Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2000
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2000
Espoo 2001 HUT-TCS-Y2000

ANNUAL REPORT FOR THE YEAR 2000

Kimmo Varpaaniemi (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 2000
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2000
Espoo 2001 HUT-TCS-Y2000

ANNUAL REPORT FOR THE YEAR 2000

Kimmo Varpaaniemi (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: Picaset Oy,
Helsinki 2001

ABSTRACT: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2000. In the PDF version of this report, URL addresses are links to those addresses. For example, you get to the home page of the laboratory by clicking http://www.tcs.hut.fi/index.html.

CONTENTS

1 PERSONNEL

1.1 University staff

Ojala, Leo, Lic.Sc. (Tech.) (cf. 1.3)	Professor in Digital Systems Science. Head of the Laboratory. Retired on October 31.
Niemelä, Ilkka, D.Sc. (Tech.) (cf. 1.2, 1.3, 1.5)	Professor in Computer Science since August 1. Head of the Laboratory since November 1.
Kangasniemi, Ulla	Secretary of the Laboratory.
Husberg, Nisse, D.Sc. (Tech.) (cf. 1.2, 1.3)	Professor (pro tem).
Janhunen, Tomi, D.Sc. (Tech.) (cf. 1.3)	Professor (pro tem). Senior Assistant since February 1 until August 1 (on leave). Teaching Researcher since August 1 (on leave since November 1).
Lassila, Eero, Lic.Sc. (Tech.) (cf. 1.5)	Laboratory Manager since February 1 (on leave).
Varpaaniemi, Kimmo, D.Sc. (Tech.) (cf. 1.4, 1.5)	Senior Assistant since February 1 (on leave).

1.2 Docents

Husberg, Nisse, D.Sc. (Tech.) (cf. 1.1, 1.3)	Docent in Verification since November 1.
Niemelä, Ilkka, D.Sc. (Tech.) (cf. 1.1, 1.3, 1.5)	Docent in Logic and its Applications in Computer Science and Engineering.
Ukkonen, Esko, D.Phil.	Docent in Theoretical Computer Science. Professor in Computer Science (University of Helsinki and the Academy of Finland).
Östergård, Patric R.J., D.Sc. (Tech.) (cf. 1.3, 1.5)	Docent in Coding Theory. Teaching Researcher until March 6 (on leave). Professor in Information Theory (HUT, Department of Electrical and Communications Engineering) since August 1 (on leave).

1.3 Main teachers of the active courses of the year 2000

Heinonen, Rauno, Lic.Sc. (Tech.)	Tik-79.148	Introduction to Theoretical Computer Science (spring)
Heljanko, Keijo, Lic.Sc. (Tech.) (cf. 1.5)	Tik-79.186	Reactive Systems (spring)
Herttua, Ilkka, Stud.Tech.	Tik-79.232	Safety-Critical Systems (spring)
Huima, Antti, M.Sc. (Tech.)	Tik-79.159	Cryptography and Data Security (spring)
Husberg, Nisse, Professor (pro tem), D.Sc. (Tech.), Docent (cf. 1.1, 1.5)	Tik-79.185 Tik-79.193 Tik-79.298	Verification (autumn) Formal Description Techniques for Concurrent Systems (spring) Postgraduate Course in Digital Systems Science (autumn)
Janhunen, Tomi, Professor (pro tem), D.Sc. (Tech.) (cf. 1.1)	Tik-79.144 Tik-79.154 Tik-79.189 Tik-79.230 Tik-79.295	Logic in Computer Science: Foundations (autumn) Logic in Computer Science: Special Topics II (autumn) Student Project in Theoretical Computer Science (spring) Foundations of Agent-Based Computing (spring) Individual Studies (spring)
Kettunen, Esa, M.Sc. (Tech.) (cf. 1.4, 1.5)	Tik-79.179 Tik-79.231	Parallel and Distributed Digital Systems (spring) Parallel and Distributed Digital Systems (autumn)
Niemelä, Ilkka, Professor, D.Sc. (Tech.), Docent (cf. 1.1, 1.2, 1.5)	Tik-79.146 Tik-79.189 Tik-79.240 Tik-79.295	Logic in Computer Science: Special Topics I (spring) Student Project in Theoretical Computer Science (autumn) Special Course in Computational Complexity (autumn) Individual Studies (autumn)
Ojala, Leo, Professor, Lic.Sc. (Tech.) (cf. 1.1)	Tik-79.189 Tik-79.192 Tik-79.194 Tik-79.295 Tik-79.298	Student Project in Theoretical Computer Science (spring) Special Course in Theoretical Computer Science (autumn) Seminar on Theoretical Computer Science (spring) Individual Studies (spring) Postgraduate Course in Digital Systems Science (spring)
Östergård, Patric R.J., Professor (Dept. of ECE), D.Sc. (Tech.), Docent (cf. 1.2, 1.5)	Tik-79.161 Tik-79.163	Combinatorial Algorithms (spring) Special Course in Combinatorial Algorithms (autumn)

1.4 Teaching assistants in the active courses of the year 2000

Aalto, Annikka, Stud.Tech.	Tik-79.179	Parallel and Distributed Digital Systems (spring)
Beaver, Harriet, Stud.Tech. (cf. 1.5)	Tik-79.192 Tik-79.194	Special Course in Theoretical Computer Science (autumn) Seminar on Theoretical Computer Science (spring)
Haanpää, Harri, Lic.Sc. (Tech.) (cf. 1.5)	Tik-79.161	Combinatorial Algorithms (spring)
Honkola, Jukka, Stud.Tech. (cf. 1.5)	Tik-79.179 Tik-79.231	Parallel and Distributed Digital Systems (spring) Parallel and Distributed Digital Systems (autumn)
Junttila, Tommi, Lic.Sc. (Tech.) (cf. 1.5)	Tik-79.240	Special Course in Computational Complexity (autumn)
Jussila, Toni, M.Sc. (Tech.) (cf. 1.5)	Tik-79.144	Logic in Computer Science: Foundations (autumn)
Kaski, Petteri, Stud.Tech. (cf. 1.5)	Tik-79.163	Special Course in Combinatorial Algorithms (autumn)
Kettunen, Esa, M.Sc. (Tech.) (cf. 1.3, 1.5)	Tik-79.298	Postgraduate Course in Digital Systems Science (spring)
Syrjänen, Tommi, M.Sc. (Tech.) (cf. 1.5)	Tik-79.144 Tik-79.148 Tik-79.154 Tik-79.230	Logic in Computer Science: Foundations (autumn) Introduction to Theoretical Computer Science (spring) Logic in Computer Science: Special Topics II (autumn) Foundations of Agent-Based Computing (spring)
Tauriainen, Heikki, M.Sc. (Tech.) (cf. 1.5)	Tik-79.154	Logic in Computer Science: Special Topics I (spring)
Tynjälä, Teemu, M.Sc. (Tech.) (cf. 1.5)	Tik-79.192	Special Course in Theoretical Computer Science (autumn)
Varpaaniemi, Kimmo, D.Sc. (Tech.) (cf. 1.1, 1.5)	Tik-79.298	Postgraduate Course in Digital Systems Science (autumn)

1.5 Researchers and research assistants

Aura, Tuomas	D,Sc. (Tech.)	Researcher
Beaver, Harriet	Stud.Tech. (cf. 1.4)	Research Assistant (except February)
Elfström, Jan	M.Sc. (Tech.)	Researcher (until November 6)
Falck, Emil	Stud.Tech.	Research Assistant (June 1 – August 31)
Gaus, Marco	Stud.Tech. (cf. 4.3)	Trainee (August 16 – October 15)
Haanpää, Harri	Lic.Sc. (Tech.) (cf. 1.4)	Researcher
Heljanko, Keijo	Lic.Sc. (Tech.) (cf. 1.3)	Researcher
Hietalahti, Maarit	Stud.Tech.	Research Assistant (except February)
Honkola, Jukka	Stud.Tech. (cf. 1.4)	Research Assistant
Junttila, Tommi	Lic.Sc. (Tech.) (cf. 1.4)	Researcher
Jussila, Toni	M.Sc. (Tech.) (cf. 1.4)	Researcher (since August 1)
Kaski, Petteri	Stud.Tech. (cf. 1.4)	Research Assistant (May 15 – July 31)
Kettunen, Esa	M.Sc. (Tech.) (cf. 1.3, 1.4)	Researcher (until July 1)
Lassila, Eero	Lic.Sc. (Tech.) (cf. 1.1)	Researcher
Latvala, Timo	M.Sc. (Tech.)	Research Assistant (until November 1) Researcher (since November 1)
Mäkelä, Marko	Lic,Sc. (Tech.)	Researcher
Mäki, Silja	M.Sc.	Researcher
Norrman, Vesa	Stud.Tech.	Research Assistant (June 1 – August 31)
Niemelä, Ilkka	D.Sc. (Tech.) (cf. 1.1, 1.2, 1.3)	Senior Fellow of the Academy of Finland (until August 1)
Nurmela, Kari J.	D,Sc. (Tech.)	Researcher
Pääkkönen, Rauni	Stud.Tech.	Research Assistant (since June 1)
Schulz, André	Stud.Tech. (cf. 4.3)	Trainee (since August 1)
Simons, Patrik	D.Sc. (Tech.)	Researcher (until February 1)
Syrjänen, Tommi	M.Sc. (Tech.) (cf. 1.4)	Researcher
Taurianen, Heikki	M.Sc. (Tech.) (cf. 1.4)	Research Assistant (until November 1) Researcher (since November 1)

