HELSINKI UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
DIGITAL SYSTEMS LABORATORY

Annual Report
May 1997

ANNUAL REPORT FOR THE YEAR 1996

edited by JOHAN LILIUS

Digital Systems Laboratory
Department of Computer Science and Engineering
Helsinki University of Technology
Otaniemi, FINLAND

Helsinki University of Technology
Department of Computer Science and Engineering
Digital Systems Laboratory
P.O. Box 1100
FIN–02015 HUT, FINLAND

HELSINKI UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DIGITAL SYSTEMS LABORATORY
Annual Report
May 1997

Annual Report for the Year 1996

edited by JOHAN LILIUS
Ass. Professor

Introduction:

This report describes the educational and research activities of the Digital Systems Laboratory at Helsinki University of Technology during the year 1996.

The educational and research activities of the Chair and of the Laboratory have recently been concentrated upon the areas: specification, modelling, and analysis of parallel and distributed digital systems and theoretical computer science.

Printing: Picaset Oy, 1998

Helsinki University of Technology
Department of Computer Science and Engineering
Digital Systems Laboratory
P.O. Box 1100
FIN–02015 HUT, FINLAND

Phone: +358–9–4511
Telefax: +358–9–465 077
E-mail: lab@saturn.hut.fi

Contents

1 Personnel

The university resources of the Chair consist of one *professor*, one *assistant professor*, one *teaching assistant*, a *laboratory manager*, and a *secretary*. A heavy load of the teaching tasks is also set to a large number of the students who, at the same time, are participating in the post-graduate education. The need of more permanent personnel resources for management, teaching, and research has been strongly felt during the whole history of the Chair.

1.1 University staff

Ojala, Leo	Prof.	Head of the Laboratory
Kangasniemi, Ulla	Mrs.	Laboratory Secretary
Niemelä, Ilkka	Dr.Tech.	Docent
Ukkonen, Esko	Prof.	Docent
Östergård, Patric	Dr.Tech.	Docent
Lilius, Johan	Dr.Tech.	Laboratory Manager on leave of absence 1.1.–31.12.
Sandqvist, Sam	Lic.Tech.	Laboratory Manager as substitute 1.1.–31.8.
Husberg, Nisse	Dr.Tech.	Laboratory Manager as substitute 1.9.–31.12.
Niemelä, Ilkka	Dr.Tech.	Assistant Professor on leave of absence 1.1–31.12.
Lilius, Johan	Dr.Tech.	Assistant Professor as substitute 1.1.–31.12.
Tiusanen, Mikko	Ph.D.	Assistant on leave of absence 1.1.–31.12.
Jyrinki, Tero	Stud.Tech.	Assistant as substitute 1.1.–28.2.
Penttinen, Olli-Matti	Stud.Tech.	Assistant as substitute 1.3.–31.8.
Malmqvist, Markus	Stud.Tech.	Assistant as substitute 1.3.–31.8.

1.2 Special lecturers

Heinonen, Rauno	Lic.Tech.	spring and autumn term
Kettunen, Esa	M.Sc.Eng.	spring and autumn term
Nikander, Pekka	M.Sc.Eng.	autumn term

also:

Aura, cf. 1.4	spring and autumn term
Janhunen, cf. 1.4	spring and autumn term
Lilius, cf. 1.1	autumn term
Nurmela, cf. 1.4	spring term
Sandqvist, cf. 1.1, 1.4	autumn term
Ukkonen, cf. 1.1	spring term

1.3 Part-time teaching assistants

Salmenkaita, Jukka-Pekka	Stud.Tech.	autumn term
Grönberg, Peter	Stud.Tech.	spring term

also:

Aura, cf. 1.4	spring and autumn term
Heljanko, cf. 1.4	spring and autumn term
Junttila, cf. 1.4	autumn term
Nikander, cf. 1.2	autumn term
Penttinen, cf. 1.4	spring term
Simons, cf. 1.4	spring and autumn term

