johan Wallén. Programme committee member: Helger Lipmaa.
9th International Financial Cryptography and Data Security Conference, Roseau, Dominica, 28 February to 3 March. Programme committee member: Helger Lipmaa.

March

WSEAS International Conference on Automation and Information, Buenos Aires, Argentina, 1 to 3 March. Participants: Catharina Candolin and Janne Lundberg
WCC 2005 International Workshop on Coding and Cryptography, Bergen, Norway, 14 to 18 March. Programme committee member: Kaisa Nyberg.
1th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR-11), Montevideo, Uruguay, 14 to 18 March. Programme committee member: Ilkka Niemelä.

April

ALCOMA 05, Algebraic Combinatorics and Applications, Thurnau, Germany, 3 to 10 April. Presentation: "Nonexistence of Perfect Steiner Triple", Petteri Kaski.
Seminar Nonmonotonic Reasoning, Answer Set Programming and Constraints, Schloss Dagstuhl,Wadern,Germany, 24 to 29 April. Participants: Ilkka Niemelä, Tomi Janhunen, Emilia Oikarinen and Tommi Syrjänen. Programme committee chairman: Ilkka Niemelä. Session chair: Tomi Janhunen and Ilkka Niemelä. Invited presentation: "Translating Normal Logic Programs into Propositional Theories", Tomi Janhunen.

May

ADHOC 2005 Wireless Ad-hoc Networks, Stockholm, Sweden, 3 to 4 May. Poster: "Cooperation in clustered ad hoc networks", Maarit Hietalahti.
WEA 2005: 4th International Workshop on Efficient and Experimental Algorithms, Santorini Island, Greece, 10 to 13 May. Participant: Pekka Orponen.
PAKDD-05, The Ninth Pacific-Asia Conference on Knowledge Discovery and Data Mining, Hanoi, Vietnam, 18 to 20 May. Participant: Satu Elisa Schaeffer.
Eurocrypt 2005, Aarhus,Denmark, 22 to 26 May. Participants: Kaisa Nyberg, Emilia Käsper, Sven Laur and Johan Wallén. Programme committee member and session chair: Kaisa Nyberg.
Workshop on the Petri Net Markup Language 2005(PNML 05)-Towards an ISO/IEC Standard Transfer Syntax for Petri Nets, Espoo, Finland, 26 May. Programme committee members: Nisse Husberg and Kimmo Varpaaniemi. Organizing committee chairman: Kimmo Varpaaniemi. Organizing committee member: Nisse Husberg. Session chair: Kimmo Varpaaniemi.

Symmetric Key Encryption Workshop, Aarhus,Denmark, 26 to 27 May. Participants: Kaisa Nyberg, Emilia Käsper, Sven Laur and Johan Wallén.

June

Commercial Information Technology for Military Operations Workshop (CITMO 2005), Plovdiv Bulgaria, 15 to 17 June. Participant: Catharina Candolin. Invited presentation: "Securing the decision making process in counter terrorist operations", Catharina Candolin.

8th International Conference on Theory and Applications of Satisfiability Testing, St. Andrews, Scotland, 19 to 23 June. Participant: Pekka Orponen. Programme committee member: Ilkka Niemelä.

July

ICCL Summer School 2005 Logic-based Knowledge Representation, Dresden, Germany, 2 to 17 July. Participant: Emilia Oikarinen.

Western European Workshop on Research in Cryptology, Leuven, Belgium, 5 to 7 July. Programme committee member: Kaisa Nyberg.

17th International Conference on Computer Aided Verification (CAV 2005), Edinburgh, England, 7 to 12 July. Participants: Keijo Heljanko, Tommi Junttila, Timo Latvala and Jori Dubrovin.

4th European Conference on Information Warfare and Security, University of Glamorgan, England, 11 to 12 July. Programme committee member and session chair: Catharina Candolin.

20th International Conference on Automated Deduction, Tallinn, Estonia, 22 to 27 July. Programme committee member: Ilkka Niemelä.

Answer Set Programming: Advances in Theory and Implementation (ASP 05), Bath, England. 27 to 29 July. Participants: Tomi Janhunen and Ilkka Niemelä. Programme committee member: Tomi Janhunen and Ilkka Niemelä.