Tiittula, Lauri	Stud.Tech.	Research Assistant (June 1 – September 30)
Tynjälä, Teemu	M.Sc. (Tech.) (cf. 1.4)	Researcher
Varpaaniemi, Kimmo	D.Sc. (Tech.) (cf. 1.1, 1.4)	Researcher
Viljanen, Joose	M.Sc.	in civil service (discharged on August 30)
Östergård, Patric R.J.	D.Sc. (Tech.) (cf. 1.2, 1.3)	Senior Fellow of the Academy of Finland

2 EDUCATIONAL ACTIVITIES

The aim of the education at the undergraduate level is to give students basic insight into theoretical computer science and parallel and distributed digital systems, as well as learning in applying the theoretical results to practice. At the post-graduate level knowledge in the aforementioned areas will be completed further, especially in some particular theoretical questions. During the year 2000, the following courses were active, i.e. arranged as lectures, seminars or projects.

Tik-79.144 Logic in Computer Science: Foundations
(autumn, 2 credits ; main teacher: Tomi Janhunen)

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

Tik-79.146 Logic in Computer Science: Special Topics I
(spring, 2 credits ; main teacher: Ilkka Niemelä)

Contents: Basics of modal logic. Current applications in computer science.

Tik-79.148 Introduction to Theoretical Computer Science
(spring, 2 credits ; main teacher: Rauno Heinonen)

Contents: Basics of the theory of formal languages and automata. Theory of computation. Fundamental limitations of computers.

Tik-79.154 Logic in Computer Science: Special Topics II
(autumn, 2 credits ; main teacher: Tomi Janhunen)

Contents: Efficient implementation methods for propositional logic. Logical foundations and implementation techniques of rule-based systems. Current applications.

Tik-79.159 Cryptography and Data Security
(spring, 3 credits ; main teacher: Antti Huima)

Contents: Cryptographic algorithms and protocols. Modern symmetric and asymmetric encryption. Digital signatures. Protection of integrity. Cryptographic hash functions. Authentication protocols. Key exhange and identification protocols. Design and analysis of cryptographic protocols. Electronic commerce. Steganography. New directions in data security.

Tik-79.161 Combinatorial Algorithms
(spring, 2 credits ; main teacher: Patric R.J. Östergård)

Contents: Basic algorithms and computational methods for combinatorial problems. Combinatorial structure generation (e.g. permutations). Search methods. Graph algorithms and combinatorial optimization. Algorithm complexity.

Tik-79.163 Special Course in Combinatorial Algorithms
(autumn, 2 credits ; main teacher: Patric R.J. Östergård)

Contents: Contemporary research problems and applications in combinatorial algorithms and combinatorial optimization.

Tik-79.179 Parallel and Distributed Digital Systems
(spring, 3 credits ; main teacher: Esa Kettunen)

Contents: Modelling and analysis of parallel and distributed digital systems. Concurrency. Basics of Petri nets and process algebra (CCS). Using computer-aided methods for the analysis and verification of telecommunication systems, especially communication protocols.

Tik-79.185 Verification
(autumn, 3 credits ; main teacher: Nisse Husberg)

Contents: Verification and analysis of parallel and distributed systems using tools. Applications to telecommunication protocols. Practical verification methods, e.g. partial reachability analysis. Introduction to current research problems.

Tik-79.186 Reactive Systems
(spring, 2 credits ; main teacher: Keijo Heljanko)

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

Tik-79.189 Student Project in Theoretical Computer Science
(3 credits ; main teachers: Leo Ojala, Tomi Janhunen,
and Ilkka Niemelä)

Tik-79.192 Special Course in Theoretical Computer Science
(autumn, 2 credits ; main teacher: Leo Ojala)

Contents: Current applications in theoretical computer science.

Tik-79.193 Formal Description Techniques for Concurrent Systems
(spring, 2 credits ; main teacher: Nisse Husberg)

Contents: Validation, testing and analysis methods for large concurrent systems, embedded systems and real-time software.

Tik-79.194 Seminar on Theoretical Computer Science
(spring, 2 credits ; main teacher: Leo Ojala)

Contents: Current trends and research problems in theoretical computer science.

Tik-79.230 Foundations of Agent-Based Computing
(spring, 3 credits ; main teacher: Tomi Janhunen)

Contents: Structure of software agents. Rational and intelligent agents. Architectures, implementation technologies and applications of agent-based systems.

Tik-79.231 Parallel and Distributed Digital Systems
(autumn, 3 credits ; main teacher: Esa Kettunen)

Contents: Modelling and analysis of parallel and distributed digital systems. Concurrency. Basics of Petri nets and process algebra (CCS). Using computer-aided methods for the analysis and verification of telecommunication systems, especially communication protocols.

Tik-79.232 Safety-Critical Systems
(spring, 2 credits ; main teacher: Ilkka Herttua)

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

Tik-79.240 Special Course in Computational Complexity
(autumn, 3 credits ; main teacher: Ilkka Niemelä)

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

Tik-79.295 Individual Studies
(1–10 credits ; main teachers: Leo Ojala, Tomi Janhunen, and Ilkka Niemelä)

Tik-79.298 Postgraduate Course in Digital Systems Science
(10 credits ; main teachers: Leo Ojala and Nisse Husberg)

Contents: Insight into current research problems in theoretical computer science.

3 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 3.1, 3.2, 3.3, and 3.4. For more applied research funding has been awarded by the National Technology Agency of Finland as well as companies and other non-academic partners. This research is described in Sections 3.5 and 3.6.

3.1 Computational methods in coding theory and discrete mathematics

This subsection describes research which during the year 2000 was carried out by Patric R.J. Östergård (the leader), Harri Haanpää, Petteri Kaski, and Kari J. Nurmela. During the year 2000, the research project contributed to the publications [2, 3, 4, 5, 7, 9, 10, 11, 12, 49, 52, 57].

The aim of the research 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, just to mention a few. They have also been applied to a variety of practical problems, many of which are related to telecommunications. Both exhaustive and stochastic methods are used.

The stochastic methods used include simulated annealing, tabu search, and evolutionary algorithms; however, almost without exception, tabu search has turned out to yield the best performance for the problems under study. As an example, a new bound for a Ramsey number, $R(5,9) > 120$, was obtained in this manner (using tabu search).

As for exhaustive methods, the main focus has been on orderly generation of discrete structures. Using these, classification results have been obtained for various structures, including balanced incomplete block designs (BIBDs), resolvable BIBDs, balanced ternary designs, covering arrays, covering codes, linear codes, etc. Structures for which other (algebraic, combinatorial, and computational) methods have been applied include Bhaskar Rao designs, complete caps, constant-composition codes, constant weight codes, error-correcting codes, etc. One of the main results obtained is a computational proof that no (15,5,4) RBIBD exists.

New algorithms for the maximum clique problem and for the more general maximum-weight clique problem have been developed and an implementation of the latter algorithm has been made available electronically via http://www.tcs.hut.fi/Personnel/patric.html. The new algorithms perform better than previous algorithms for many classes of random graphs and certain other types of graphs (especially graphs related to code construction).

Many of the computational results have been obtained with very CPU-intensive computations, some of which have been distributed over the entire computer network of the laboratory using the distributed batch system autoson.

3.2 Constraint programming based on default rules

This subsection describes research which during the year 2000 was carried out by Ilkka Niemelä (the leader), Harriet Beaver, Keijo Heljanko, Tomi Janhunen, Tommi Junttila, Toni Jussila, Patrik Simons, Tommi Syrjänen, and Heikki Tauriainen. During the year 2000, the research project contributed to the publications [6, 13, 15, 19, 21, 24, 25, 26, 29, 30, 31, 32, 39, 42, 43, 44, 45, 48, 50, 53, 54, 56, 62, 65, 66, 67, 68].