1.4 Researchers

Aura, Tuomas	Stud.Tech.	Research assistant 1.1.–28.2.
	M.Sc.Eng	Researcher 1.3.–31.12.
Blom, Simo	Stud.Tech.	Research assistant 1.3.–31.12.
Heljanko, Keijo	Stud.Tech.	Research assistant 1.12.–31.12.
Husberg, Nisse	Dr.Tech.	Researcher 1.1.– 31.8. cf. also 1.1
Huima, Antti	Stud.Tech.	Research assistant 1.11.–31.12.
Janhunen, Tomi	Lic.Tech.	Researcher 1.1.–31.12.
Jyrinki, Tero	Stud.Tech.	Research assistant 1.3.–31.12.
Junttila, Tommi	Stud.Tech.	Research assistant 1.3.–31.12.
Lassila, Eero	M.Sc.Eng.	Researcher 1.1.–31.12.
Niemelä, Ilkka	Dr.Tech.	Junior Fellow of the Academy of Finland cf. also 1.1
Nurmela, Kari	Lic.Tech.	Researcher 1.1.–31.12.
Penttinen, Olli-Matti	Stud.Tech.	Research assistant 1.1.–28.2.
Rintanen, Jussi	Lic.Tech.	Researcher 1.6.–9.7.
Simons, Patrik	M.Sc.Tech.	Researcher 1.1.–31.12.
Schmidt, Karsten	Dr.Ing.	Researcher 1.11.–31.12.
Varpaaniemi, Kimmo	Lic.Tech.	Researcher 1.1.–8.7.
Östergård, Patric	Dr.Tech.	Senior Fellow of the Academy of Finland cf. also 1.1

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.

In the following list, for each course it is given in parentheses: the code according to the Study Programme of the University; the number of study credits (abbr. by *crt*, one crt signifies 40 hours of effective work), abbreviations *spt.*, *aut.*, and *N/A* express the spring term, autumn term, and non-availability during the calendar year, respectively; and the name(s) of the lecturer(s).

2.1 Theoretical computer science

Logic in Computer Science: Basics

(Tik-79.144; 2 crts, aut.; *Janhunen*)
Propositional and predicate calculus; syntax, semantics, and proof theory of these. Applications of logic in computer science, e.g. mechanical theorem proving and logic programming.

Logic in Computer Science: Special Topics

(Tik-79.145; 3 crts, spt.; *Janhunen*)
The basics of modal and epistemic logics: proof, model theory and decidability results. Nonmonotonic logics and their applications in computer science.

Introduction to Theoretical Computer Science

(Tik-79.148; 2 crts, aut.; *Heinonen*)
Basics of the theories of automata and formal languages. Computability theory. Principal limitations of computers.

Algorithms and Computability

(Tik-79.153; 2 crts, aut.; *Heinonen*)
Models of computation. Complexity theory. The principles of construction of algorithms. Classification and reducibility of problems. Decidability.

Formal Description of Computing Systems

(Tik-79.157; 2 crts, aut.; *Ojala*)
Logics of knowledge. Applications to telecommunications protocols and

distributed algorithms.

Cryptography and Data Security

(Tik-79.159; 3 crts, spt.; *Aura*)
Cryptographic algorithms and protocols. Strong encryption, authentication and electronic signatures, protocols for electronic trade. Design and analysis of cryptographic protocols. New directions in data security.

Student Project in Theoretical Computer Science

(Tik-79.189; 3 crts, spt. & aut.)
An independent study in the field of theoretical computer science.

Special Course on Theoretical Computer Science

(Tik-79.192; 2 crts, aut.; *Sandqvist*)
The course focuses on some current application of theoretical computer science. The topic varies from year to year. The topic in autumn 1996: The theory of genetic algorithms.

Seminar on Theoretical Computer Science

(Tik-79.194; 2 crts, spt.; *Ojala*)
Stochastic Petri nets and their applications

Seminar on theoretical Computer Science

(Tik-79.194; 3 crts, aut.; *Aura*)
Formal models of information security systems.

Postgraduate Course on Digital Systems Science

(Tik-79.198, 10 crts, spt. + aut.; *Ojala*)
Topics of the spring term: mathematical logic; model theory.

Topics of the autumn term: partial-order verification methods.

2.2 Parallel and distributed systems

Parallel and Distributed Digital Systems

(Tik-79.179; 3 crts, aut.; *Lilius*)
Introduction to net theory. Net classes, their properties and analysis techniques. Process algebra. Temporal Logic.

