Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2003
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2003
Espoo 2004 HUT-TCS-Y2003

ANNUAL REPORT FOR THE YEAR 2003

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 2003
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2003
Espoo 2004 HUT-TCS-Y2003

ANNUAL REPORT FOR THE YEAR 2003

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
FIN-02015 HUT, Finland
Tel. +358-9-451 1
Fax. +358-9-451 3369
E-mail: lab@tcs.hut.fi

Printing: Multiprint Oy,
Helsinki 2004

ABSTRACT: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2003.

CONTENTS

1 INTRODUCTION

Laboratory for Theoretical Computer Science is a part of the Department of Computer Science and Engineering at Helsinki University of Technology. It is responsible for teaching of basic theoretical computer science in the degree programme of computer science and engineering. The Master's level and postgraduate education and research in the laboratory focus on five main areas: computational logic, computational complexity, verification, mobility management, and cryptology.

In the year 2003 the Laboratory of Theoretical Computer Science continued its growth. Two new docents, Tomi Janhunen and Kimmo Varpaaniemi, were appointed. The number of personnel increased slightly and more than 50 persons were employed in research or teaching positions during the year. The budget of the laboratory is heavily based on external sources and in 2003 less than 40% of the total incoming funding was provided by the university. The biggest external sources of funding were the National Technology Agency of Finland (TEKES) and industry, Academy of Finland and Helsinki Graduate School in Computer Science and Engineering (HeCSE). The results in research and education also grew. For example, two doctoral theses and five Licentiate's theses were completed and the list of publications includes over 90 items for the year 2003. More detailed information on personnel, education, research, visits, and publications in the laboratory in 2003 can be found in the following sections.

2 PERSONNEL

The personnel of the Laboratory for Theoretical Computer Science in 2003 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

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

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

Orponen, Pekka; D.Phil., Professor, on leave 2003-08-01/2004-07-31 as Senior Scientist (funded by Academy of Finland)

Husberg, Nisse; D.Sc. (Tech.), Professor (pro tem)

Lipmaa, Helger; PhD, Professor (pro tem)

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

2.2 Docents

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

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

Janhunen, Tomi; D.Sc. (Tech.), Docent in Computational Logic, from 2004-04-01

Nyberg, Kaisa; D.Phil., 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, from 2003-09-01

2.3 Staff

Grenman, Teddy; Stud. (Tech.), System administrator, 2003-01-15/2003-03-31

Haanpää, Harri; Lic.Sc. (Tech.), Researcher, until 2003-07-31, Teaching Researcher 2003-08-01/2004-07-31

Heljanko, Keijo; D.Sc. (Tech.), Teaching Researcher, on leave 2003-04-01/2004-03-31

Kangasniemi, Ulla; Secretary

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

Klaus, Katja; Secretary

Kotimäki, Jaakko; Stud. (Tech.), System administrator, from 2003-03-01

Lassila, Eero; Lic.Sc. (Tech.), Laboratory manager, on leave until 2003-12-31

Lintulaakso, Tuomo; Laboratory Manager, until 2003-12-31

Saastamoinen, Taneli; M.Sc., System administrator (in non-military service), 2003-09-15/2004-09-15

Varpaaniemi, Kimmo; D.Sc. (Tech.), Teaching Researcher

2.4 Researchers

Autere, Antti; M.Sc. (Tech.), Researcher, until 2003-07-31

Candolin, Catharina; M.Sc. (Tech.), Researcher

Griffiths, Evan; Ph.D., Researcher, 2003-09-01/2003-12-31

Elkind, Edith; M.Sc., Researcher, 2003-08-01/2003-08-31

Hietalahti, Maarit; M.Sc. (Tech.), Researcher

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

Jussila, Toni; Lic.Sc. (Tech.), Researcher

Kaski, Petteri; Lic.Sc. (Tech.), Researcher

Keinänen, Misa; MA, Researcher

Kodym, Ladislav; M.Sc. (Tech.), Researcher, until 2003-02-22

Latvala, Timo; Lic.Sc. (Tech.), Researcher

Laur, Sven; M.Sc., Research assistant, 2003-01-09/2003-05-31

Lundberg, Janne; M.Sc. (Tech.), Researcher

Mäkelä, Marko; D.Sc. (Tech.), Researcher

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

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

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

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

Virtanen, Satu; Lic.Sc. (Tech.), Researcher

Wallén, Johan; M.Sc. (Tech.), Researcher

2.5 Research Assistants

Aho, Pauli; Stud. (Tech.), Research assistant, 2003-05-19/2003-08-31

Falck, Emil; Stud. (Tech.), Research assistant

Haddad, Wassim; M.Sc., Researcher, 2003-01-13/2003-12-17

Honkola, Jukka; Stud. (Tech.), Research assistant, 2003-06-01/2003-08-31

Järvisalo, Matti; Stud. (Tech.), Research assistant

Lambert, Maxime; B.Sc., Research assistant, 2003-06-02/2003-08-08

Nikkilä, Raimo; Stud. (Tech.), Research assistant, 2003-06-01/2003-08-31

Nuorvala, Ville; Stud. (Tech.), Research assistant

Pyhälä, Tuomo; Stud. (Tech.), Research assistant, until 2003-02-28

Saarinen, Markku-Juhani O.; Stud. (Phil.), Research assistant

Seitz, Sakari; Stud. (Tech.), Research assistant, until 2003-03-31, from 2003-08-11

Silander, Tapio; Stud. (Tech.), Research assistant

Särelä, Mikko; Stud. (Tech.), Research assistant

Tuominen, Antti; Stud. (Tech.), Research assistant

Tykkälä, Tommi; Stud. (Tech.), Research assistant, 2003-06-01/2003-08-31

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

Riihimäki, Vesa; Stud. (Tech.), T–79.165

Tynjälä, Teemu; Lic.Sc. (Tech.), T–79.231, 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.

3.1 Active Courses in 2003

In 2003, the following courses were active, that is, arranged as lectures, seminars, or projects.

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.

T–0.050 Introduction to Postgraduate Studies in Computer Science (1 cr)

spring, Pekka Orponen

This is a broad introductory course on the facilities and research skills required for successful graduate study in Computer Science and Engineering. The course is obligatory for all new postgraduate students (admitted as of 1 Oct 2002 or later) at the Department of Computer Science and Engineering.

T–79.144 Logic in Computer Science: Foundations (2 cr)

autumn, Tomi Janhunen (Jussila, Järvisalo, Oikarinen)

This is an introductory course on logic and its applications in computer science. Subjects covered: propositional logic, predicate logic, induction principle, model and proof theory, semantic/analytic tableaux, resolution, and some examples of applications.

T–79.146 Logic in Computer Science: Special Topics I (2 cr)

spring, Ilkka Niemelä (Tauriainen)

This is an advanced course on logic and its applications in computer science and engineering covering the following topics: modal logics (syntax, semantics, proof theory and computational properties) and applications of temporal logic in concurrent and distributed systems.

T–79.148 Introduction to Theoretical Computer Science (2 cr)

spring, Pekka Orponen (Syrjänen, Latvala, Pyhälä, Särelä)
autumn, Harri Haanpää (Syrjänen, Aho, Latvala, Särelä, Tykkälä)

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

T–79.149 Discrete Structures (2 cr)

autumn, Leo Ojala & Kimmo Varpaaniemi

The course in Autumn 2003 is concerned with cellular automata (theory, applications and current research problems).

T–79.154 Logic in Computer Science: Special Topics II (2 cr)
autumn, Tomi Janhunen (Syrjänen)

Efficient implementation techniques for propositional logic and rule-based reasoning. Current applications.