The goal of the research is to develop a novel constraint programming paradigm based on default rules and study its applications. The project has focused on logic program type rules and the stable model semantics. We have developed a C++ implementation of the approach, the `Smodels` system [39], which is among the leading systems in the area and used in dozens of research groups all over the world. `Smodels` is available via http://www.tcs.hut.fi/Software/smodels/index.html. In 2000, the basic language of `Smodels` has been extended, novel implementation techniques have been developed, expressivity issues have been studied and various applications areas have been investigated. The work is described in more detail below.

Extending the rule language
(*Ilkka Niemelä, Patrik Simons, and Tommi Syrjänen*)

In many applications normal logic program rules lack expressivity to handle cardinalities, weights and optimization. We have developed an extended rule language which allows for cardinality and weight constraints and optimization capabilities and devised a generalization of the stable model semantics for it [19]. Also novel implementation methods for computing stable models of the extended language have been developed. More details on the techniques can be found in Patrik Simons' doctoral dissertation [53].

The extended rule languages allows also the use of logical variables, function symbols and built-in arithmetic. For that we have developed an instantiator which transforms a logic program with variables into an equivalent variable-free program, possibly simplifying it in the process. Our implementation, `lparse`, has been designed to be the front-end of the `Smodels` system [39], but it has also been used with, e.g., the DeReS default logic reasoning system developed in the University of Kentucky.

Interesting family of benchmarks for rule-based systems has been developed by considering the DES cipher and known plaintext attacks against it [26]. It turns out that `Smodels` is very competitive against state of the art satisfiability checkers in this benchmark set.

Expressive power analysis of rule-based languages
(*Tomi Janhunen*)

This research continues earlier work on classifying non-monotonic logics on the basis of their expressive powers. The classification method is based on the existence of polynomial, faithful and modular (PFM) translation functions between non-monotonic logics under consideration. As a result, a wide variety of non-monotonic logics have been arranged to form an expressive power hierarchy (EPH). In 2000, Przymusinski's stationary default logic (STDL) was taken into consideration [29]. It was established that STDL resides in its own class of EPH which (i) is located between the classes containing Reiter's default logic and classical propositional logic and (ii) is incomparable with the other classes of EPH. Moreover, the method based on PFM translation functions was accommodated to the case of normal logic programs in order to study how the number of positive subgoals affects the expressiveness of rules [30]. The results indicate that constraining the number of positive subgoals to be at most n reduces the expressiveness of rules when $n = 0$ or $n = 1$, and there is no reduction when $n \geq 2$. The methods for computing disjunctive stable models were also considered [31]. The objective in this research was to use the existing implementations of the stable model semantics of normal logic programs (e.g., the `Smodels` systems implemented in the laboratory [39]) for computations. To establish this, two translations for disjunctive logic programs had to be developed. The first translation captures partial stable models of a disjunctive logic programs in terms of total stable models. The second translation consists of two normal logic programs that (i) generate candidates for the total stable models of a disjunctive logic program and (ii) test the minimality of the candidates, respectively.

Software configuration management (*Tommi Syrjänen*)

Modern software products are large and complex and they may contain hundreds or thousands of interacting components. The aim of software configuration management research is to find new methods for representing configuration knowledge and constructing valid configurations that satisfy user requirements.

The current software configuration research in the laboratory concentrates on developing rule-based methods for expressing configuration knowledge using the stable model semantics of logic programs as a formal framework. Several new highly-expressive types of rules have been developed that make it possible to obtain more compact representations of product constraints. Also, the problems of diagnosing faulty configurations and finding optimal configurations have been researched [43, 44]. As a case study, a formal configuration model of the Debian GNU/Linux system has been developed.

Product configuration (*Ilkka Niemelä*)

Together with the product data management group at Helsinki University of Technology (Timo Soininen, Juha Tiihonen, Reijo Sulonen) we have developed general methodology for product configuration [42]. 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. Moreover, `Smodels` provides a promising inference engine on top of which intelligent automatic configurators can be built.

Bounded model checking (*Keijo Heljanko and Ilkka Niemelä*)

Bounded model checking has been recently introduced as a memory efficient way of finding bugs in reactive systems. We have shown that bounded model checking can be efficiently implemented on top of the `Smodels` system [13]. The translation also benefits from the inherent concurrency present in the model, a feature which has not been previously addresses in bounded model checking.

Boolean circuit satisfiability checking
(*Tommi Junttila and Ilkka Niemelä*)

Propositional satisfiability (SAT) checking can be seen as a special case of stable model computation for logic program type rules. As this case appears frequently in applications, special purpose methods for it have been developed using ideas from the implementation techniques for stable model computation developed in the project. Most state of the art SAT checkers require that the input must be transformed into conjunctive normal form (CNF) and the algorithms are based on working with CNF formulae. We decided to study an alternative approach where Boolean circuits are used as the input format for the SAT checker. Boolean circuits provide a natural and compact way of encoding problems allowing structure sharing. A tableau algorithm for solving satisfiability problems has been developed. It works directly on Boolean circuits without any CNF transformation. A C++ implementation of the algorithm, the `BC-Sat` system, is available via http://www.tcs.hut.fi/%7etjunttil/bcsat/index.html. The system has been applied to bounded model checking problems with encouraging results [30].

3.3 Formal methods in distributed systems

This subsection describes research which during the year 2000 was carried out by Leo Ojala (the leader until November 1), Ilkka Niemelä (the leader since November 1), Tuomas Aura, Harrier Beaver, Keijo Heljanko, Tomi Janhunen, Tommi Junttila, Rauni Pääkkönen, Heikki Tauriainen, and Teemu Tynjälä. During the year 2000, the research project contributed to the publications [1, 15, 20, 23, 24, 25, 27, 28, 33, 34, 38, 40, 41, 45, 46, 47, 48, 50, 51, 54, 55, 62, 64, 68].

This is a basic research project on analysis and design methods of parallel and distributed systems. It focuses on model checking, symmetries, agent-based computing, information security, and quantum computing. Below more details on the research is given.

Prefix-based model checking (*Keijo Heljanko*)

Research concentrated on using symbolic methods to alleviate the state explosion problem in model checking. The main approach used is a method called *complete finite prefixes* originally devised by McMillan. We have created a new prefix based linear time temporal logic (LTL) model checking procedure [24, 48]. Also computational complexity issues of model checking with prefixes has been addressed in [25]. In co-operation with the `MARIA` project efficient handling of fairness in model checking [6] has been researched.

Testing implementations of algorithms for translating linear time temporal logic formulae into Büchi automata
(*Heikki Tauriainen and Keijo Heljanko*)

Automata-theoretic model checking tools for linear time temporal logic (LTL) use algorithms which translate LTL properties into Büchi automata. These algorithms have to be implemented very carefully to ensure the correctness of model checking results in practice. In this research we have devised methods for detecting errors in LTL-to-Büchi translation algorithm implementations by (i) checking for known relationships between a pair of automata obtained from two complementary LTL formulae and (ii) comparing the model checking results obtained using independent LTL-to-Büchi translation algorithm implementations. Incorrect implementations are identified with the help of a restricted LTL model checking algorithm for single computation paths. Most of the test methods have been integrated into the `lbtt` software package available via http://www.tcs.hut.fi/%7ehtauriai/index.html.

Symmetries in verification (*Tommi Junttila*)

The symmetry reduction method is a way to alleviate the state space explosion problem occurring in the state space analysis of concurrent systems. It exploits the symmetries (automorphisms) of the state space by considering only one representative state per each set of mutually symmetric states. Thus a potentially much smaller set of states have to be considered during the state space analysis. Our earlier work has concentrated on the application of the symmetry reduction method to high-level Petri nets, i.e. nets having complex data types as tokens. During the year 2000, the research has focused on the computational complexity of the sub-problems appearing in the method when applied to a class of low-level nets, namely Place/Transition-Nets. We have done a thorough classification of the sub-problems, showing that many of them are equivalent to well-known graph theoretical problems such as graph isomorphism or are NP-complete [51]. The results have also been submitted to a journal.

Agent-based framework (*Tomi Janhunen and Rauni Pääkkönen*)

This research aims to create a framework for agent-based computing where agents have communication and coordination capabilities to operate in a heterogenous and distributed environment, and agents perform non-trivial reasoning tasks. In particular, the interest is to investigate how knowledge representation and reasoning capabilities are integrated in a distributed multi-agent system so that agents can be specified in a declarative, implementation independent way. In 2000, a declarative language was designed for the formal description of multi-agent systems by combining features from both rule-based languages and Petri nets in order to obtain a more expressive language [15]. The language has distinguished primitives for agents (i) to communicate with each other and (ii) to interact with the environment in which they operate. The first prototype of a system that enables automated execution of specifications in the language was also implemented.