Parallel and Distributed Computation

(Tik-79.184; 3 crts, spt.; *Heljanko* and *Husberg*)
Formal specification and verification of parallel systems. Modelling and analysis of communication protocols. Partial analysis of reachability graphs.

Reactive Systems

(Tik-79.187; 3 crts, spt.; *Nurmela*)
Linear temporal logic in specification of distributed systems.

Formal Description Techniques for Concurrent Systems

(Tik-79.193; 2 crts, spt.; *Kettunen*)
Specification, validation, testing and analysis methods for large parallel, embedded, and real time systems. Specification languages LOTOS and SDL.

3 Research activities

The particular research topics and projects are described in the following subsections. In the descriptions the members of the research groups are given in parentheses, beginning with the leading or senior researcher.

3.1 Theoretical studies

Petri net research *(Ojala, Lilius, Varpaaniemi)*

- *Petri Net Semantics for Object-Oriented Languages* (Lilius)

  The translation from the object-based language OB(PN)^2 to a class of high-level Petri nets was was extended to include inheritance, dynamic dispatch and synchronisation constraints. The new language is called O^2(PN)^2 (Object-Oriented Basic Petrin Net Programming Notation). This translation defines the semantics of a OB(PN)^2 program as a net, which can then be analyzed using existing reachability analysis tools. The O^2(PN)^{2}language is an extension of B(PN)^2 as defined by Best and Hopkins, and the semantics is inspired by the B(PN)^2 ssemantics defined in terms of M-nets. The translation relies on the CCS-like composition operators defined for M-nets. Each program construct is translated to a box (a special kind of net) or an operation for combining boxes. Thus in essence each program is translated into an expression in the algebra of boxes.

- *Relieving the state space explosion* (Varpaaniemi)

The stubborn set method is one of the methods that try to relieve the state space explosion problem that occurs in state space generation. The verification of nexttime-less LTL (linear time temporal logic) formulas with the aid of the stubborn set method has been studied. In Valmari's presentation about stubborn sets in verification of nexttime-less LTL formulas, the computation of stubborn sets is directed by atomic formulas only, and the reduced state space can be used for verifying any nexttime-less LTL-formula that is constructible from those atomic formulas. Peled has improved the method by utilizing the structure of the formula and by making the technique fully compatible with fairness assumptions. However, Peled has utilized the structure of the formula only in cases when fairness is assumed or the formula expresses a safety property. Varpaaniemi has improved these approaches by utilizing the structure of the formula when no fairness is assumed and the formula is arbitrary.

Applications of logic in computer science and engineering *(Niemelä, Janhunen, Rintanen, Simons)*

The research has concentrated on knowledge representation and it has been focused on *nonmonotonic reasoning*, one of the key areas in knowledge representation. We have studied intensively automated deduction, semantics, as well as priorities and specificity in nonmonotonic reasoning.

- *Automating nonmonotonic reasoning* (Niemelä, Simons)

  This is a continuation of our earlier research where we have developed a framework for devising decision methods for nonmonotonic logics. We have employed the framework for developing (i) a new kind of a logic programming system implementing the stable model and well-founded semantics for normal logic programs and (ii) an efficient decision method for minimal model reasoning (circumscription) needed in implementing disjunctive logic programs.

  (i) Implementation of declarative semantics of logic programs (Niemelä, Simons)

  In recent years new declarative semantics for logic programming have been proposed but relative little work has been directed to developing implementations of the new semantics. Our aim is to make a serious attempt to implement the leading approaches for normal programs, i.e. the stable model and the well-founded semantics, with the main emphasis on the former one. In order to achieve as efficient an implementation as possible, we have adapted the Dowling-Gallier algorithm for computing deductive closures of Horn clauses to the special needs of stable model computation. The result is a simple implementation that employs powerful pruning techniques to find stable models in space proportional to the input. We have tested the implementation with a wide variety of test cases and compared it with a state of the art implementation of the stable model semantics, the SLG system. The tests show that for ground programs our implementation clearly outperforms SLG. The implementation is available at `http://saturn.hut.fi/pub/smodels/`.