T–79.157 Formal Description and Verification of Computing Systems (2 cr)
spring, Nisse Husberg

This course is about formal modeling of distributed and parallel systems. The most important use of the formal model is verification of system properties. In spring 2003 the focus is on "unifying Petri Nets" based on a new book with the same title.

T–79.159 Cryptography and Data Security (3 cr)
spring, Helger Lipmaa (Saarinen, Wallén)

This is an introductory course on cryptology and data security. We plan to teach the course according to textbook, and our preliminary plan is to cover the first 12 chapters, and spend the last few lectures for "new and recent" material.

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

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

T–79.165 Graph Theory (3 cr)
spring, Petteri Kaski & Patric Östergård (Riihimäki)

Introduction to graph theory. Trees, planar graphs, directed graphs. Graph coloring. Symmetries and the automorphism group. Fundamental graph algorithms. Applications. A code-share course: S–72.343/T–79.165.

T–79.179 Parallel and Distributed Digital Systems (3 cr)
spring, Marko Mäkelä (Honkola)

Modeling digital systems. Understanding and describing concurrency. Basics of Petri nets and process algebra (CCS). Utilising computer aided methods.

T–79.185 Verification (2 cr)
autumn, Nisse Husberg

This is an advanced course about verification of parallel and distributed systems.

T–79.186 Reactive Systems (2 cr)
spring, Keijo Heljanko (Latvala)

Specification and verification of properties of reactive systems using temporal logic. Basics of computer aided verification methods and algorithms.

T–79.189 Student Project in Theoretical Computer Science (3 cr)
spring & autumn, Professors and Teaching Researchers

Independent student project on a subject from the field of theoretical computer science. The project is usually done individually but can be done in groups of up to three people.

T–79.190 Testing of Concurrent Systems (2 cr)
autumn, cancelled due to illness

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

T–79.192 Special Course in Theoretical Computer Science (2 cr)
autumn, Hannu Kari

In autumn 2003 the course takes the form of an interactive lecture on special issues of military grade wireless ad hoc networks. Some specific topics include: security, reliability, mobility management, routing, level of trust, and context awareness.

T–79.194 Seminar on Theoretical Computer Science (2 cr)
spring, Ilkka Niemelä (Järvisalo)

A seminar on current research topics in theoretical computer scince. The topic in 2003: satisfiability checking methods for propositional logic.

T–79.230 Foundations of Agent-Based Computing (3 cr)
spring, Tomi Janhunen (Särelä)

Structure of software agents. Rational and intelligent agents. Architectures, implementation techniques and applications for agent-based computing.

T–79.231 Parallel and Distributed Digital Systems (3 cr)
autumn, Teemu Tynjälä (Honkola)

Modelling digital systems. Understanding and describing concurrency. Basics of Petri nets and process algebra (CCS). Utilising computer aided methods. This is the English version of T–79.179, which is lectured in Finnish.

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

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

T–79.240 Special Course in Computational Complexity (3 cr)
autumn, Ilkka Niemelä (Järvisalo)

This is an advanced course on computational complexity covering topics such as NP-completeness, randomized algorithms, cryptography, approximation algorithms, parallel algorithms, polynomial hierarchy, PSPACE-completeness.

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

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

T–79.300 Postgraduate Course in Theoretical Computer Science (2–10 cr)
spring, Nisse Husberg
autumn, Pekka Orponen

Spring: The seminar focuses on Modelling and Verification of Petri Nets for Systems Engineering. Applications especially from Telecommunications will also be studied (modelling of dynamical systems, e.g. mobility and protocol verification).

The main literature is a recent book by Girault and Valk: "Petri Nets in Systems Engineering" (Springer 2003) but also conference proceedings and journal articles are used.

Autumn: Stochastic algorithms such as MCMC sampling, simulated annealing and genetic algorithms provide the currently perhaps most powerful general methodology for the approximate handling of computationally demanding tasks. While these techniques are being widely and successfully applied to the solution of everyday practical problems, their theoretical foundations remain a fascinating, little-charted territory disclosing deep connections between computer science, mathematics, and theoretical physics. We take a concentrated look into some of the tools and analyses that have been applied to probe this area in recent years.

T–79.503 Foundations of Cryptology (3 cr)
autumn, Kaisa Nyberg

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

T–79.514 Special Course on Cryptology (2–6 cr)
autumn, Helger Lipmaa

In autumn 2003, the topic of this course is Privacy-Preserving Data Mining.

The goal of data-mining is usually quite opposite to the privacy: different companies are interested in obtaining as much information about you and your friends as possible, to be able to use it later as they need — either by storing everything, or just storing the necessary bits of the data that is necessary to later build up some models on the data. Clearly, people are however not interested in giving away their personal data for free, and thus might object in submitting their data at all.

In privacy-preserving data-mining, one encourages people to submit some data that helps in building up data models without revealing too much information about clients. If done properly, this might result in companies getting more data, and thus in them being able to build more appropriate models. PPDM also looks on other areas of data-mining, that are as important: e.g., on possibilities of running data-mining algorithms (e.g., ID3) on two separate databases, owned by different companies (e.g., the genome databases).

T–79.515 Cryptology: Special Topics (2–6 cr)
spring, Helger Lipmaa

In spring 2003, the topic of this course is Pairing-Based Cryptography. Simply put, pairing is an efficiently computable bilinear mapping. If a pairing exists on some algebraic structure, the Decisional Diffie-Hellman problem on this structure will be easy. In some specific cases (like supersingular elliptic curves) this gives raise to a situation where decisional Diffie-Hellman is easy, but computational Diffie-Hellman is hard. Based on this disparity, cryptographers have lately proposed (literarily) many interesting cryptographic protocols that are considerably more efficient than the their previous counterparts. Due to that, study of pairings has been one of the most active branches of cryptography during the last two or three years. Researchers have proposed efficient identity-based encryption schemes and signature schemes, signature schemes, aggregate signature schemes, three-party key agreement protocols, etc. cryptographic protocols. The seminar is based on Menezes's tutorial slides, and one to three different papers are discussed during every seminar.

4 RESEARCH ACTIVITIES

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). More details on this research is given in Sections 4.1, 4.2, 4.4, 4.5, and 4.6. For more applied research funding has been awarded by non-academic partners. This research is described in Sections 4.3 and 4.7.

4.1 Computational Logic

Research in the area of computational logic has been carried in a project funded by the Academy of Finland titled "Applications of rule-based constraint programming" led by Prof. Ilkka Niemelä. More detailed description of the research is given below.

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 [42,43]. The project has developed an efficient ASP system called `Smodels` which is used in dozens of research groups world wide.

In many applications normal logic program rules lack expressivity to handle cardinalities, weights and optimization. We have extended the basic language to allow specific cardinality and weight constraints. We have developed a formal stable model semantics for cardinality constraint programs with variables and showed how the idea can be generalized to other extensions of the basic ASP semantics. The extended rule language allows the use of logical variables, function symbols and built-in arithmetic. We have also defined a decidable subset of cardinality constraint programs with function symbols and examined its computational complexity. [65, 74].

In many applications preferences need to be expressed. In order to capture preferences as ranked options we have studied a new connective ($\times$) that allows to represent alternative, ranked options for problem solutions in the heads of rules. Expression $A \times B$ intuitively means: if possible A, but if A is not possible, then at least B. The semantics of logic programs with ordered disjunction is based on a preference relation on answer sets. We show that this can be implemented using answer set solvers for normal programs. The implementation is based on a generator which produces candidate answer sets and a tester which checks whether a given candidate is maximally preferred and produces a better candidate if it is not. The complexity of reasoning tasks based on the new connective has also been studied.