Security research (*Tuomas Aura*)

Security research at the laboratory in the year 2000 focused on two areas: denial-of-service (DoS) and ad-hoc network security (cf. 3.6). The research has dealt with the use of certificates in network security protocols [38, 47] as well as methods against DoS attacks [23, 34]. These issues are addressed in Tuomas Aura's doctoral dissertation [46].

DoS attacks against Internet services have become a common problem. The attackers prevent legitimate access to a service such as a web site by artificially consuming all its resources (processing capacity, memory, or communications bandwidth). Our goal was to look for general principles behind such attacks and for ways to make the services more resistant to them.

We extended our earlier work on stateless protocols to design an authentication protocol that protects the server against many resource-exhaustion attacks. The server remains stateless until the client has been authenticated. Moreover, the client is required to perform expensive cryptographic computation before the server does. This is an example of the general principle that the cost of a DoS attacks should always be at least as high as the value of the resources it consumes from the service. The cost of attack vs. damage relation was also the basis of our analysis of the robustness of network topologies when links and nodes are disabled by an attacker.

In ad-hoc networks, we looked at two closely linked problems: group membership management and group key establishment. The dynamic nature of the ad-hoc networks and their lack of security infrastructure means that the normal solutions for these problems become unusable of inefficient. We developed a distributed mechanism for creating groups and managing them based on public-key membership certificates. Towards the end of the year, we also laid out the basic design for a contributory key-agreement protocol for networks with arbitrary topology. The protocol is a generalization of the Diffie-Hellmann exchange. It uses a theoretically minimal number of messages. This work is still in progress.

Our protocols can be used, for example, in wireless networks formed by personal electronic devices of a single person, or by a self-organizing group of sensors that are distributed randomly to the field.

Modelling Feynman's quantum computer using high-level Petri nets — a computational approach
(*Harriet Beaver, Leo Ojala, and Teemu Tynjälä*)

Petri Nets have been successfully used to model systems based on classical physics. The aim of our study is to model Feynman's quantum computer, one of the first quantum computers suggested, using high-level Petri Nets. Feynman's quantum computer is based on a circuit of quantum logic gates in a similar way as classical computers are based on boolean gates and circuits. At the time of invention, Feynman could not give a time bound for the completion of his computer's computation; a periodical measuring procedure was needed. The periodical measurement allows us to use a computational approach. We model the use and operation of Feynman's computer using predicate/transition nets; the quantum mechanical background of the operation is also described using the same formalism. Naturally, in order to carry out the task of modelling quantum mechanical phenomena, we had to extend Predicate/Transition net formalism with complex numbers.

3.4 Generative string rewriting with sound parallelism

This subsection describes research which during the year 2000 was carried out by Eero Lassila. During the year 2000, the research project contributed to the publications [16, 50].

It is studied how context-sensitive rewriting operations could be parallelized without disrupting the semantics of the string under rewriting. Specifically, it should be possible to freely adjust the degree of parallelism in the rewriting process without any need to modify the rewriting rules. Such an adjustment is allowed to change the structure but not the semantics of the output.

The short-term goal of this research is to devise a general formal model, and the long-term one is to apply the model to practical tasks like optimizing code generation.

3.5 The `MARIA` project

This subsection describes research which during the year 2000 was carried out by Leo Ojala (the leader until November 1), Nisse Husberg (the leader since November 1), Jan Elfström, Emil Falck, Keijo Heljanko, Timo Latvala, Marko Mäkelä, André Schulz, Lauri Tiittula, Teemu Tynjälä, and Kimmo Varpaaniemi. During the year 2000, the research project contributed to the publications [6, 8, 14, 17, 18, 20, 22, 28, 33, 35, 36, 37, 40, 41, 50, 58, 61, 63, 64].

The `MARIA` project started in 1998 and aims at creating a verification and debugging tool for industrial size concurrent systems. For the years 1998–2000, the project was funded by the National Technology Agency of Finland, Nokia Research Center, Nokia Networks (formerly known as Nokia Telecommunications), Elisa Communications (formerly known as Helsinki Telephone Corporation) and Finnish Rail Administration.

The increase of distributed systems with asynchronous communication, especially within telecommunications, demands new approaches to testing and verifying since in a distributed system, reproducing an observed error is inherently difficult, whereas a conventional debugging tool may interact with the system in a way that rather complicates than simplifies reproduction of errors. Therefore, it is necessary to work with formal models of the system and perform analysis of the possible states and paths of this model.

The tool [64] developed in the project has the name `MARIA` and is a reachability analysis tool for high-level Petri nets. The laboratory has a long experience in the development of reachability analysis tools for high-level Petri nets. The `PRENA` tool was developed in the late 80's. The `PROD` tool [63] was created in the early 90's and has been developed further since then, even after the development of `MARIA` started. Development of `PROD` is justified at least until `MARIA` replaces `PROD` in all important respects.

The `MARIA` project has also done some case studies in taking some real industrial problems and performing analysis. Experience from these case studies has guided the development of the analyzer both on the modelling and the analysis side. During the years 1998–2000, `PROD` was the major tool used in the case studies.

The `MARIA` tool (*Emil Falck, Timo Latvala, and Marko Mäkelä*)

The `MARIA` tool uses algebraic nets as the basic formalism and has a very developed type system. This makes it possible to model systems in an efficient way and also makes the analysis more efficient because intermediate states caused by low level handling of complex data structures is avoided. `MARIA` is modular, and it is easy to add new analysis methods and new front-ends. The front-ends can input system descriptions in standard languages like SDL and automatically translate these into formal models which are analyzed. This lowers the threshold of using the analyzer for engineers and programmers and helps avoiding modelling errors in large systems. In the end of the year 2000, `MARIA` was able to handle tens of millions of states in an efficient way, do model checking on-the-fly, support fairness constraints and perform simulation step-by-step. The year 2000 involved thorough optimization of `MARIA`. The memory and disk requirements of the reachability graph manager were reduced by improving encoding and by implementing a fully disk-based search structure. The analyzer saw a more than 5-fold performance increment thanks to an option that translates models to executable machine code and a redesign of the algorithm that computes successor states. Implementation of model checking algorithms was another central issue.

Model checking (*Keijo Heljanko and Timo Latvala*)

Verification of liveness properties of systems requires in many cases fairness constraints to be imposed on the system. In the context of modeling and analysis with Petri nets, fairness constraints have been defined but the results have not been extended to model checking. In this work Coloured Petri nets were extended with fairness constraints on the transitions. The semantics of the fairness constraints are defined with a fair Kripke structure. Model checking linear time temporal logic (LTL) properties of the Petri net is facilitated by introducing a new LTL model checking procedure. The procedure employs Streett automata to cope with the fairness constraints efficiently. Also, new algorithms for the emptiness checking problem of Streett automata and counterexample generation were designed. The new procedure has been implemented in the `MARIA` analyzer. Some experiments have been performed to test the implementation and compare it with other ways of coping with fairness constraints. The results show that the procedure scales well when compared to alternative approaches.

The SDL front-end
(*Marko Mäkelä, André Schulz, and Teemu Tynjälä*)

One of the major tasks in the `MARIA` project has been the development of an SDL (CCITT Standard SDL-92) front-end to the `MARIA` analyzer. The year 2000 involved completing the semantic analysis of SDL and implementing the actual translation from SDL to the input language of `MARIA`.

Stubborn sets (*Kimmo Varpaaniemi*)

Since `PROD` was used in case studies in the `MARIA` project and the stubborn set method is `PROD`'s best supported method against state space explosion, it was justified to continue the long-term research on the method and implement the obtained ideas in `PROD`. The emphasis during the year 2000 was in the minimization of the number of enabled transitions in a stubborn set by using a logic program with stable model semantics. On the tool level, this meant refining the interconnection between `PROD` and the `Smodels` tool [66] of the laboratory.

A PLC-based railway traffic control system
(*Jan Elfström, Lauri Tiittula, and Kimmo Varpaaniemi*)

A PLC-based railway traffic control system designed by Mipro Oy for the Haapamäki – Seinäjoki railway section was analyzed. The goal was to find out whether the system is correct w.r.t. its specifications. Though that goal was not reached, several mysterious features in the PLC program listings were found and reported to both Mipro Oy and Finnish Rail Administration. Since the `PROD` analyzer was successful in the analysis in all other respects except in overcoming the state space explosion, it is motivated to continue with the case.