(ii) Minimal model reasoning (Niemelä)

Minimal model reasoning plays an important role in disjunctive logic programs (dlps) because practically all semantics for dlps are generalizations of minimal model reasoning. The current state of the art in automating minimal model reasoning is not very satisfying because all proposed methods are based on an assumption that an exponential amount of memory (with respect to the program size) is available. We have overcome this problem by devising a novel characterization of minimal models which makes it possible to test whether a model is a minimal one independent of other models using one theorem prover call. This method has been integrated to a new kind of a tableau method, hyper-tableaux, which seems particularly suitable as a basis for minimal model reasoning. Now we are able to handle minimal model reasoning with very low space requirements, i.e., in the propositional case in linear space. This means that our method is able to cope with arbitrary size minimal model reasoning problems provided that enough computation time is allocated. This seems to the first such method. The method has been extended to handle very general forms of circumscription with fixed and minimized predicates. There is a prototype implementation available at `http://www.uni-koblenz.de/ag-ki/DLP/`.

The minimal model reasoning methods can handle positive dlps and our first goal in extending this to treat full dlps (with negation in the body) has been to develop an implementation of D-WFS semantics for dlps proposed by Brass and Dix. For this purpose we have devised an alternative characterization of D-WFS in terms of minimal models. It turns out that the notion of minimal models needed for D-WFS is close to standard circumscriptive models with minimized and fixed predicates but is more restricted. However, it seems that this more restricted type of minimal model reasoning can be implemented using the techniques that we have developed for circumscription.

- *Semantics of Non-monotonic Reasoning* (Janhunen)

This research continues earlier work on leading formalizations of non-monotonic reasoning such as McCarthy's circumscription, Reiter's default logic and Moore's autoepistemic logic that cover a wide range of applications. We have analyzed these logics and their variants in detail to find out (i) how easily knowledge is transformed from one logical representation into another and (ii) what these logics have in common.

The first objective has been approached by designing translation functions between non-monotonic theories such that the sets of conclusions associated with these theories (i.e. semantics) are preserved. The interconnection of default logic and autoepistemic logic has been of our central interest. This research has been fruitful in at least the following two ways. A novel translation of autoepistemic theories into default theories was found using the idea of representing autoepistemic introspection in terms of default rules. Moreover, we have devised a variant of autoepistemic logic based on separated modalities for belief and disbelief. This logic is well-behaving for translations of default theories into autoepistemic theories under Konolige's translation. This is in contrast to conventional autoepistemic logic where difficulties arise when Konolige's translation is used.

The second objective has led to the introduction of a meta-level specification of non-monotonic theories that covers the above mentioned three approaches. This framework provides the basis for our analysis of the semantics of non-monotonic reasoning. A variety of semantics such as *stable semantics* by Gelfond and Lifschitz, *stationary semantics* by Przymusinska and Przymusinski, *regular semantics* by You and Yuan, *stable class semantics* by Baral and Subrahmanian and *cautious semantics* by Janhunen can be uniformly defined starting from the specification directly and without a restriction to a particular non-monotonic theory. Most importantly, structural properties of these semantics such as cumulativity and computational complexity are also analyzable within the framework. We have especially contributed to the development and analysis of cautious semantics which is an interesting approximation between stable and stationary semantics.

- *Priorities in nonmonotonic reasoning* (Rintanen)

  The research is a continuation of earlier work on priorities in nonmonotonic reasoning. A major problem in representing knowledge is posed by the possibility of default rules that conflict. If the application of both of two default rules leads to a contradiction, they cannot both be applied. In such cases a reasoner may either remain indifferent or prioritize one rule over the other. If there is a conflict between a general default (that concerns the members of some class C) and a less general default (that concerns only a small subset of C), the less general default should be given a higher priority because it is more specific to the situation at hand. This – the specificity of default rules – is an important source of priorities, which has earlier been investigated in detail in the context of inheritance networks.

A priority mechanism that uses lexicographic comparison has been introduced to Reiter's default logic. This priority mechanism has been used as a basis for investigating the complexity of prioritized default reasoning, algorithms for automated default reasoning, and representation of inheritance reasoning in default logic. Also several embeddings of earlier systems of prioritized default reasoning in prioritized default logic have been devised.