We have also investigated the combination of answer set programming and qualitative optimization techniques. Answer set optimization programs (ASO programs) have two parts. The generating program produces answer sets representing possible solutions and the preference program expresses user preferences. It induces a preference relation on the answer sets of the generating program based on the degree to which rules are satisfied. Possible applications of ASO programming have been studied, complexity results obtained and promising implementation techniques developed [13].

Translation-Based Techniques for Knowledge Representation

Tomi Janhunen

In 2003, we have concentrated on developing a new technique to translate normal logic programs into sets of classical clauses. As a consequence, efficient *SAT solvers* can be utilized to compute answer sets for normal logic programs [20, 61]. The translation is based on a novel characterization of stable models in terms of *level numberings*. In contrast to earlier approaches, we establish the following attractive properties: (i) a bijective relationship between stable models and classical models, (ii) each normal logic program has a fixed translation that need not to be augmented later on when classical models are computed, (iii) the time needed to translate a normal logic program given as input is sub-quadratic, i.e. proportional to the length of the program (in symbols) times the number of bits needed to represent the number of atoms appearing in the program.

In [4], we have continued the expressiveness analysis of non-monotonic logics. The objective is to compare two syntactically restricted variants of Reiter's *default logic* (DL), namely *normal* DL (NDL) and *semi-normal* DL (SNDL), with the original DL. Using the existence of a polynomial, faithful, and modular (PFM) translation as a criterion, we establish that SNDL and DL are of equal expressive power, which strictly exceeds that of NDL. This setting remains valid even if we consider *prerequisite-free* fragments of DL, NDL, and SNDL. In total, these results contrast with Imielinski's result, which states that prerequisite-free and semi-normal default theories can be modularly translated into preferential entailment.

Disjunctive Logic Programming

Tomi Janhunen and Ilkka Niemelä

We have continued our earlier work on developing implementation methodology for disjunctive logic programs under the (partial) stable model semantics. The key idea in our approach is to unfold partiality and disjunctions from a logic program using suitable program transformations. This enables us to use an existing implementation of stable models for normal (disjunction-free) programs as the core inference engine. To assess the feasibility of such an architecture we have implemented a system called GnT [86] for computing stable models of disjunctive programs. The performance of the system is surprisingly close to that of DLV which is a state-of-the-art system for disjunctive programs.

Testing the Equivalence of Logic Programs

Tomi Janhunen and Emilia Oikarinen

It is typical in answer set programming (ASP) that a given problem can be formulated in many different ways and the programmer ends up with a series of alternative formulations when optimizing the amount of memory reserved by the program, and/or the running time elapsed on a particular ASP implementation. This gives rise to a meta-level problem of ensuring that the various formulations are equivalent. In 2003, we have concentrated on generalizing our translation-based verification method to the case of disjunctive logic programs [44, 64, 82]. The idea is to trans-

late any two disjunctive programs of interest into a single disjunctive logic program whose answer sets (if such exist) yield counter-examples to the equivalence of the two. We have implemented a translator called DLPEQ [91] that enables the verification of equivalence with the GNT system [86]. Our experiments suggest that the translation-based method is competitive against an explicit cross-check of answer sets. This is especially the case if the programs being verified possess several answer sets and are likely to be nonequivalent. However, if the number of answer sets is low, then the naive cross-checking approach is likely to be faster.

Product Configuration

Ilkka Niemelä

Together with the product data management group at Helsinki University of Technology (Timo Soininen, Juha Tiihonen, Reijo Sulonen) we have been developing general methodology for product configuration. It has turned out that the new types of rules supported by `Smodels` play an important role in representing configuration knowledge in a compact and maintainable form.

The product data management group has developed a configurator prototype based on this methodology using `Smodels` as the inference engine. Four real products from two domains have been modeled and tested. For these products the inference engine turned out to be efficient enough for practical use [54].

Boolean Circuit Satisfiability Checking

Tommi Junttila, Matti Järvisalo, and Ilkka Niemelä

A variety of interesting propositional satisfiability problem (SAT) instances stem from, e.g., such areas as planning, model checking of finite state systems, testing, and hardware verification. Therefore there is a high demand for more efficient SAT checkers. Recognizing the factors that affect the difficulty of SAT checking is crucial if one is to find more efficient methods for the task. Most current state-of-the-art SAT checkers assume that the input formulae are in conjunctive normal form (CNF). However, using CNF makes efficient modeling of an application cumbersome, and additionally often hides information about the structure of the original problem.

Boolean circuits provide a compact and structure-preserving presentation for problems in many domains. A non-clausal generalization of the Davis-Putnam-Logemann-Loveland procedure to Boolean circuits has been developed and implemented by Junttila and Niemelä during recent years. During 2003 the relative proof complexity of variations of this method has been studied. The variations are obtained by restricting the use of the cut (splitting) rule in several natural, locality based ways. The results obtained so far have been accepted for presentation in an international conference and a winter school in early 2004. In addition, Järvisalo's Master's thesis dealing with the subject is due in early 2004.

Bounded Model Checking

Keijo Heljanko, Toni Jussila, and Ilkka Niemelä

Bounded model checking has been recently introduced as a memory efficient way of locating errors in reactive systems. We have continued to work on bounded model checking using both the `BCSat` and the `Smodels` system developed in the laboratory as the underlying NP-solvers.

The work with `BCSat` has concentrated on efficiently using the parallelism present in the model to speed up model checking. We have developed an efficient encoding for 1-safe Petri Nets and another for labeled transition systems (LTSs). The goal is to use the knowledge obtained from this more abstract domain in the analysis of `SPINB` models. The idea is to try to process the model as far as possible in a single step by exploiting both the local structure of a single LTS and the parallelism of the synchronization product. The work has resulted in the development of a competitive non-standard execution models reducing the needed bound [21, 87]. At the moment, it is investigated whether the bound could be reduced further by allowing transitions to be merged to an atomic block.

The work based on `Smodels` has resulted in a new bounded LTL model checking procedure for 1-safe Petri Nets [3]. The use of logic programs with the stable model semantics leads to a compact (first published linear size) encoding of bounded LTL model checking. Furthermore, the inherent concurrency of the system is exploited by the use of so called step semantics, resulting in very competitive performance compared to other bounded model checking tools [3].

Solution Techniques for 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 such systems. We have studied efficient solution techniques for classes of Boolean equation systems. We have devised algorithms for solving conjunctive/disjunctive form Boolean equation systems which may contain alternating fixed points [60]. Also, we have applied answer set programming techniques to solve generic systems of Boolean equations. We have devised a mapping from Boolean equation systems to normal logic programs which allows for determining the solutions by using an answer set programming approach.

Conformance Testing

Keijo Heljanko and Tuomo Pyhälä

In formal conformance testing, a black-box implementation is tested against a specification. The main focus of the research is on-the-fly conformance testing algorithms, where an implementation is tested against a specification by doing test generation from the specification during test execution. An on-the-fly formal conformance testing tool Bomotest 1.5 [92] has been developed in the project. It integrates bounded model checking technology with specification coverage based test selection meth-

ods [50]. Additional information about the approach can be found from the Master's Thesis of Tuomo Pyhälä [83].

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

Heikki Tauriainen

This research has developed the theory of translating future-time propositional linear temporal logic (LTL) into nondeterministic ω-automata via alternating automata by adapting ideas from the theory of generalized nondeterministic automata to alternating automata. A generalized definition for alternating automata provides for heuristics that can be used to optimize the size of alternating automata during translation using special translation rules and language containment tests that exploit the restricted structure of the automata that arise in the translation. The translation construction also reveals a syntactic subclass of LTL, all formulas in which can be translated directly into nondeterministic automata whose size remains linear in the length of the formulas. These results are described in [67, 75]. Additionally, a direct emptiness checking algorithm for generalized nondeterministic Büchi automata has been developed [66].