Formal Equivalence Verification Workshop, Madonna di Campliglio, Italy, 27 July to 1 August. Participant: Tommi Junttila.

August

Nineteenth International Joint Conference on Artificial Intelligence (IJCAI05), Edinburgh, England, 30 July to 5 August. Participant: Ilkka Niemelä.

Third Workshop on Model Checking and Artificial Intelligence (MoChArt'05), San Francisco, United States. Programme committee member: Ilkka Niemelä.

6th Max-Planck Advanced Course on the Foundations of Computer Science, Saarbrücken, Germany. 29 August to 2 September. Participant: Harri Haanpää.

September

WiSe 2005, ACM Workshop on Wireless Security, Cologne, Germany, 2 September. Programme committee member: Kaisa Nyberg.

LPNMR 2005, Logic Programming and Nonmonotonic Reasoning, Diamante, Italy, 5 to 8 September. Participants: Ilkka Niemelä, Tomi Janhunen and Emilia Oikarinen. Programme committee member and session chair: Ilkka Niemelä.

1st International Summer School on Constraint Programming, Acquafredda di Marate, Italy, 10 to 16 September. Participant: Matti Järvisalo.

28th German Conference on Artificial Intelligence (KI 2005), Koblenz, Germany, 11 to 14 September. Programme committee member: Ilkka Niemelä.

International Conference on Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX 2005), Koblenz, Germany, 11 to 14 September. Programme committee member: Ilkka Niemelä.

5th International School on Foundations of Security Analysis and Design, Bertinoro University, Bertinoro, Italy, 18 to 24 September. Participant: Mikko Särelä.

Smi's 7th Annual Conference on Military Data Fusion, London, UK, 28 to 29 September. Invited presentation: Catharina Candolin.

October

CP 2005 Eleventh International Conference on Principles and Practice of Constraint Programming and ICLP 2005 Twenty First International Conference on Logic Programming, Barcelona, Spain, 1 to 5 October. Programme committee member and session chair: Ilkka Niemelä.

NCW-Seminar, Buenos Aires, Argentina, 3 to 8 October. Participant: Catharina Candolin.

SINPRODE 2005, Buenos Aires, Argentina, 5 to 10 December. Invited presentation: Catharina Candolin.

ICTAC 2005 – International Colloquium on Theoretical Aspects of Computing, Hanoi, Vietnam, 17 to 21 October. Participant: Misa Keinänen.

ETSI IP6 Plugtests, Sophia Antipolis, France, 17 to 21 October. Participants: Antti Tuominen and Ville Nuorvala.

Nordsec 2005 - The 10th Nordic Workshop on Secure IT-systems, Tartu, Estonia, 20 to 21 October. Participants: Catharina Candolin and Johan Wallén.

ReflekTori 2005 – Tekniikan opetuksen symposium, TKK Dipoli, Espoo, 20 to 21 October. Participant and workshop organizer: Matti Järvisalo. Participant: Emilia Oikarinen.

Seminar on Deduction Applications, Dagstuhl, Germany, 23 to 28 October. Participant: Ilkka Niemelä.

Sixth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, Aarhus, Denmark, 24 to 26 October. Programme committee member: Kimmo Varpaaniemi.

7th Estonian Computer Science Theory Days, Viinistu, Estonia, 28 to 30 October. Participant: Emilia Käsper.

November

5th Annual Finnish/Baltic Sea Conference on Computer Science Education, Joensuu, 17 to 20 November. Participant: Matti Järvisalo.
6th Australian IWAR Conference, Deakin University, Geelong, Victoria, 24 to 25 November. Participant: Catharina Candolin.
IFM 2005 Fifth Intenational Conference on Intergrated Formal Methods, Eindhoven, The Netherlands, 29 November to 2 December. Participant: Toni Jussila.

December

ICICS 2005 Seventh International Conference on Information and Communication Security, Beijing, China, 10 to 13 December. Participant: Sven Laur.

5.2 Visits

January

Henrik Petander worked at National ICT Australia (NICTA) from October 2004 to May 2005.
Helger Lipmaa visited Institute for Infocomm Research, Singapore, from 16 to 30 January.

February

Helger Lipmaa visited Indiana University at Bloomington, USA, from 12 to 17 February and gave an invited talk.
Keijo Heljanko visited University of Stuttgart, Institute of Formal Methods in Computer Science, Germany, from 16 to 27 February.
Satu Elisa Schaeffer visited Universidad de Chile, Santiago, Chile, from 28 February to 16 December, to work on her doctoral thesis.