The ISDN-DSS1 protocol

(*Jan Elfström, Nisse Husberg, Marko Mäkelä, Lauri Tiittula, Teemu Tynjälä, and Kimmo Varpaaniemi*)

The ISDN-DSS1 protocol was analyzed, involving analysis of the standard of the protocol as well as black box testing of an exchange of Elisa Communications. The goal was to find something that could cause incorrect accounting. Though that goal was not reached, much was learnt about how to analyze standards expressed partially in SDL and partially in natural language. Accounting is actually beyond the scope of the standard of ISDN-DSS1. It can even be conjectured that the subproject should have concentrated on some implementation description instead of the standard.

Distributed dynamic channel allocation

(*Nisse Husberg, Leo Ojala, and Teemu Tynjälä*)

As mobile terminals (and base stations) become more prevalent, the centralized channel allocation algorithms become the performance bottleneck in the system. One solution is to adopt a distributed channel allocation algorithm instead. Distributed algorithms, however, are very difficult to verify in practice. In this subproject, a distributed dynamic channel allocation algorithm for mobile computing was modelled using high level Petri nets and the `MARIA` input language. The model was very simple because high level constructs and complex data types are used. It was analyzed and found to fulfil a simple safety requirement. This case was used to guide the development of the `MARIA` analyzer.

3.6 Agent 007: security in ad-hoc networks

This subsection describes research which during the year 2000 was carried out by Tomi Janhunen (the leader), Tuomas Aura, Maarit Hietalahti, and Silja Mäki. Agent 007 was a project on the security aspects of *ad-hoc networks*. Ad-hoc networks are created for temporary purposes and without supporting infrastructure. Within this project, an ad-hoc network was considered as a group of nodes connected with unreliable transmission channels so that the overall topology of the network forms an arbitrary connected graph. The project concentrated on establishing the mutual trust relationships among the members of the group as well as creating a distributed key management within a group. As concrete outcomes of the project, protocols for (i) robust membership management of ad-hoc groups [38] and (ii) efficient group key establishment for ad-hoc networks have been developed.

4 CONFERENCES, VISITS AND GUESTS

4.1 Conferences

No conference was attended before March.

March

CGTC (31st Southeastern International Conference on Combinatorics, Graph Theory and Computing), Boca Raton FL, USA, March 13–17. Talks given by Harri Haanpää (*A Lower Bound for a Ramsey Number*) and Patric R.J. Östergård (*Recent classification results for BIBDs and their resolutions*).

GRATRA (Joint APPLIGRAPH / GETGRATS Workshop on Graph Transformation Systems), Berlin, Germany, March 25–27. Participant: Leo Ojala.

TACAS (6th International Conference on Tools and Algorithms for the Construction and Analysis of Systems), Berlin, Germany, March 27 – April 1. Participants: Nisse Husberg and Leo Ojala.

CBS (International Workshop on Communication-Based Systems), Berlin, Germany, March 31 – April 1. Participant: Leo Ojala.

April

Security Protocols Workshop, Cambridge, UK, April 3–5. A talk given by Tuomas Aura (*DOS-resistant authentication with client puzzles*).

NMR (8th International Workshop on Nonmonotonic Reasoning), Breckenridge CO, USA, April 9–11. A plenary talk given by Ilkka Niemelä (*Answer Set Programming*). An ordinary talk given by Niemelä (*DES: a Challenge Problem for Nonmonotonic Reasoning Systems*). The `Smodels` tool demonstrated by Niemelä. Other participant: Maarit Hietalahti.

KR (7th International Conference on Principles of Knowledge Representation and Reasoning), Breckenridge CO, USA, April 12–15. A talk given by Ilkka Niemelä (*Unfolding Partiality and Disjunctions in Stable Model Semantics*). Other participant: Maarit Hietalahti.

AIPS (5th International Conference on Artificial Intelligence Planning & Scheduling), Breckenridge CO, USA, April 14–17. Participants: Maarit Hietalahti and Ilkka Niemelä.

May

STOC (32nd Annual ACM Symposium on Theory of Computing), Portland OR, USA, May 21–23. Participant: Leo Ojala.

ISMVL (30th IEEE International Symposium on Multiple-Valued Logic), Portland OR, USA, May 23–25. Participant: Leo Ojala.

Sihteereiden työn kehittäminen (seminar about secretary work), Tallinn, Estonia, May 30. Participant: Ulla Kangasniemi.

June

MOVEP (Modelling and Verification of Parallel Processes, Computer Science and Automated Systems Summer School), Nantes, France, June 19–23. Participant: Timo Latvala.

ISIT (IEEE International Symposium on Information Theory), Sorrento, Italy, June 25–30. A talk given by Patric R.J. Östergård (*Error-correcting codes over an alphabet of four elements*). A session chaired by Östergård.

ICATPN (21st International Conference on Application and Theory of Petri Nets), Aarhus, Denmark, June 26–30. A talk given by Teemu Tynjälä (*Modelling and Analysing the SDL Description of the ISDN-DSS1 Protocol*). A session chaired by Leo Ojala. The `MARIA` tool demonstrated by Marko Mäkelä. Other participants: Jan Elfström, Nisse Husberg, Tommi Junttila, Timo Latvala, and Kimmo Varpaaniemi. Ojala is a member of the programme committee.

Workshop on Practical Use of High-Level Petri Nets, Aarhus, Denmark, June 27. Talks given by Nisse Husberg (*Modelling and Analysing a Distributed Dynamic Channel Allocation Algorithm for Mobile Computing Using High-Level Net Methods*) and Marko Mäkelä (*Condensed Storage of Multi-Set Sequences*). Other participants: Jan Elfström, Tommi Junttila, Timo Latvala, Leo Ojala, Teemu Tynjälä, and Kimmo Varpaaniemi. Husberg is a member of the programme committee.

July

CSFW (13th IEEE Computer Security Foundations Workshop), Cambridge, UK, July 3–5. Participant: Maarit Hietalahti.

ICALP (27th International Colloquium on Automata, Languages and Programming), Geneva, Switzerland, July 9–15. Participant: Keijo Heljanko.

CAV (12th International Conference on Computer-Aided Verification), Chicago IL, USA, July 15–21. Participants: Keijo Heljanko and Leo Ojala.

PODC (19th ACM Symposium on Principles of Distributed Computing), Portand OR, USA, July 16–19. Participant: Leo Ojala.

SCI / ISAS (4th World Multiconference on Systems, Cybernetics and Informatics; 6th International Conference on Information Systems, Analysis and Synthesis), Orlando FL, USA, July 23–26. Talks given by Teemu Tynjälä (1st talk: *Modelling and Analysis of TCN Standard Message*

Transport Protocol by Net-Theoretical Methods; 2nd talk: *Modelling a Distributed Wireless Channel Allocation Algorithm for Cellular Systems with Mobile Base Stations Using Predicate/Transition Nets*). A session chaired by Tynjälä.

CL (1st International Conference on Computational Logic), London, UK, July 24–28. An invited tutorial given by Ilkka Niemelä (*Stable Model Semantics: From Theory to Implementations and Applications*). Ordinary talks given by Tomi Janhunen (*Comparing the Expressive Powers of Some Syntactically Restricted Classes of Logic Programs*), Ilkka Niemelä (*Towards an Efficient Tableau Method for Boolean Circuit Satisfiability Checking*), and Tommi Syrjänen (*Including Diagnostic Information in Configuration Models*). Two sessions chaired by Niemelä.

AAAI (17th National Conference on Artificial Intelligence), Austin TX, USA, July 30 – August 3. An invited tutorial given by Ilkka Niemelä together with Mirosław Truszczyński (*Practical Tools for Knowledge Representation and Nonmonotonic Reasoning*).

August

IFIP TCS (1st IFIP International Conference on Theoretical Computer Science), Sendai, Japan, August 17–19. Participant: Leo Ojala.

ECAI (14th European Conference on Artificial Intelligence), Berlin, Germany, August 20–25. Participants: Tomi Janhunen and Tommi Syrjänen.

Configuration Workshop in conjunction with ECAI, Berlin, Germany, August 21–22. A talk given by Tommi Syrjänen (*Optimizing Configurations*).

WODES (5th Workshop on Discrete Event Systems), Ghent, Belgium, August 21–23. A talk given by Marko Mäkelä (*Modular Reachability Analyzer for High-Level Petri Nets*).

EXPRESS (7th International Workshop on Expressiveness in Concurrency), University Park PA, USA, August 21. Participant: Keijo Heljanko.

CONCUR (11th International Conference on Concurrency Theory), University Park PA, USA, August 22–25. A talk given by Keijo Heljanko (*Model Checking with Finite Complete Prefixes is PSPACE-Complete*).

MTCS (1st Workshop on Models for Time-Critical Systems), University Park PA, USA, August 26. Participant: Keijo Heljanko.