Symmetries in Verification

Tommi Junttila

The symmetry reduction method is a way to alleviate the combinatorial explosion problem occurring in the state space analysis of concurrent systems. It exploits the symmetries (i.e., automorphisms) of the state space by considering only one representative state from each orbit of states induced by the symmetries. Thus a potentially much smaller set of states has to be considered during the state space analysis. The work is concentrated on the application of the symmetry reduction method to Petri nets and related formalisms.

During the year 2003, the results obtained during the previous years were collected together and published as the doctoral dissertation of Tommi Junttila [71]. In addition, two papers on results concerning the core algorithms needed in the symmetry reduction method, namely the algorithms for the *orbit problem* either comparing whether two states are equivalent under the symmetries or producing a canonical representative for a state, have been submitted.

4.2 Computational Complexity and Combinatorics

Work in the area of computational complexity and combinatorics led by Prof. Pekka Orponen is structured in three research groups, *Computational Models and Mechanics*, *Coding Theory and Optimisation*, and *Distributed Algorithmics*.

Computational Models and Mechanics

Evan Griffiths, Sakari Seitz, Satu Virtanen 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.

S.V.'s Lic.Sc. (Tech.) thesis on the characteristics of nonuniform random graph models [69,77] was accepted with honours by the department council in April 2004. She continued to work with P.O. on efficient online clustering and sampling algorithms for large graphs. S.V. presented some aspects of this work at two workshops and the *First Latin American Web Congress* [56], and it has attracted quite favourable international attention. The methods developed are also applicable to ad hoc clustering of hierarchical networks of mobile devices. S.V.'s joint paper with Doc. Pekka Nikander (Ericsson NomadicLab) on this topic will be presented in 2004.

S.S. and P.O. continued their investigations into the theory and applications of stochastic search methods. Their paper on the surprising efficiency of the so called *Record-to-Record Travel (RRT)* algorithm in finding solutions to random instances of the Satisfiability problem close to its phase transition threshold was presented at a LICS'03 workshop in June [53]. In October, a joint postgraduate course on *Complexity Transitions in Optimisation Problems* was organised together with the Engineering Physics department.

E.G. and P.O. collaborated on trying to understand so called "No Free Lunch" phenomena in optimisation, and discovered a surprising characterisation of NFL landscapes in terms of certain kinds of combinatorial designs. This work will be published in 2004.

In addition, some of E.G.'s old work on recursion theory [1], and P.O.'s work on computational statistics [51] and the computational power of neural network models [8–10] appeared in print in 2003.

In 2000–2003 the CMM group was the coordinating partner in the multidisciplinary consortium *Stochastic Adaptive Dynamics of Complex Systems (STADYCS)* (`http://www.math.utu.fi/MaDaMe/projects/orponen.html`), funded by the Academy of Finland as part of its *Mathematical Methods and Modelling in the Sciences (MaDaMe)* research programme. The other partners in this consortium were the Laboratories of Physics, Mathematics, and Computational Engineering at HUT, the Departments of Mathematics, Economics, and Ecology and Systematics at the University of Helsinki, and the Department of Mathematics at the University of Turku. Following the conclusion of the MaDaMe programme, a more focused Academy-funded project on *Algorithms for Nonuniform Networks (ANNE)* will commence in January 2004.

Coding Theory and Optimisation

Harri Haanpää and Petteri Kaski

The area of research of this group is the study of existence and enumeration problems in coding theory and discrete mathematics using computational methods, and enhancing these by algebraic and combinatorial results. The methods are developed in a general framework, and

have been applied to numerous discrete structures such as codes, designs and graphs. The group works in close collaboration with Prof. Patric Östergård and his group at the Electrical Engineering Department.

In 2003 the emphasis was on classification algorithms. The main focus has been on orderly generation of discrete structures — backtrack search with isomorph rejection. With algorithms of this type, classification results have been obtained for various structures, including Steiner triple systems, near resolvable 2-designs, conference matrices, one-factorizations of regular graphs, whist tournaments, sum and difference coverings 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. During the year 2003, this research contributed to the journal articles [2, 5]. The Licentiate's thesis of Petteri Kaski from 2002 was published as a report [62] in 2003; also, the Doctoral dissertation of Harri Haanpää was submitted for pre-examination.

Distributed Algorithmics

Antti Autere, Emil Falck, Maarit Hietalahti, Petteri Kaski, 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 is done in close collaboration with researchers from the University of Helsinki Department of Computer Science and the HUT Networking Laboratory, as part of the consortium *Networking and Architecture for Proactive Systems (NAPS)* (`http://www.cs.helsinki.fi/u/floreen/naps.html`), funded by the Academy of Finland as part of its *Proactive Computing (PROACT)* research programme. In September 2003 also a new TEKES-funded project on *Security and Mobility in Hierarchical Ad Hoc Networks (SAMOYED)* commenced, by a funding decision made by TEKES retroactively in mid-December.

The NAPS collaboration focused in Autumn 2002 and Spring 2003 on the multicast time maximisation problem in energy constrained ad hoc networks, and a report on this topic was presented at a MobiCom'03 workshop in September [19]. In Autumn 2003, the emphasis of the NAPS work shifted towards energy-efficient and fault-tolerant data gathering techniques in wireless sensor networks. Reports on this work are currently under review for publication in 2004.

Within the SAMOYED project in Autumn 2003, M.H. worked towards her Lic.Sc. (Tech.) thesis on security and trust relations in mobile networks, and M.S. towards his M.Sc. (Tech.) thesis on mobility models. Both theses will be completed in 2004. In addition, the SAMOYED group held biweekly discussion meetings on the literature on hierarchical ad hoc networks, with the goal of producing a comprehensive literature survey on the topic in Spring 2004.

Also in 2003, A.A. completed the first version of his dissertation

manuscript, which is currently under revision. The topic of the work is the theory and applications of the A^* search algorithm, including its use in energy-efficient routing in ad hoc networks.

4.3 Mobility Management

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

CAN: Core Ad Hoc Networks

Catharina Candolin, Hannu H. Kari

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 [18]. 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.

The Mobility/Multicast Subproject of Brocom

Wassim Haddad, Hannu H. Kari, 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 air 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. The most relevant publication from the subproject in the year 2003 is a paper [40], where the current implementation of our caching architecture was described.

GO-CORE — A Mobility Architecture for Heterogeneous Wireless Networks

Hannu H. Kari, Ville Nuorvala, Henrik Petander, Tapio Silander, and Antti Tuominen

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 prices. 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 [90]. The 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.

4.4 Verification

Software Verification

Marko Mäkelä and Timo Latvala

The group applies state space exploration methods to the verification of safety properties in distributed software systems. Our efforts focused on techniques for model checking modular Petri nets. During the year

2003, this research contributed to the conference paper [41], a submitted paper, and Mäkelä's Doctoral Thesis [72].

Analysis of the RLC Protocol

Teemu Tynjälä

The analysis of the RLC (Radio Link Control) protocol (a UMTS radio network layer protocol and an OSI data link layer protocol) had started in the `ANNAMARIA` project and was finalised. Several `MARIA` models of the SDL specification of the protocol were manually constructed. Due to carefully selected abstractions, certain fundamental positive analysis results were eventually obtained and documented in Tynjälä's Licentiate's Thesis [76].

Model Checking Safety Properties

Timo Latvala

We continued studying different techniques for efficient model checking of safety properties. The research resulted in a conference paper [34] and an update version of the SCHECK–software [88].