March

Catharina Candolin and Janne Lundberg visited Talcan University, Santiago, Chile, from 5 to 11 March.
Catharina Candolin visited University of Newcastle and University of Edinburg, England, from 30 March to 3 April.

May

Maarit Hietalahti visited University of Karlstad, Sweden, from 4 to 6 May.

June

Kaisa Nyberg visited France Telecom Research and Development, 4 days.

July

Tomi Janhunen visited University of Potsdam and met Prof. Schaub's research group, Potsdam, Germany, from 6 to 14 July.
Catharina Candolin visited US Army Research Laboratory in London, UK, on 12 July.

October

Catharina Candolin visited Air Force Base in Buenos Aires, Argentina, from 8 to 12 October.
Tomi Janhunen visited Vienna University of Technology and met Thomas Eiter's research group, from 22 to 28 October.

November

Catharina Candolin gave invited talk in Naval Research Lab, Office of Secretary of Defence, George Mason University in Washington and Space and Navel Warfare Center, San Diego State University, from 12 to 21 November.
Mikko Särelä presented project research results at Ericsson Kista Center, Stockholm, Sweden, on 17 November.
Ilkka Niemelä visited National ICT Australia (NICTA). Australia's Information and Communications Technology centre of excellence from 29 November 2005 to 21 January 2006.

December

Mikko Särelä visited University of California, San Diego, CALIT2 Institute, to work in WIISARD project from 4 December 2005 to 31 July 2006.
Harri Haanpää visited Tallinn Tehnikaülikool to act as the official opponent for Tarmo Veskioja, from 9 to 10 December.

5.3 Guests

In this section the various academic visits to the Laboratory for Theoretical Computer Science in 2005 are summarized. The host is given at the end of each entry.

January

Alkassar Ammar, M.Sc., Sirrix AG and University of Saarland, Estonia, 6 days, research. January, Lipmaa.

March

Michael Kaminski, Prof., Computer Science Department, Germany, 1 day, research. 15 March, Niemelä.
Gerd Brewka, Prof., Universität Leipzig, Germany, 3 days, research. 15 to 18 March, Niemelä.

Torsten Schaub, Prof., Universität Potsdam, Germany, 3 days, research. 15 to 18 March, Niemelä.
Martin Gebser, Dipl.-Inf., Universität Potsdam, Germany, 5 days, research. 14 to 18 March, Niemelä.
Jean Gressman, Dipl.-Inf., Universität Potsdam, Germany, 5 days, research. 14 to 18 March, Niemelä.

April

Krishnamurthy Supriya, Swedish Institute of Computer Science, Sweden, 2 days, research. 22 to 24 April, Orponen.

June

Gunnar Brinckmann, Prof. Universiteit Gent, Belgium, 3 days, opponent for Petteri Kaski. 14 to 17 June, Orponen.

August

Kim Larsen, 3 days, opponent for Timo Latvala. 11 to 14 August, Husberg.

September

Nitesh Saxena, Nokia NCR, Helsinki, gave TCS-forum talk. 16 September, Nyberg.

October

Marc Denecker, Assoc. Prof., Department of Computer Science, Katholieke Universiteit Leuven, Belgium, 7 days. 17 to 23 October, Niemelä.
Maarten Mariën, M.Sc., Department of Computer Science, Katholieke Universiteit Leuven, Belgium, 7 days. 17 to 23 October, Niemelä.
Gene Tsudik, Prof., Computer Science Department, University of California, Irvine, USA, 7 days. 17 to 23 October 2005, Nyberg.

November

Tadao Saito, Prof., Chuo University, Japan gave an invited presentation "Reformation of Telecommunication Network and Teletraffic". 1 November, Kari.
Armin Biere, Prof., Johannes Kepler University, Austria, 3 days, opponent for Toni Jussila. 16 to 19 November, Niemelä.

December

Jyrki Kivinen, Prof, Department of Computer Science, University of Helsinki, opponent of Antti Autere. 16 December, Orponen.
Matthew Warren, Prof., Deakin University, Australia 3 days, opponent for Catharina Candolin. 18 to 21 December, Kari.