Hallinto- ja toimistohenkilöstön kesäseminaari (summer seminar for administration and office employees), Turku, Finland, August 24–25. Participant: Ulla Kangasniemi.

STeP (Suomen Tekoälytutkimuksen Päivät, Finnish Artificial Intelligence Days), Helsinki University of Technology, Espoo, Finland, August 28–31. Participant: Harriet Beaver.

7th International SPIN Workshop on Model Checking of Software, Stanford CA, USA, August 30 – September 1. A talk given by Heikki Tauriainen (*Testing SPIN's LTL Formula Conversion into Büchi Automata with Randomly Generated Input*).

September

ODSA (Optimal Discrete Structures and Algorithms), Rostock, Germany, September 11–13. Talks given by Harri Haanpää (*Sets in* Z_n *with Distinct Sums of Pairs*), Petteri Kaski (*Enumeration of Balanced Ternary Designs*), Kari J. Nurmela (*New Covering Arrays*), and Patric R.J. Östergård (*Is there a* $2-(22,8,4)$ *design with a* $2-(10,4,4)$ *subdesign?*).

FOSAD (International School on Foundations of Security Analysis and Design), Bertinoro, Italy, September 18–30. Participants: Maarit Hietalahti and Silja Mäki.

JELIA (7th European Workshop on Logic in Artificial Intelligence), Málaga, Spain, September 29 – October 2. A talk given by Tomi Janhunen (*Capturing Stationary and Regular Extensions with Reiter's Extensions*). Ilkka Niemelä is a member of the programme committee.

October

AWPN (Algorithmen und Werkzeuge für Petrinetze, 7th Workshop on Algorithms and Tools for Petri Nets), Koblenz, Germany, October 2–3. Participant: Leo Ojala.

CS&P (Concurrencey, Specification & Programming Workshop), Berlin, Germany, October 9–11. A talk given by Marko Mäkelä (*Applying Compiler Techniques to Reachability Analysis of High-Level Models*).

FORTE / PSTV (Formal Description Techniques for Distributed Systems and Communication Protocols (FORTE XIII); Protocol Specification, Testing and Verification (PSTV XX); IFIP TC 6 / WG 6.1 Joint International Conference), Pisa, Italy, October 10–13. Participant: Teemu Tynjälä.

NWPT (12th Nordic Workshop on Programming Theory), Bergen, Norway, October 11–13. Talks given by Nisse Husberg (*On the Necessity of Using High Level Constructs in the Analysis of Real Systems*) and Timo Latvala (*Model Checking LTL Properties of High-Level Petri Nets with Fairness Constraints*). A session chaired by Husberg.

NORDSEC (5th Nordic Workshop on Secure IT Systems), Reykjavik, Iceland, October 12–13. A talk given by Silja Mäki (*Robust Membership Management for Ad-hoc Groups*). Other participant: Maarit Hietalahti.

SAFECOMP (19th International Conference on Computer Safety, Reliability and Security), Rotterdam, The Netherlands, October 24–27. Participant: Leo Ojala.

November

Ad hoc -radiotekniikkaseminaari (radio engineering seminar), Riihimäki, Finland, November 8. Participants: Tuomas Aura, Maarit Hietalahti, Tomi Janhunen, Silja Mäki, and Ilkka Niemelä.

Kolloquium über Kombinatorik (Colloquium on Combinatorics), Braunschweig, Germany, November 17–18. A talk given by Patric R.J. Östergård (*Recent Existence and Nonexistence Results in Design Theory*).

December

ACCMCC (25th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing), Christchurch, New Zealand, December 4–8. A talk given by Kari J. Nurmela (*Lower bounds on 2-covering arrays by exhaustive search*).

4.2 Visits

Tuomas Aura visited Microsoft Research, Cambride, UK, on April 6–7.

Jan Elfström visited Mipro Oy, Mikkeli, Finland, on March 13.

Keijo Heljanko visited Technical University of Munich, Germany, on September 1 – October 31.

Nisse Husberg and Kimmo Varpaaniemi visited the Control and Automation Laboratory of Chalmers University of Technology, Gothenburg, Sweden, on September 22.

Ilkka Niemelä visited Technical University of Dresden, Germany, on June 5–8.

Kari J. Nurmela visited the Computer Engineering Laboratory of University of Oulu, Finland, on May 29–30.

Leo Ojala visited University of California at Berkeley, USA, for one day in July.

Teemu Tynjälä visited LAAS-CNRS, Toulouse, France, on December 11–20.

Patric R.J. Östergård visited University of Linköping, Sweden, on January 26–28.

4.3 Guests

Professor Pierre Azéma from LAAS-CNRS, Toulouse, France, stayed for five days, gave a talk (*Protocol Specification and Debugging by Message Sequences*) on February 25, and was hosted by Nisse Husberg.

Professor Simon Foley from University College Cork, Ireland, stayed for four days, was the opponent in the public examination of Tuomas Aura's doctoral dissertation on November 17, and was hosted by Ilkka Niemelä.

Stud.Tech. Marco Gaus (cf. 1.5) from Technical University of Clausthal, Germany, stayed for three months and was hosted by Ilkka Niemelä.

Pierre-Olivier Ribet from LAAS-CNRS, Toulouse, France, stayed for five days, gave a talk (*Some LAAS Tools Related to Petri Nets*) on December 8, and was hosted by Nisse Husberg.

D.Sc. (Tech.) Jussi Rintanen from Albert-Ludwigs-Universität Freiburg, Germany, stayed for five days, gave a talk (*Automated Reasoning with Quantified Boolean Formulae*) on October 11, and was hosted by Ilkka Niemelä.

Stud.Tech. André Schulz (cf. 1.5) from Brandenburg University of Technology Cottbus, Germany, stayed for five months, gave a talk (*Translation Rules from Standard SDL to* `MARIA` *Input Language*) on October 31, and was hosted by Nisse Husberg.

PhD E.M. Thurman from U.S. Geological Survey, USA, stayed for two days and was hosted by Kari J. Nurmela.

Professor Mirosław Truszczyński from University of Kentucky, USA, stayed for seven days, was the opponent in the public examination of Patrik Simons' doctoral dissertation on April 28, gave a talk (*Answer Set Programming and DATALOG with Constraints*) on May 2, and was hosted by Ilkka Niemelä.

5 PUBLICATIONS

5.1 Journal articles

[1] Tuomas Aura and Johan Lilius, "A causal semantics for time Petri nets," *Theoretical Computer Science*, Vol. 243, No. 1–2, pp. 409–447.
http://www.elsevier.nl/gej-ng/10/41/16/177/21/35/abstract.html

[2] Alexander Davydov and Patric R.J. Östergård, "New Quaternary Linear Codes with Covering Radius 2," *Finite Fields and Their Applications*, Vol. 6, No. 2, pp. 164–174.
http://www.idealibrary.com/links/doi/10.1006/ffta.1999.0271

[3] Alexander Davydov and Patric R.J. Östergård, "On Saturating Sets in Small Projective Geometries," *European Journal of Combinatorics*, Vol. 21, No. 5, pp. 563–570.
http://www.idealibrary.com/links/doi/10.1006/eujc.1999.0373

[4] T. Aaron Gulliver and Patric R.J. Östergård, "New binary linear codes," *Ars Combinatoria*, Vol. 56, No. 1, pp. 105–112.

[5] Filip Karlemo and Patric R.J. Östergård, "On sliding block puzzles," *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol. 34, No. 1, pp. 97–107.

[6] Timo Latvala and Keijo Heljanko, "Coping with Strong Fairness," *Fundamenta Informaticae*, Vol. 43, No. 1–4, pp. 175–193.

[7] Kari J. Nurmela, "Conjecturally optimal coverings of an equilateral triangle with up to 36 equal circles," *Experimental Mathematics*, Vol. 9, No. 1, pp. 241–250.

[8] Kimmo Varpaaniemi, "Stable Models for Stubborn Sets," *Fundamenta Informaticae*, Vol. 43, No. 1–4, pp. 355–375.

[9] Patric R.J. Östergård, "Classification of binary/ternary one-error-correcting codes," *Discrete Mathematics*, Vol. 223, No. 1–3, pp. 253–262. http://www.elsevier.nl/gej-ng/10/16/24/134/24/39/abstract.html

[10] Patric R.J. Östergård, "Enumeration of $2-(12,3,2)$ designs," *The Australasian Journal of Combinatorics*, Vol. 22, No. 1, pp. 227–231.

[11] Patric R.J. Östergård, "Computer search for small complete caps," *Journal of Geometry*, Vol. 69, No. 1–2, pp. 172–179.