Formal Model Generation and Analysis of SDL

Annikka Aalto (Yomi Solutions), Nisse Husberg, and Kimmo Varpaaniemi

Petri net based analysis of SDL is an old research topic in the laboratory, and the earliest tools for the purpose were built in the late 1980's. The current research continues the work done in the projects Maria (1998–2000) and Anna-Maria (2001). The main goal is to build a practical collection of methods for alleviating the state space explosion problem. The status of the current research was reported in the 11$^{\text{th}}$ International SDL Forum [12].

Bounded Model Checking on a Railway Traffic Control System

Kimmo Varpaaniemi

In the Maria project (1998–2000), a traffic control system for the railway section between Haapamäki and Seinäjoki was analysed using explicit-state model checking tools. Due to a high degree of nondeterminism in the system, the coverability of explicit-state approaches remained low. So, the analysis of the system was continued after the project, and several symbolic model checking tools were used. The results of that work were reported in the CS&P'2003 Workshop [55].

4.5 Simulation of quantum computers using stochastic Petri nets

Leo Ojala, Olli-Matti Penttinen, and Heikki Rantanen

We have developed a methodology to simulate the time behaviour of quantum computers using stochastic Petri nets. The free evolution of a closed quantum system obeys the Schrödinger differential equation. In the case of Feynman's architecture we will get a set of linear differential first-order equations whose solution gives the free evolution of the computer.

The time aspect of stochastic Petri nets allows us to find a systematic solution procedure [48]. It has been used to study quantum interference in Feynman's computers [45] and in simulation of quantum swap computer [46].

4.6 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.

4.7 Cryptology

Helger Lipmaa, Sven Laur, Markku-Juhani O. Saarinen and Johan Wallén

This group studies the security of different cryptographic primitives and protocols, their efficiency but also applications of cryptology in the real life. H.L. created this relatively new group in 2001, and it was joined by M-J.S. and J.W. in the beginning of 2002 and by S.L. in the beginning of 2003 (for 4 months) and then again in the beginning of 2004. We also had several temporary visitors.

During 2002, our group produced five conference papers in top workshops and conferences [35–37, 52, 57], one M.Sc. thesis [85] (defended under H.L.'s supervision) and several research reports [58, 59, 63, 70].

In particular, we studied the security of symmetric primitives. Research into cryptanalysis of block ciphers based on hash functions cul-

minated in [52], where novel results are presented about SHACAL-1 and other such constructions. This work sheds light into the design principles of the underlying hash functions such as SHA-1; we find that a good hash compression function is not necessarily a good block cipher. The opposite is true by definition.

We continued our research on differential cryptanalysis, proposing a novel methodology to efficiently analyze the strength of modular addition w.r.t. differential cryptanalysis [57, 85]. The conference publication [57] presents very efficient algorithms for studying the linear properties of addition. The Master's thesis [85] and the corresponding technical report [70] develops a new general method for analysing the differential and linear properties of functions based on addition. This method greatly simplifies previous analyses of the differential and linear properties of addition and allows generalisations to more complicated functions.

From the cryptographic protocols side, we designed the most efficient cryptographic Vickrey auction protocol [37], that has a 10–100 times smaller communicational complexity, compared to the predecessors. We proposed a novel methodology for constructing efficient statistical zero-knowledge arguments of knowledge for a relatively large class of languages, based on the classical work done by Matiyasevich and others when tackling Hilbert's 10th problem [35]. Finally, one of the very fundamental primitives in cryptography is oblivious transfer, efficiency of which is the bottleneck in fundamental two-party computation protocols. We proposed the first two-round verifiable oblivious transfer protocol and a related verifiable private equality test protocol [36].

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 2003. The conferences are grouped by person and ordered chronologically. Information concerning possible presentations and other modes of participating in a conference are likely to be incomplete.

Catharina Candolin

IEEE Southeastcon 2003, Ocho Rios, St. Ann, Jamaica. April 2003. Paper.

CITMO workshop, Ronneby, Sweden. April 2003. Session chair.

Eurocrypt 2003, Warsaw, Poland. May 2003.

The 2003 International conference on wireless networks ICWN'03, Las Vegas, United States. June 2003. Paper.

The 2nd European Conference on Information Warfare (ECIW2003), Reading, United Kingdom. June–July 2003. Paper.

The 7th WSEAS International Conference on Communications (ICCON), Corfu, Greece. July 2003.

The 7th Multiconference on Systemics, Cybernetics, and Informatics, Orlando, Florida, United States. July 2003. Paper.

Ottawa Linux Symposium, Ottawa, Canada. July 2003. Paper.

International Symposium on Telecommunications (IST 2003), Isfahan, Iran. August 2003. Paper.

IEEE 9th Asia-Pacific Conference on Communication, Penang, Malaysia. September 2003. Paper.

IEEE MILCOM 2003, Boston, United States. October 2003. Paper.

The 4th Australian Information Warfare and IT Security Conference, Adelaide, Australia. November 2003. Paper.

Australian information security management conference, Perth, Australia. November 2003.

Harri Haanpää

Kolloquium über Kombinatorik, Magdeburg, Germany. November 2003. Presentation.

Nisse Husberg

Program committee meeting of Petri net conference 2003, Eindhoven, Holland. February–March 2003.

Tomi Janhunen

Tietojenkäsittelytieteen päivät, Otaniemi, Finland. May 2003.

Answer Set Programming: Advances in Theory and Implementation (ASP 03), Messina, Italy. September 2003. Paper.

Annual meeting of WASP project, Messina, Italy. September 2003.

Toni Jussila

Computer Aided Verification (CAV) conference, Denver, United States. July 2003.

The First International Workshop on Bounded Model Checking, Boulder, Colorado, United States. July 2003. Paper.

Hannu H. Kari

CITMO-workshop, Ronneby, Sweden. April 2003. Invited presentation, Session chair.

Workshop on Secure IT and Vulnerabilities of Commercial Wireless Components. November 2003. Invited presentation.

Petteri Kaski

DIALM-POMC 2003 Joint Workshop on Foundations of Mobile Computing, San Diego, United States. September 2003.

ACM SIGMOBILE MobiCom, San Diego, United States. September 2003.

Kolloquium über Kombinatorik, Magdeburg, Germany. November 2003. Presentation.

Sven Laur

8th Estonian Winter School in Computer Science, Palmse, Estonia. March 2003.

Timo Latvala

Spin 2003, Portland, United States. May 2003. Paper.

Nordic Workshop on Programming Theory, Turku, Finland. October 2003. Presentation.

Helger Lipmaa

Fast Software Encryption 2003, Lund, Sweden. February 2003. Member of programme committee, session chair.

8th Estonian Winter School in Computer Science, Palmse, Estonia. March 2003. Member of programme committee, session chair.

Eurocrypt 2003, Warsaw, Poland. May 2003.

Estonian Theory Days, Pedase, Estonia. October 2003. Member of programme committee, session chair, presentation.

NordSec Workshop, Gjøvik, Norway. October 2003. Member of programme committee, session chair.

ISICS 2003, Seoul, Korea. November 2003. Paper.

ASIACRYPT 2003, Taipei, Taiwan. November 2003. Paper.

Marko Mäkelä

24th International Conference on the Application and Theory of Petri Nets, Eindhoven, Netherlands. June 2003. Paper.

Ilkka Niemelä

Tietojenkäsittelytieteen päivät, Espoo, Finland. May 2003. Session chair.

CADE-19 Workshop on Model Computation - Principles, Algorithms, Applications, Miami, United States. July 2003. Invited presentation.

19th International Conference on Automated Deduction (CADE-19), Miami, United States. Member of programme committee, session chair. July–August 2003.

Answer Set Programming: Advances in Theory and Implementation, Messina, Italy. September 2003. Session chair.

Annual meeting of WASP project, Messina, Italy. September 2003.

8th Scandinavian Conference on Artificial Intelligence (SCAI'03), Bergen, Norway. November 2003. Invited presentation.