6 SCIENTIFIC EXPERT TASKS

This section summarizes the scientific expert tasks carried out by the personnel of Laboratory for Theoretical Computer Science in 2005. 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, from 2005, Finnish delegate on behalf of National Emergency Service Agency at EU CI2RCO project dealing with Critical Information Infrastructure Research Co-ordination; from 2005 to 2008, chairman of the board of Institute for Digital Communications (IDC) at TKK; from 2005, professor member of the Master's programmes "Master's Programme in Mobile Computing – Services and Security" and "Nordic International Master's Programme in Security and Mobile Computing"

Ilkka Niemelä, member of the Executive Committee of the Association for Logic Programming; Steering Committee Member of the International Workshops on Nonmonotonic Reasoning; Steering Committee Member of the International Conferences on Logic Programming and Nonmonotonic Reasoning.

Kaisa Nyberg, member of the board of Finnish Mathematical Society.

6.2 Memberships in editorial boards

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.

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

6.3 Scientific expert duties

Harri Haanpää, official opponent at a doctoral defence, Tallinn Tehnikaülikool, Estonia.

Hannu H. Kari, evaluation of two candidates for professor position on area of "tietojärjestelmät, erityisesti tietoturva (computer systems, especially security)" (position number 2777) at University of Oulu, Finland.

Ilkka Niemelä, statement concerning filling a professor position, University of Cyprus, Associate Professorship in Computer Science, Cyprus; statement concerning filling a professor position, Texas Tech University, Horn Professorship, United States.

Kaisa Nyberg, statement concerning filling a professor position, Memorial University of Newfoundland, Faculty of Engineering and Applied Science, Canada.

7 PUBLICATIONS

7.1 Journal Articles

[1] Patrik Floréen, Petteri Kaski, Jukka Kohonen, and Pekka Orponen. Exact and approximate balanced data gathering in energy-constrained sensor networks. *Theoretical Computer Science*, 344(1):30–46, November 2005.

[2] Patrik Floréen, Petteri Kaski, Jukka Kohonen, and Pekka Orponen. Lifetime maximization for multicasting in energy-constrained wireless networks. *IEEE Journal on Selected Areas in Communications*, 23(1):117–126, January 2005.

[3] Evan Griffiths and Pekka Orponen. Optimization, block designs and No Free Lunch theorems. *Information Processing Letters*, 94(2):55–61, April 2005.

[4] Harri Haanpää. No 17-player triplewhist tournament has nontrivial automorphisms. *Journal of Combinatorial Designs*, 13:345–348, 2005.

[5] Harri Haanpää and Petteri Kaski. The near resolvable 2-(13, 4, 3) designs and thirteen-player whist tournaments. *Designs, Codes and Cryptography*, 35(3):271–285, June 2005.

[6] Matti Järvisalo, Tommi Junttila, and Ilkka Niemelä. Unrestricted vs restricted cut in a tableau method for Boolean circuits. *Annals of Mathematics and Artificial Intelligence*, 44(4):373–399, 2005.

[7] Toni Jussila, Keijo Heljanko, and Ilkka Niemelä. BMC via on-the-fly determinization. *International Journal on Software Tools for Technology Transfer*, 7(2):89 – 101, 2005.

[8] Petteri Kaski. Isomorph-free exhaustive generation of designs with prescribed groups of automorphisms. *SIAM Journal on Discrete Mathematics*, 19(3):664–690, 2005.

[9] Petteri Kaski and Patric R. J. Östergård. One-factorizations of regular graphs of order 12. *Electronic Journal of Combinatorics*, 12:R2, 2005.

[10] Janne Lundberg, Catharina Candolin, and Hannu H. Kari. Multicast source authentication for limited devices. *WSEAS Transactions on Computers*, 4(4), 2005.

[11] Sakari Seitz, Mikko Alava, and Pekka Orponen. Focused local search for random 3-satisfiability. *Journal of Statistical Mechanics: Theory and Experiment*, P06006:1–27, June 2005.

[12] Kimmo Varpaaniemi. On stubborn sets in the verification of linear time temporal properties. *Formal Methods in System Design*, 26(1):45–67, January 2005. © 2005 Springer Science + Business Media, Inc. (Norwell, MA, USA; Dordrecht, The Netherlands; Berlin, Germany).