[12] Patric R.J. Östergård and William D. Weakley, "Classification of binary covering codes," *Journal of Combinatorial Designs*, Vol. 8, No. 6, pp. 391–401. http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=73504489

5.2 Articles in collections

[13] Keijo Heljanko and Ilkka Niemelä, "Petri Net Analysis and Nonmonotonic Reasoning," in [50], pp. 7–19. http://www.tcs.hut.fi/%7ekepa/publications/hn-lncs.ps.gz

[14] Nisse Husberg, "30 Years: From Digital Filters to High Level Petri Nets," in [50], pp. 21–31.

[15] Tomi Janhunen, "Specifying Agent-Based Systems with Nets and Logic Programs," in [50], pp. 33–46.

[16] Eero Lassila, "On Tree Belts and Belt-Selectors," in [50], pp. 47–58.

[17] Marko Mäkelä, "`MARIA`: Modular Reachability Analyser for High-Level Petri Nets," in K.H. Mortensen (Ed.), *Petri Nets 2000: Tool Demonstrations*, University of Aarhus, Denmark, pp. 59–63.

[18] Marko Mäkelä, "Modular Reachability Analyser," in [50], pp. 75–85.

[19] Ilkka Niemelä and Patrik Simons, "Extending the `Smodels` system with cardinality and weight constraints," in J. Minker (Ed.), *Logic-Based Artificial Intelligence*, Kluwer Academic Publishers, Boston MA, USA, pp. 491–521.

[20] André Schulz and Teemu Tynjälä, "Translation Rules from Standard SDL to MARIA Input Language," in [50], pp. 105–114.

[21] Tommi Syrjänen, "Modelling the Game of Life using Logic Programs," in [50], pp. 115–124.
http://www.tcs.hut.fi/%7etssyrjan/publications/syrjanen_life.ps.gz

[22] Kimmo Varpaaniemi, "Modelling of a PLC-Based Railway Traffic Control System," in [50], pp. 131–140.
http://www.tcs.hut.fi/Publications/papers/kv181000.ps.gz

5.3 Conference papers

[23] Tuomas Aura, Matt Bishop, and Dean Sniegowski, "Analyzing single-server network inhibition," in *Proceedings of the 2000 IEEE Computer Security Foundations Workshop*, IEEE Computer Society Press, Los Alamitos CA, USA, pp. 108–117.

[24] Javier Esparza and Keijo Heljanko, "A New Unfolding Approach to LTL Model Checking," in U. Montanari, D. Rolim, and E. Welzl (Eds.), *Automata, Languages and Programming*, Lecture Notes in Computer Science, Vol. 1853, Springer-Verlag, Berlin, Germany, pp. 475–486.

[25] Keijo Heljanko, "Model Checking with Finite Complete Prefixes is PSPACE-Complete," in C. Palamidessi (Ed.), *CONCUR 2000 — Concurrency Theory*, Lecture Notes in Computer Science, Vol. 1877, Springer-Verlag, Berlin, Germany, pp. 108–122.
http://link.springer.de/link/service/series/0558/bibs/1877/18770108.htm

[26] Maarit Hietalahti, Fabio Massacci, and Ilkka Niemelä, "DES: a Challenge Problem for Nonmonotonic Reasoning Systems," in proceedings of the 8th International Workshop on Nonmonotonic Reasoning, Breckenridge CO, USA, April. http://xxx.lanl.gov/abs/cs.AI/0003039

[27] John R. Hughes, Tuomas Aura, and Matt Bishop, "Using conservation of flow as a security mechanism in network protocols," in *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos CA, USA, pp. 132–141.

[28] Nisse Husberg, Teemu Tynjälä, and Kimmo Varpaaniemi, "Modelling and Analysing the SDL Description of the ISDN-DSS1 Protocol," in M. Nielsen and D. Simpson (Eds.), *Application and Theory of Petri Nets 2000*, Lecture Notes in Computer Science, Vol. 1825, Springer-Verlag, Berlin, Germany, pp. 244–260.
http://link.springer.de/link/service/series/0558/bibs/1825/18250244.htm

[29] Tomi Janhunen, "Capturing Stationary and Regular Extensions with Reiter's Extensions," in M. Ojeda-Aciego, I.P. de Guzmán, G. Brewka, and L. Moniz Pereira (Eds.), *Logics in Artificial Intelligence: European Workshop, JELIA 2000*, Lecture Notes in Artificial

Intelligence, Vol. 1919, Springer-Verlag, Berlin, Germany, pp. 102–117. http://link.springer.de/link/service/series/0558/bibs/1919/19190102.htm

[30] Tomi Janhunen, "Comparing the Expressive Powers of Some Syntactically Restricted Classes of Logic Programs," in J. Lloyd, V. Dahl, U. Furbach, M. Kerber, K.-K. Lau, C. Palamidessi, L. Moniz Pereira, Y. Sagiv, and P.J. Stuckey (Eds.), *Computational Logic — CL 2000*, Lecture Notes in Artificial Intelligence, Vol. 1861, Springer-Verlag, Berlin, Germany, pp. 852–866. http://link.springer.de/link/service/series/0558/bibs/1861/18610852.htm

[31] Tomi Janhunen, Ilkka Niemelä, Patrik Simons, and Jia You, "Unfolding Partiality and Disjunctions in Stable Model Semantics," in A. Cohn, F. Giunchiglia, and B. Selman (Eds.), *Principles of Knowledge Representations and Reasoning: Proceedings of the 7th International Conference*, Morgan Kaufmann Publishers, San Francisco CA, USA, pp. 411–419.

[32] Tommi Junttila and Ilkka Niemelä, "Towards an Efficient Tableau Method for Boolean Circuit Satisfiability Checking," in J. Lloyd, V. Dahl, U. Furbach, M. Kerber, K.-K. Lau, C. Palamidessi, L. Moniz Pereira, Y. Sagiv, and P.J. Stuckey (Eds.), *Computational Logic — CL 2000*, Lecture Notes in Artificial Intelligence, Vol. 1861, Springer-Verlag, Berlin, Germany, pp. 553–567. http://link.springer.de/link/service/series/0558/bibs/1861/18610553.htm

[33] Teijo Kuoppala, Nisse Husberg, and Teemu Tynjälä, "Modelling and Analysis of TCN Standard Message Transport Protocol by Net-Theoretical Methods," in J. Lee, M. Juric, A. Bruzzone, D. Klovshy, and M. Fujita (Eds.), *SCI2000 Proceedings*, International Institute of Informatics and Systematics, Orlando FL, USA, pp. 661–667.

[34] Jussipekka Leiwo, Pekka Nikander, and Tuomas Aura, "Towards network denial of service resistant protocols," in S. Qing and J.H.P. Eloff (Eds.), *Information Security for Global Information Infrastructures*, IFIP Series, Vol. 175, Kluwer Academic Publishers, Boston MA, USA, 10 p.

[35] Marko Mäkelä, "Condensed Storage of Multi-Set Sequences," in K. Jensen (Ed.), *Practical Use of High-Level Petri Nets*, DAIMI PB-547, University of Aarhus, Denmark, pp. 111–125. http://www.daimi.au.dk/pn2000/proceedings/pn2000_hlpnworkshop.pdf

[36] Marko Mäkelä, "Modular Reachability Analyzer for High-Level Petri Nets," in R. Boel and G. Stremersch (Eds.), *Discrete Event Systems: Analysis and Control*, Series in Engineering and Computer Science, Vol. 569, Kluwer Academic Publishers, Boston MA, USA, pp. 477–478.

[37] Marko Mäkelä, "Applying Compiler Techniques to Reachability Analysis of High-Level Models," in H.-D. Burkhard, L. Czaja, A. Skowron, and P.H. Starke (Eds.), *Workshop: Concurrency,*

Specification & Programming, Volume 1, Humboldt-Universität zu Berlin, Informatik-Bericht Nr. 140, Berlin, Germany, pp. 129–141. http://www.tcs.hut.fi/%7emsmakela/papers/compiler.pdf

[38] Silja Mäki, Tuomas Aura, and Maarit Hietalahti, "Robust Membership Management for Ad-hoc Groups," in U. Erlingsson (Ed.), *NordSec 2000 — Proceedings of the Fifth Nordic Workshop on Secure IT Systems*, Reykjavik University, Iceland, pp. 151–168. http://www.tcs.hut.fi/Publications/papers/aura/maki-aura-hietalahti-nordsec00.pdf

[39] Ilkka Niemelä, Patrik Simons, and Tommi Syrjänen, "`Smodels`: A System for Answer Set Programming," in proceedings of the 8th International Workshop on Nonmonotonic Reasoning, Breckenridge CO, USA, April. http://xxx.lanl.gov/abs/cs.AI/0003033

[40] Leo Ojala, Nisse Husberg, and Teemu Tynjälä, "Modelling and Analysing a Distributed Dynamic Channel Allocation Algorithm for Mobile Computing Using High-Level Net Methods," in K. Jensen (Ed.), *Practical Use of High-Level Petri Nets*, DAIMI PB-547, University of Aarhus, Denmark, pp. 73–90. http://www.daimi.au.dk/pn2000/proceedings/pn2000_hlpnworkshop.pdf

[41] Leo Ojala, Nisse Husberg, and Teemu Tynjälä, "Modelling a Distributed Wireless Channel Allocation Algorithm for Cellular Systems with Mobile Base Stations Using Predicate/Transition Nets," in J. Lee, M. Juric, A. Bruzzone, D. Klovshy, and M. Fujita (Eds.), *SCI2000 Proceedings*, International Institute of Informatics and Systematics, Orlando FL, USA, pp. 678–683.