Emilia Oikarinen

Tietojenkäsittelytieteen päivät, Espoo, Finland. May 2003.

Pekka Orponen

Tietojenkäsittelytieteen päivät, Otaniemi, Finland. May 2003.

LICS'03 Workshop on Typical Case Complexity and Phase Transitions, Ottawa, Canada. June 2003. Presentation.

Tuomo Pyhälä

The 3rd International Conference on Application of Concurrency to System Design (ACSD'2003, Guimarães, Portugal. June 2003. Paper.

Markku-Juhani Saarinen

Fast Software Encryption 2003, Lund, Sweden. February 2003. Paper.

8th Estonian Winter School in Computer Science, Palmse, Estonia. March 2003.

Mikko Särelä

The 10th colloquium on Structural Information and Communication Complexity (SIROCCO 2003), Umeå, Sweden. June 2003. International Workshop on Interconnection Networks (IWIN 2003), Umeå, Sweden. June 2003.

Kimmo Varpaaniemi

The 11th SDL Forum, Stuttgart, Germany. July 2003. Paper.

Workshop on Concurrency, Specification and Programming (CS&P'2003), Czarna, Poland. September 2003. Paper.

Satu Virtanen

The Twelfth International World Wide Web Conference / Second Workshop on Algorithms and Models for the Web-Graph, Budapest, Hungary. May 2003. Presentation.

Conference on Growing Networks and Graphs in Statistical Physics, Finance, Biology and Social Systems, Rome, Italy. September 2003.

First Latin American Web Conference, Santiago, Chile. November 2003. Poster, presentation.

Neural Information Processing Systems Conference, Vancouver and Whistler, Canada. December 2003. Poster.

Johan Wallén

Fast Software Encryption 2003, Lund, Sweden. February 2003. Paper.

8th Estonian Winter School in Computer Science, Palmse, Estonia. March 2003. Presentation.

Eurocrypt 2003, Warsaw, Poland. May 2003. Presentation.

5.2 Visits

Candolin: RMIT University, Melbourne, Australia. 4 days. November 2003.

Haddad: Ericsson Research Laboratory, Canada, 5 months.

Heljanko: University of Stuttgart, Institute for Formal Methods in Computer Science, Germany, 12 months, April 2003 to March 2004.

Janhunen: Working Group on Answer Set Programming, Technical University of Potsdam, Germany, 7 days. June 2003.

Keinänen: Centrum voor Wiskunde en Informatica, Amsterdam, Netherlands, 3 months. September to December 2003.

Nuorvala, Petander, and Tuominen: Co-operation with Japanese WIDE project. Adding support for Mobile IPv6 to Linux implementation of IPv6. Japan, 3 weeks. September to October 2003.

Saarinen: Cryptology research group of Katholieke Universiteit Leuven. Participation and lecture in summer course on cryptography. Belgium, 3 weeks. June 2003.

5.3 Guests

Official Opponents of Doctoral Dissertations

Emerson, Allen E.; Professor, Department of Computer Sciences, University of Texas at Austin, United States, 6 days, opponent of Tommi Junttila. October to November 2003.

Kindler, Ekkart; Dr., Universität Paderborn, Germany, 3 days, opponent of Marko Mäkelä. November 2003.

Other Guests

Elkind, Edith; M.Sc., Princeton University, United States, 4 weeks, research. August 2003.

Fischmann, Matthias; M.Sc., Humboldt University, Berlin, Germany, 4 weeks, research. August 2003.

Heinrich-Litan, Laura; Dr., Abteilung für Mathematische Optimierung, Technische Universität Braunschweig, Germany, 5 days, teaching and research. October 2003.

Khomenko, Victor; Dr., University of Newcastle upon Tyne, United Kingdom, 5 days, research. January 2003.

Lambert, Maxime; B.Sc., Rice University, Houston, United States, 2 months, research. June to August 2003.

Laud, Peeter; PhD, University of Tartu, Estonia, 2 days, research. May 2003.

Linke, Thomas; Dr., Potsdam University, Germany, 5 days, research. December 2003.

Rijmen, Vincent; PhD, Katholieke Universiteit Leuven, Belgium, 5 days, teaching. May 2003.

Satoh, Ken; Professor National Institute of Informatics, Foundations of Information Research Division, Japan, 1 day, research. August 2003.

6 PUBLICATIONS

6.1 Journal Articles

[1] E. Griffiths. Limit lemmas and jump inversion in the enumeration degrees. *Archive for Mathematical Logic*, 42(6), 2003.

[2] H. Haanpää and P. R. J. Östergård. Classification of whist tournaments with up to 12 players. *Discrete Appl. Math.*, 129:399–407, 2003.

[3] K. Heljanko and I. Niemelä. Bounded LTL model checking with stable models. *Theory and Practice of Logic Programming*, 3(4&5):519–550, 2003. Also available as (CoRR: arXiv:cs.LO/0305040).

[4] T. Janhunen. Evaluating the effect of semi-normality on the expressiveness of defaults. *Artificial Intelligence*, 144(1–2):233–250, March 2003.

[5] P. Kaski, L. B. Morales, P. R. J. Östergård, D. A. Rosenblueth, and C. Velarde. Classification of resolvable 2-(14,7,12) and 3-(14,7,5) designs. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 47:65–74, 2003.

[6] P. Orponen. Mitä tietojenkäsittelyteoriaan kuuluu? *Tietojenkäsittelytiede*, 19:15–28, 2003.

[7] P. Orponen. Tietotekniikkaa ennen tietokoneita — Alan Turing ja tietotekniikan kiehtovat alkuvaiheet. *Tietoa*, pages 4–6, November 2003.

[8] J. Šíma and P. Orponen. Continuous-time symmetric Hopfield nets are computationally universal. *Neural Computation*, 15(3):693–733, March 2003.

[9] J. Šíma and P. Orponen. Exponential transients in continuous-time Liapunov systems. *Theoretical Computer Science*, 306(1–3):353–372, September 2003.

[10] J. Šíma and P. Orponen. General purpose computation with neural networks: A survey of complexity theoretic results. *Neural Computation*, 15(12):2727–2778, December 2003.

[11] K. Varpaaniemi. Towards ambitious approximation algorithms in stubborn set optimization. *Fundamenta Informaticae (Annales Societatis Mathematicae Polonae, Series IV)*, 54(2–3):279–294, February 2003. IOS Press, Amsterdam.

6.2 Conference Papers

[12] A. Aalto, N. Husberg, and K. Varpaaniemi. Automatic formal model generation and analysis of SDL. In R. Reed and J. Reed, editors, *SDL 2003: System Design, 11th International SDL Forum, Stuttgart, Germany, July 1–4, 2003, Proceedings*, volume 2708 of *Lecture Notes in Computer Science*, pages 285–299. Springer-Verlag, Berlin, 2003. © Springer-Verlag Berlin Heidelberg 2003.

[13] G. Brewka, I. Niemelä, and M. Truszczyński. Answer set optimization. In *Proceedings of the 18th International Joint Conference on*

Artificial Intelligence, pages 867–872. Morgan Kaufmann Publishers, August 2003.

[14] C. Candolin. Privacy issues in network-centric warfare. In *Proceedings of the 4th Australian Information Warfare & IT Security Conference*, Adelaide, Australia, November 2003.

[15] C. Candolin. A study of infrastructure warfare in relation to information warfare, net warfare, and network-centric warfare. In *Proceedings of the 2nd European Conference on Information Warfare (ECIW'03)*, Reading, UK, June 2003.

[16] C. Candolin and H. Kari. Ad hoc network routing based on incomplete trust. In *Proceedings of The 7th Multiconference on Systemics, Cybernetics, and Informatics*, Orlando, Florida, USA, July 2003.