7.2 Conference Papers

[13] N. Asokan, Valtteri Niemi, and Kaisa Nyberg. Man-in-the-middle in tunnelled authentication protocols. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols: 11th International Workshop*, number 3364 in LNCS, pages 28–41. Springer, Cambridge, UK, 2005.

[14] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Silvio Ranise, Peter van Rossum, and Roberto Sebastiani. Efficient satisfiability modulo theories via delayed theory combination. In Kousha Etessami and Sriram K. Rajamani, editors, *CAV 2005*, volume 3576 of *Lecture Notes in Computer Science*, pages 335–349. Springer, 2005.

[15] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Peter van Rossum, Stephan Schulz, and Roberto Sebastiani. An incremental and layered procedure for the satisfiability of linear arithmetic logic. In Nicolas Halbwachs and Lenore D. Zuck, editors, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2005)*, volume 3440 of *Lecture Notes in Computer Science*, pages 317–333. Springer, 2005.

[16] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Peter van Rossum, Stephan Schulz, and Roberto Sebastiani. The MathSAT 3 system. In Robert Nieuwenhuis, editor, *Automated Deduction – CADE-20*, volume 3632 of *Lecture Notes in Artificial Intelligence*, pages 315–321. Springer, 2005.

[17] Gerd Brewka, Ilkka Niemelä, and Mirosław Truszczyński. Prioritized component systems. In *Proceedings of the Twentieth National Conference on Artificial Intelligence*, pages 596–601. AAAI Press, July 2005.

[18] Catharina Candolin. Ensuring decision making during information operations. In *Proceedings of the 4th European Conference on Information Warfare (ECIW'05)*, University of Glamorgan, Wales, UK, July 2005.

[19] Catharina Candolin. Securing the infrastructure in information operations. In Bill Hutchinson, editor, *Proceedings of the 4th European Conference on Information Warfare and Security*, 2005.

[20] Catharina Candolin, Janne Lundberg, and Hannu Kari. Packet level authentication in military networks. In *Proceedings of the 6th Australian Information Warfare & IT Security Conference*, Geelong, Australia, November 2005.

[21] Bart Goethals, Sven Laur, Helger Lipmaa, and Taneli Mielikäinen. On private scalar product computation for privacy-preserving data. In Choonsik Park and Seongtaek Chee, editors, *The 7th Annual International Conference on Information Security and Cryptology (ICISC 2004)*, pages 366–381, Seoul, South-Korea, 2005. Springer.

[22] Jean Gressmann, Tomi Janhunen, Robert Mercer, Torsten Schaub, Sven Thiele, and Richard Tichy. Platypus: A platform for distributed answer set solving. In Chitta Baral, Gianluigi Greco, Nicola Leone, and Giorgio Terracina, editors, *Proceedings of the 8th International Conference on Logic Programming and Nonmonotonic Reasoning*, pages 227–239, Diamante, Italy, September 2005. Springer-Verlag.

[23] Keijo Heljanko, Tommi Junttila, and Timo Latvala. Incremental and complete bounded model checking for full PLTL. In Kousha Etessami and Sriram K. Rajamani, editors, *Proceedings of the 17th International Conference on Computer Aided Verification (CAV'2005)*, volume 3576 of *Lecture Notes in Computer Science*, pages 98–111, Edinburgh, Scotland, United Kingdom, July 2005. Springer-Verlag.

[24] Keijo Heljanko and Alin Ştefănescu. Complexity results for checking distributed implementability. In Jörg Desel and Yosinori Watanabe, editors, *Proceedings of the 5th International Conference on Application of Concurrency to System Design (ACSD'2005)*, pages 78–87, St Malo, France, June 2005. IEEE Computer Society.

[25] Maarit Hietalahti. Cooperation in clustered ad hoc networks. In *Proceedings of the 5th Scandinavian Workshop on Wireless Ad-hoc Networks Adhoc'05*, Stockholm, Sweden, May 2005.

[26] Petteri Kaski. Nonexistence of perfect Steiner triple systems of orders 19 and 21. *Bayreuther Mathematische Schriften*, 74:130–135, 2005. Proceedings of ALCOMA05, April 3–10, Thurnau, Germany.