[42] Timo Soininen, Ilkka Niemelä, Juha Tiihonen, and Reijo Sulonen, "Unified Configuration Knowledge Representation Using Weight Constraint Rules," in proceedings of the Configuration Workshop in conjunction with the 14th European Conference on Artificial Intelligence, Berlin, Germany, August, pp. 79–84. http://www.cs.hut.fi/%7epdmg/ECAI2000WS/Proceedings.pdf

[43] Tommi Syrjänen, "Including Diagnostic Information in Configuration Models," in J. Lloyd, V. Dahl, U. Furbach, M. Kerber, K.-K. Lau, C. Palamidessi, L. Moniz Pereira, Y. Sagiv, and P.J. Stuckey (Eds.), *Computational Logic — CL 2000*, Lecture Notes in Artificial Intelligence, Vol. 1861, Springer-Verlag, Berlin, Germany, pp. 837–851. http://link.springer.de/link/service/series/0558/bibs/1861/18610837.htm

[44] Tommi Syrjänen, "Optimizing Configurations," in proceedings of the Configuration Workshop in conjunction with the 14th European Conference on Artificial Intelligence, Berlin, Germany, August, pp. 85–90. http://www.cs.hut.fi/%7epdmg/ECAI2000WS/Proceedings.pdf

[45] Heikki Tauriainen and Keijo Heljanko, "Testing SPIN's LTL Formula Conversion into Büchi Automata with Randomly Generated Input,"

in K. Havelund, J. Penix, and W. Visser (Eds.), *SPIN Model Checking and Software Verification*, Lecture Notes in Computer Science, Vol. 1885, Springer-Verlag, Berlin, Germany, pp. 54–72.

5.4 Research reports

[46] Tuomas Aura, *Authorization and Availability — Aspects of Open Network Security* (exactly the same publication as [55]), Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A64, Espoo, November, 42 p. http://www.tcs.hut.fi/Publications/papers/aura/HUT-TCS-A64.pdf

[47] Tuomas Aura and Carl Ellison, *Privacy and Accountability in Certificate Systems*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A61, Espoo, April, 17 p. http://www.tcs.hut.fi/Publications/papers/aura/HUT-TCS-A61.pdf

[48] Javier Esparza and Keijo Heljanko, *A New Unfolding Approach to LTL Model Checking*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A60, Espoo, April, 32 p. http://www.tcs.hut.fi/Publications/reports/A60.ps.gz

[49] Harri Haanpää, *Computational Methods for Ramsey Numbers* (essentially the same publication as [57]), Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A65, Espoo, November, 50 p.

[50] Nisse Husberg, Tomi Janhunen, and Ilkka Niemelä, *Leksa Notes in Computer Science: Festschrift in Honour of Professor Leo Ojala*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A63 (cf. 5.2), Espoo, October, 140 p.

[51] Tommi Junttila, *Computational Complexity of the Place/Transition-Net Symmetry Reduction Method*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A59, Espoo, April, 16 p. http://www.tcs.hut.fi/%7etjunttil/publications/Junttila_A59.pdf

[52] Kari J. Nurmela and Patric R.J. Östergård, *Covering a Square with up to 30 Equal Circles*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A62, Espoo, June, 14 p. http://www.tcs.hut.fi/Publications/reports/A62.ps.gz

[53] Patrik Simons, *Extending and Implementing the Stable Model Semantics* (exactly the same publication as [56]), Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A58, Espoo, April, 109 p. http://www.tcs.hut.fi/Publications/reports/A58.ps.gz

[54] Heikki Tauriainen, *Automated Testing of Büchi Automata Translators for Linear Temporal Logic* (essentially the same publication as [62]), Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Reports HUT-TCS-A66, Espoo, December, 86 p. http://www.tcs.hut.fi/Publications/reports/A66.pdf

5.5 Doctoral dissertations

[55] Tuomas Aura, *Authorization and Availability — Aspects of Open Network Security* (exactly the same publication as [46]). Publically examined on November 17. Accepted by Department of Computer Science and Engineering on December 4. Aura received the degree of D.Sc. (Tech.) on December 15.
http://www.tcs.hut.fi/Publications/papers/aura/HUT-TCS-A64.pdf

[56] Patrik Simons, *Extending and Implementing the Stable Model Semantics*, (exactly the same publication as [53]). Publically examined on April 28. Accepted by Department of Computer Science and Engineering on May 22. Simons received the degree of D.Sc. (Tech.) on May 22. http://www.tcs.hut.fi/Publications/reports/A58.ps.gz

5.6 Licentiate's theses

[57] Harri Haanpää, *Computational Methods for Ramsey Numbers* (essentially the same publication as [49]). Accepted by Department of Computer Science and Engineering on June 12. Haanpää received the degree of Lic.Sc. (Tech.) on June 12.

[58] Marko Mäkelä, *A Reachability Analyzer for Algebraic System Nets*. Accepted by Department of Computer Science and Engineering on April 10. Mäkelä received the degree of Lic.Sc. (Tech.) on April 10.
http://www.tcs.hut.fi/%7emsmakela/LicTech/rasn.pdf

5.7 Master's theses

[59] Mika Jalkanen, *Sales Statistics Process, Formal Specification and Implementation*. Accepted by Department of Computer Science and Engineering on August 28. Jalkanen received the degree of M.Sc. (Tech.) on September 1.

[60] Teijo Kuoppala, *Junan tiedonsiirtoverkkoon kuuluvien reaaliaikaprotokollien mallintaminen ja analysointi verkkoteoreettisin menetelmin*. Accepted by Department of Electrical and Communications Engineering on March 28. Kuoppala received the degree of M.Sc. (Tech.) on May 20.

[61] Timo Latvala, *Model Checking Linear Temporal Logic of Petri Nets with Fairness Constraints.* Accepted by Department of Electrical and Communications Engineering on October 17. Latvala received the degree of M.Sc. (Tech.) on October 17. http://www.tcs.hut.fi/%7etimo/master.ps.gz

[62] Heikki Tauriainen, *Automated Testing of Büchi Automata Translators for Linear Temporal Logic* (essentially the same publication as [54]). Accepted by Department of Computer Science and Engineering on October 30. Tauriainen received the degree of M.Sc. (Tech.) on October 30.

5.8 Software

[63] Lasse Anderson, Johannes Helander, Keijo Heljanko, Tomi Janhunen, Robert Jürgens, Ismo Kangas, Kari J. Nurmela, Kenneth Oksanen, Olavi Pesonen, Marko Rauhamaa, James Reilly, Heikki Suonsivu, Kimmo Valkealahti, Kimmo Varpaaniemi, and Pauli Väisänen, *PROD 3.3.08 — an advanced tool for efficient reachability analysis.* http://www.tcs.hut.fi/Software/prod/index.html

[64] Jan Elfström, Emil Falck, Teemu Hirsimäki, Petteri Kekäläinen, Timo Latvala, Marko Mäkelä, André Schulz, Teemu Tynjälä, and Kimmo Varpaaniemi, *MARIA — a modular reachability analyzer.* http://www.tcs.hut.fi/Software/maria/index.html

[65] Tommi Junttila, *BCSat — a satisfiability checker for Boolean circuits.* http://www.tcs.hut.fi/%7etjunttil/bcsat/index.html

[66] Patrik Simons, *Smodels-2.26 — a system for answer set programming.* http://www.tcs.hut.fi/Software/smodels/index.html

[67] Tommi Syrjänen, *lparse-1.0 — a local grounder for Smodels.* http://www.tcs.hut.fi/Software/smodels/lparse/index.html

[68] Heikki Tauriainen, *lbtt — a LTL-to-Büchi translator testbench.* http://www.tcs.hut.fi/%7ehtauriai/index.html

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2000