[17] C. Candolin and H. Kari. Distributing incomplete trust in wireless ad hoc networks. In *Proceedings of IEEE Southeastcon 2003*, Ocho Rios, St. Ann, Jamaica, April 2003.

[18] C. Candolin and H. H. Kari. An architecture for context aware management. In *Proceedings of IEEE MILCOM 2003*, Boston, Massachusetts, USA, October 2003.

[19] P. Floréen, P. Kaski, J. Kohonen, and P. Orponen. Multicast time maximization in energy constrained wireless networks. In A. Richa and J. Welch, editors, *Proceedings of the 2003 Joint Workshop on Foundations of Mobile Computing (DIALM-POMC'03, San Diego CA, September 2003)*, pages 50–58, New York NY, 2003. Association for Computing Machinery.

[20] T. Janhunen. A counter-based approach to translating normal logic programs into sets of clauses. In M. de Vos and A. Provetti, editors, *Answer Set Programming: Advances in Theory and Implementation*, pages 166–180, Messina, Sicily, September 2003. CEUR. http://ceur-ws.org/Vol-78/.

[21] T. Jussila, K. Heljanko, and I. Niemelä. BMC via on-the-fly determinization. In *Proceedings of the first International Workshop on Bounded Model Checking*, volume 89 of *ENTCS*, Boulder, Colorado, USA, July 2003. Elsevier.

[22] H. H. Kari. Future of heterogeneous wireless networks. In *TecIT Forum*, Helsinki, Jan. 2003. Kontakti.Net. Electronic publication.

[23] H. H. Kari. Lannistaako langaton LAN? In *Tietotekniikan ammattilaiset 2003*, Helsinki, Apr. 2003. Tietotekniikan liitto. Electronic publication.

[24] H. H. Kari. Liikkuvan käyttäjän tietoturva. In *Tietoturvatapahtuma 2003*, Helsinki, Feb. 2003. Communications Security, Stonesoft, F-Secure. Electronic publication.

[25] H. H. Kari. Military-grade wireless ad hoc -networks. In *Seminar on wireless networks*, Stockholm, Sweden, May 2003. Kungliga Tekniska Högskolan.

[26] H. H. Kari. Mobile and internet revolutions. In *TestIT Summit 2003*, Helsinki, Nov. 2003. Conformiq, Borland. Electronic publication.

[27] H. H. Kari. Packet level autenthication (PLA). In *Data Security 2003*, Helsinki, Oct. 2003. Tieturi. Electronic publication.

[28] H. H. Kari. Securing communication in wired and wireless military networks. In *National Security 2003*, Helsinki, Oct. 2003. Tieturi. Electronic publication.

[29] H. H. Kari. Securing communication in wired and wireless military networks packet level autenthication (PLA). In *Workshop on Secure IT and Vulnerabilities of Commercial Wireless Components*, Stockholm, Sweden, Nov. 2003. IDG Europe, ONR FIO, USAITC-A.

[30] H. H. Kari. Security in future networks. In *Tietoturvaseminaari*, Helsinki, May 2003. Cisco Systems, SSH Communications Security. Electronic publication.

[31] H. H. Kari. Yksityisyys langattomissa verkoissa. In *Corporate Security*, Espoo, May 2003. Teleware, Tietoturva ry. Electronic publication.

[32] H. H. Kari and C. Candolin. Context aware management architecture. In *Commercial Information Technology for Military Operations (CITMO 2003)*, Ronneby, Sweden, Apr. 2003. IDG Europe AB, CD-ROM.

[33] M. Komu, M. Kousa, J. Lundberg, and C. Candolin. An implementation of HIP for Linux. In *Proceedings of Ottawa Linux Symposium*, Ottawa, Canada, July 2003.

[34] T. Latvala. Efficient model checking of safety properties. In *Model Checking Software. 10th International SPIN Workshop*, pages 74–88. Springer, 2003.

[35] H. Lipmaa. On Diophantine Complexity and Statistical Zero-Knowledge Arguments. In C. S. Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 398–415, Taipei, Taiwan, November 30–December 4 2003. Springer-Verlag.

[36] H. Lipmaa. Verifiable Homomorphic Oblivious Transfer and Private Equality Test. In C. S. Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 416–433, Taipei, Taiwan, November 30–December 4 2003. Springer-Verlag.

[37] H. Lipmaa, N. Asokan, and V. Niemi. Secure Vickrey Auctions without Threshold Trust. In *Financial Cryptography 2002*, volume 2357 of *Lecture Notes in Computer Science*, pages 87–101, Southhampton Beach, Florida, 11–14 Mar. 2002. Springer-Verlag.

[38] J. Lundberg and C. Candolin. Hierarchical multicast caching. In *Proceedings of IEEE 9th Asia-Pacific conference on communications*, Penang, Malaysia, September 2003.

[39] J. Lundberg and C. Candolin. Mobility in the Host Identity Protocol (HIP). In *Proceedings of the International Symposium on Telecommunications (IST2003)*, Isfahan, Iran, August 2003.

[40] J. Lundberg, C. Candolin, and H. H. Kari. Support for transparent multicast content distribution to mobile wireless clients. In *Proceedings of the 2003 International Conference on Wireless Networks (ICWN 2003)*, Las Vegas, Nevada, USA, June 2003.

[41] M. Mäkelä. Model checking safety properties in modular high-level nets. In W. M. van der Aalst and E. Best, editors, *Application and Theory of Petri Nets 2003: 24th International Conference, ICATPN 2003*, number 2679 in Lecture Notes in Computer Science, pages 201–220, Eindhoven, The Netherlands, June 2003. Springer-Verlag, Berlin, Germany.

[42] I. Niemelä. Answer set programming: an approach to declarative problem solving. In *Proceedings of Eighth Scandinavian Conference on Artificial Intelligence*, pages 189–191, Bergen, Norway, November 2003. IOS Press. Extended abstract of a key note talk.

[43] I. Niemelä. Answer set programming: From model computation to problem solving. In *Proceedings of CADE-19 Workshop on Model Computation — Principles, Algorithms, Applications*, Miami, Florida, USA, July 2003. Extended abstract of an invited talk.

[44] E. Oikarinen. Logiikkaohjelmien ekvivalenssitestaus. In A. Korhonen and J. Tarhio, editors, *Tietojenkäsittelytieteen päivät 2003*, pages 44–47, Espoo, Finland, May 2003. Yliopistopaino. In Finnish.

[45] L. Ojala and O.-M. Penttinen. Simulating quantum interference in Feynman's $\sqrt{\text{NOT}}$-computer with stochastic Petri nets. In *Proceedings of the European Simulation and Modelling Conference (ESMc2003)*, pages 494–502, Naples, Italy, Oct. 2003.

[46] L. Ojala, O.-M. Penttinen, and H. Rantanen. A novel application of stochastic Petri nets: Simulation of serial quantum computers—Feynman's swap computer. In P. Kemper, editor, *On-site Proceedings of ICALP03 Satellite Workshop on Stochastic Petri Nets and Related Formalisms*, number 780/2003 in Forschungsberichte des Fachbereichs Informatik der Universität Dortmund, pages 103–122, Eindhoven, the Netherlands, June 2003.

[47] L. Ojala, H. Rantanen, E. Parviainen, O.-M. Penttinen, and J. Reunanen. Feynman's Quantum Computer modeled using Petri nets: Full adder circuit. In *Proceedings of the 7th World Multiconference on Systemics, Cybernetics and Informatics (SCI'2003)*, Orlando, FL, USA, 2003.