[27] Misa Keinänen. Obtaining memory efficient solutions to boolean equation systems. In *Electronic Notes in Theoretical Computer Science*, volume 133, pages 175–191. Elsevier, May 2005.

[28] Misa Keinänen and Ilkka Niemelä. Solving alternating boolean equation systems in answer set programming. In U. Geske D. Seipel, M. Hanus and O. Bartenstein, editors, *Applications of Declarative Programming and Knowledge Management*, volume 3392 of *Lecture Notes in Computer Science*, pages 134–148. Springer-Verlag, 2005.

[29] Timo Latvala, Armin Biere, Keijo Heljanko, and Tommi Junttila. Simple is better: Efficient bounded model checking for past LTL. In Radhia Cousot, editor, *Verification, Model Checking and Abstract Interpretation 2005, 6th International Conference VMCAI'05, Paris, France*, volume 3385 of *Lecture Notes in Computer Science*, pages 380–395. Springer, January 2005.

[30] Sven Laur, Helger Lipmaa, and Taneli Mielikäinen. Private itemset support counting. In Sihan Qing, Wenbo Mao, Javier Lopez, and Guilin Wang, editors, *Information and Communications Security, 7th International Conference, ICICS 2005, Beijing, China, Proceedings*, volume 3783 of *Lecture Notes in Computer Science*, pages 97–111. Springer, 2005.

[31] Janne Lundberg, Catharina Candolin, and Hannu Kari. Multicast source authentication for limited devices. In *Proceedings of International Conference on Automation and Information (ICAI'05)*, Buenos Aires, Argentina, March 2005.

[32] Ilkka Niemelä. Answer set programming: an approach to declarative problem solving. In M. H. Hamza, editor, *Proceedings of the IASTED International Conference on Artificial Intelligence and Applications*, Innsbruck, Austria, 2005.

[33] Kaisa Nyberg. IKE in ad-hoc IP networking. In *Security in Ad-hoc and Sensor Networks*, pages 139–151. Springer, Heidelberg, Germany, 2005.

[34] Emilia Oikarinen. Translating parallel circumscription into disjunctive logic programming. In *ICCL Summer School Student Workshop 2005*, Dresden, Germany, July 2005. TU Dresden.

[35] Emilia Oikarinen and Tomi Janhunen. CIRC2DLP — translating circumscription into disjunctive logic programming. In Chitta Baral, Gianluigi Grego, Nicola Leone, and Giorgio Terracina, editors, *Logic Programming and Nonmonotonic Reasoning, Proceedings of the 8th International Conference on Logic Programming and Nonmonotonic Reasoning*, volume 3662 of *Lecture Notes in Artificial Intelligence*, pages 405–409, Diamante, Italy, September 2005. Springer-Verlag. System Description.

[36] Pekka Orponen and Satu Elisa Schaeffer. Local clustering of large graphs by approximate Fiedler vectors. In S. Nikoletseas, editor, *Proceedings of the 4th International Workshop on Efficient and Experimental Algorithms (WEA'05, Santorini, Greece, May 2005)*, volume 3503 of *Lecture Notes in Computer Science*, pages 524–533, Berlin Heidelberg, 2005. Springer-Verlag.

[37] Markku-Juhani O. Saarinen. Encrypted watermarks and Linux laptop security. In *Workshop on Information Security Applications (WISA 2004)*, pages 30–41, Jeju Island, Korea, 2005. Springer.

[38] Satu Elisa Schaeffer. Stochastic local clustering for massive graphs. In T. B. Ho, D. Cheung, and H. Liu, editors, *Proceedings of the Ninth Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD-05)*, volume 3518 of *Lecture Notes in Computer Science*, pages 354–360, Berlin/Heidelberg, Germany, 2005. Springer-Verlag GmbH.

[39] Sakari Seitz, Mikko Alava, and Pekka Orponen. Threshold behaviour of WalkSAT and focused Metropolis search on random 3-satisfiability. In F. Bacchus and T. Walsh, editors, *Proceedings of the 8th International Conference on Theory and Applications of Satisfiability Testing (SAT'05, St. Andrews, Scotland, June 2005)*, volume 3569 of *Lecture Notes in Computer Science*, pages 475–481, Berlin Heidelberg, 2005. Springer-Verlag.

7.3 Reports

[40] Misa Keinänen. Solving boolean equation systems. Research Report A99, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, November 2005.