[48] O.-M. Penttinen. On solving ordinary differential equation systems with Generalized Stochastic Petri Nets. In *Proceedings of the European Simulation and Modelling Conference (ESMc2003)*, pages 395–402, Naples, Italy, Oct. 2003.

[49] P. Puhakainen, C. Candolin, and H. H. Kari. Using adaptive decision making based on incomplete trust in electronic commerce. In *Proceedings of the 7th WSEAS International Conference on Communications (ICCON)*, Corfu, Greece, July 2003.

[50] T. Pyhälä and K. Heljanko. Specification coverage aided test selection. In J. Lilius, F. Balarin, and R. J. Machado, editors, *Proceeding of the 3rd International Conference on Application of Concurrency to System Design (ACSD'2003)*, pages 187–195, Guimarães, Portugal, June 2003. IEEE Computer Society.

[51] T. Ronkainen, H. Oja, and P. Orponen. Computation of the multivariate Oja median. In R. Dutter, P. Filzmoser, U. Gather, and P. J. Rousseeuw, editors, *Developments in Robust Statistics: Proceedings of the International Conference on Robust Statistics ICORS'01 (Stift Vorau, Austria, July 2001)*, pages 344–359, Berlin Heidelberg, 2003. Springer-Verlag.

[52] M.-J. O. Saarinen. Cryptanalysis of block ciphers based on SHA-1 and MD5. In T. Johansson, editor, *Fast Software Encryption 2003*, Lecture Notes in Computer Science. Springer-Verlag, 2003. To appear.

[53] S. Seitz and P. Orponen. An efficient local search method for random 3-satisfiability. In L. M. Kirousis and E. Kranakis, editors, *Proceedings of the IEEE LICS'03 Workshop on Typical Case Complexity and Phase Transitions (Ottawa, Canada, June 2003)*, volume 16 of *Electronic Notes in Discrete Mathematics*, Amsterdam, 2003. Elsevier.

[54] J. Tiihonen, T. Soininen, I. Niemelä, and R. Sulonen. A practical tool for mass-customising configurable products. In *Proceedings of the 14th International Conference on Engineering Design*, pages 1290–1299, 2003.

[55] K. Varpaaniemi. Modelling and analysing a PLC-based railway traffic control system. In L. Czaja, editor, *Concurrency, Specification and Programming: Proceedings of the CS&P'2003 Workshop, Czarna k. Ustrzyk Dolnych, Poland, September 25–27, 2003, Volume 2*, pages 539–549. Zakład Graficzny UW, zam. 591/2003, Warsaw, 2003.

[56] S. E. Virtanen. Clustering the Chilean web. In *Proceedings of the First Latin American Web Congress*, pages 229–231, Los Alamitos, CA, USA, Nov. 2003. IEEE Computer Society.

[57] J. Wallén. Linear approximations of addition modulo 2^n. In *Fast Software Encryption 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 261–273. Springer-Verlag, 2003.

6.3 Reports

[58] A. Ambainis, M. Jakobsson, and H. Lipmaa. Cryptographic Randomized Response Techniques. Technical Report 2003/027, International Association for Cryptologic Research, Feb. 10 2003.

[59] E. Elkind and H. Lipmaa. Interleaving Cryptography and Mechanism Design: The Case of Online Auctions. Technical Report 2003/021, International Association for Cryptologic Research, Feb. 3 2003.

[60] J. F. Groote and M. Keinänen. Solving disjunctive/conjunctive boolean equation systems with alternating fixed points. Technical Report SEN-R0310, Stichting Centrum voor Wiskunde en Informatica (CWI), Amsterdam, Amsterdam, Netherlands, December 2003.

[61] T. Janhunen. Translatability and intranslatability results for certain classes of logic programs. Research Report A82, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Nov. 2003.

[62] P. Kaski. A census of Steiner triple systems and some related combinatorial objects. Research Report A78, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, June 2003.

[63] H. Lipmaa. On Diophantine Complexity and Statistical Zero-Knowledge Arguments. Technical Report 2003/105, International Association for Cryptologic Research, May 25 2003.

[64] E. Oikarinen. Testing the equivalence of disjunctive logic programs. Research Report A85, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Dec. 2003.

[65] T. Syrjänen. Logic programming with cardinality constraints. Research Report A86, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Dec. 2003.

[66] H. Tauriainen. Nested emptiness search for generalized Büchi automata. Research Report A79, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, July 2003.

[67] H. Tauriainen. On translating linear temporal logic into alternating and nondeterministic automata. Research Report A83, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Dec. 2003.

[68] K. Varpaaniemi, editor. Annual report for the year 2002. Annual Report Y2002, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, June 2003.

[69] S. Virtanen. Properties of nonuniform random graph models. Research Report A77, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, May 2003.

[70] J. Wallén. On the differential and linear properties of addition. Research Report A84, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Dec. 2003.

6.4 Doctoral Dissertations

[71] T. Junttila. On the symmetry reduction method for Petri nets and similar formalisms. Research Report A80, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Sept. 2003. Doctoral dissertation.

[72] M. Mäkelä. Efficient computer-aided verification of parallel and distributed software systems. Research Report A81, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, Nov. 2003. Doctoral dissertation.

6.5 Licentiate's Theses

[73] Y. Kortesniemi. *Managing the usage of authorisation certificates.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer, 2003.

[74] T. Syrjänen. *Logic programming with cardinality constraints.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer, 2003.

[75] H. Tauriainen. *On translating linear temporal logic into alternating and nondeterministic automata.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer, 2003.

[76] T. Tynjälä. *Combining abstractions and reachability analysis: a case study of RLC protocol.* Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer, 2003.

[77] S. Virtanen. *Properties of Nonuniform Random Graph Models*. Licentiate's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer, 2003.

6.6 Master's Theses

[78] N. Cankar. Model based testing using UML. Master's thesis, Helsinki University of Technology, Department of Electrical and Communications Engineering, 2003.

[79] N. Chen. Enterprise portal as the enterprise integration solution. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

[80] A. Järvinen. Smart card based configuration and authentication in mobile IPv6. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

[81] S. Li-Kokko. An SPKI based secure multicast architecture with copyright protection. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

[82] E. Oikarinen. Testing the equivalence of disjunctive logic programs. Master's thesis, Helsinki University of Technology, Department of Engineering Physics and Mathematics, 2003.

[83] T. Pyhälä. Specification-based test selection in formal conformance testing. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

[84] T. Vainio. The applicability of Bluetooth in ad hoc networks. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

[85] J. Wallén. On the differential and linear properties of addition. Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Laboratory for Theoretical Computer Science, 2003.

6.7 Software

[86] T. Janhunen and P. Simons. GnT 2 — tool for computing stable models for disjunctive logic programs. `http://www.tcs.hut.fi/Software/gnt/`, 2003. Computer Program.

[87] T. Jussila. A BMC tool translating LTSs to boolean circuits. http://www.tcs.hut.fi/~tjussila/otf, May 2003. Software.

[88] T. Latvala. scheck1.1. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, 2003. Software.

[89] V. Nuorvala. IPv6-in-IPv6 tunnel. http://www.kernel.org/pub/linux/kernel/v2.6/, 2003. Software.

[90] V. Nuorvala, H. Petander, and A. Tuominen. MIPL Mobile IPv6 for Linux, version 1.0. http://www.mobile-ipv6.org/download.html, 2003. Software.

[91] E. Oikarinen. DLPEQ 1.9 — a tool for testing the equivalence of disjunctive logic programs. http://www.tcs.hut.fi/Software/lpeq/index.shtml#dlpeq, 2003. Computer Program.

[92] T. Pyhälä and K. Heljanko. Bomotest: A formal conformance testing tool, version 1.5. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, http://www.tcs.hut.fi/%7Etpyhala/bomotest/bomotest.html, 2003. Software.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2003