[41] Sven Laur, N. Asokan, and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings. Cryptology ePrint Archive, Report 2005/424, 2005. `http://eprint.iacr.org/`.

[42] Sven Laur and Helger Lipmaa. Additive conditional disclosure of secrets and applications. Cryptology ePrint Archive, Report 2005/378, 2005. `http://eprint.iacr.org/`.

[43] Jussi Rintanen, Keijo Heljanko, and Ilkka Niemelä. Planning as satisfiability: Parallel plans and algorithms for plan search. Technical Report 216, Institute of Computer Science, University of Freiburg, Freiburg, Germany, 2005.

[44] Jiří Šíma and Satu Elisa Schaeffer. On the NP-completeness of some graph cluster measures. Technical Report cs.CC/0506100, arXiv.org e-Print archive, `http://arxiv.org/`, June 2005.

[45] Heikki Tauriainen. A note on the worst-case memory requirements of generalized nested depth-first search. Research Report A96, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, September 2005.

7.4 Edited proceedings

[46] Gerhard Brewka, Ilkka Niemelä, Torsten Schaub, Miroslaw Truszczynski, and Joost Vennekens, editors. *05171 Abstracts Collection – Nonmonotonic Reasoning, Answer Set Programming and Constraints*, number 05171 in Dagstuhl Seminar Proceedings. Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany, 2005.

7.5 Doctoral Dissertations

[47] Antti Autere. Extensions and applications of the A^* algorithm. Research Report A98, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, November 2005. Doctoral dissertation.

[48] Catharina Candolin. *Securing Military Decision Making in a Network-centric Environment*. Doctoral dissertation, TKK Dissertations 20, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, Espoo, Finland, November 2005.

[49] Toni Jussila. On bounded model checking of asynchronous systems. Research Report A97, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, October 2005. Doctoral dissertation.

[50] Petteri Kaski. Algorithms for classification of combinatorial objects. Research Report A94, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, June 2005. Doctoral dissertation.

[51] Timo Latvala. Automata-theoretic and bounded model checking for linear temporal logic. Research Report A95, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, August 2005. Doctoral dissertation.

7.6 Licentiate's Theses

[52] Misa Keinänen. *Solving Boolean Equation Systems*. Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[53] Janne Lundberg. *A Wireless Multicast Delivery Architecture for Mobile Terminals*. Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

7.7 Master's Theses

[54] Pauli Aho. Extending a generic constraint solver over polymorphic data. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[55] Antti Hyvärinen. SATU: A system for distributed propositional satisfiability checking in computational GRIDs. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[56] Lasse Kiviluoto. Sperner capacity of directed graphs. Master's thesis, Helsinki University of Technology, Department of Electrical and Communications Engineering, 2005.

[57] Tuulia Kullberg. The effect of the access point selection method on reachability between a mobile ad hoc node and a fixed node. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[58] Stefano Marinoni. Performance of wireless ad hoc routing protocols — a simulation study in realistic environments. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[59] Topi Pohjolainen. Model checking a client-server system with a scalable level of concurrency. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[60] Anssi Rajaniemi. Verkkopankin toimintavarmuuden turvaaminen tietoverkon näkökulmasta. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[61] Ville Salmensuu. Feasibility of IPsec as a secure mobility management technology. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

[62] Tommi Vainikainen. Applying graph rewriting to model transformations. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2005.

7.8 Software

[63] Matti Järvisalo. rgen — a SAT benchmark generator, September 2005. Computer program.

[64] Tommi Junttila. NuSMV-2.2.3-CAV2005. Computer program, 2005.

[65] Emilia Oikarinen. CIRC2DLP 1.1 — software for translating parallel circumscription to disjunctive logic programming, 2005. Computer Program.

7.9 Miscellaneous publications

[66] Harri Haanpää, Matti Järvisalo, Petteri Kaski, and Ilkka Niemelä. SAT benchmarks based on 3-regular graphs, May 2005. SAT Competition 2005 benchmark description.

[67] Kimmo Varpaaniemi, editor. *Annual Report for the Year 2004*. Teknillinen korkeakoulu, Tietojenkäsittelyteorian laboratorio (Helsinki University of Technology, Laboratory for Theoretical Computer Science), Espoo, Finland, July 2005.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2005