Modern Heuristics in Optimization *(Östergård, Nurmela, Sandqvist)*

- *Stochastic Optimization and its Applications in Telecommunications* (Östergård, Nurmela)

  The aim of the research is to study new (combinatorial and global) stochastic optimization methods. These include methods such as simulated annealing, tabu search, and evolutionary algorithms. The methods have further been applied to a wide variety of problems, many of which are related to telecommunications. In the research, the performance of these and other optimization methods has also been evaluated.

  In particular, construction methods for different kinds of codes—for example covering codes, error-correcting codes, and constant-weight codes—have been developed. Some of these combinatorial and algebraic methods lead to good codes directly, while others turn code construction into an optimization problem, which then can be solved using any of the aforementioned stochastic methods. A multitude of new, record-breaking codes have been obtained.

  Many of the types of codes that have been studied have the property that they are coverings (covering codes) or packings (error-correcting codes) in the Hamming space. Recently, the approach has been carried over to coverings and packings in other spaces, for example, the Euclidean space. Whereas most code constructions are discrete optimization problems, in the Euclidean space we are mainly dealing with continuous functions. This has turned out to be a good testbed for applying methods primarily developed for discrete problems to continuous problems. Methods for finding good packings in Euclidean geometry have many practical applications; they can, for example, be used to optimize container stowage.

  Preliminary studies have been carried out on computer-aided constructions of other mathematical structures than those of the aforementioned types. Cross-connecting networks and routing problems in switching systems have also been considered within the framework of this research.

- *The Theory of Genetic Algorithms* (Sandqvist)

  This work extends the existing theoretical framework by applying logic to the modelling of the GA. The GA is characterised by two central concepts: that of evolution in time (temporal aspect), and that of Darwinian (or perhaps more often a combination of Lamarckian and Darwinian) selection of the fittest (with a stochastic aspect in selection). Using a combination of temporal logic, probabilistic logic and classical first-order logic a model of the genetic algorithm is being developed.

This model will provide useful and novel insights into e.g. the temporal evolution of the population so central to the GA. The formalism will also succintly describe the basic characteristics of the GA on a very abstract level: for instance, the mechanisms of crossover and mutation are independent of the formalism.

This work is a continuation of the Licentiate thesis (1993) of the author, and has been reported in e.g. the annual Nordic Workshop on GAs.

Abstraction mechanisms for optimizing code generation *(Lassila)*

Code generation for embedded special-purpose processors is a difficult task for compiler writers, and consequently the application programmers are often stuck with assembly language. The aim of our research is to develop powerful abstraction mechanisms for code generation. In particular, we concentrate on such assembly-level macro expansion techniques that support modular, freely hierarchical macro libraries to improve code readability, maintainability, and reusability.

In the case of macro systems, in general, it is often desirable that the final macro expansion result is independent of the expansion order of the recursively generated intermediate macro calls. This confluence property enables parallel implementation and guarantees that the effects of modifying a macro definition remain local. But the locality is also a problem: code optimization typically requires assembly-level macros to be sensitive to their context. For instance, they should know which registers are free and which ones contain useful values. A traditional mechanism for propagating contextual information is the use of global expansion-time variables. Relying on them, however, means that the expansion has to take place strictly from left to right, so that confluence is lost while it is still impossible to pass information in the opposite direction.

We are proposing a novel macro expansion scheme that is functional and specifically adjusted to the task of code synthesis. It offers both confluence and context-sensitivity, and it can be profitably combined with more conventional code generation and optimization techniques. As yet, we have devised a formal expansion model and implemented an elementary prototype of the suggested retargetable code generation tool.

Modelling information security systems *(Aura, Huima)*

The objective of the project is to develop formal modelling, analysis and development methods for information security systems. Logical proof-techniques and state-space analysis are widely used in development of secrecy and authentication systems. The current methods, however, lack rigorous semantic foundation and are applicable to limited ranges of problems. There is a clear industrial demand for design and quality assurance techniques in the area. The project began with analysis and development of mobile authentication protocols. This resulted in pending patent applications. Also, a prototype protocol analyzer was developed after a survey of the state of art in automatic verification. The present protocols lack rigorous protection against denial-of-service attacks. We studied the application of stateless protocols in systems with denial-of-service threats. Some work was done on information hiding in order to survey the limits of controlling information flows. Emphasis of future research will be on modelling of security of agent-based systems.

3.2 Technical projects

PROD 3.2 *(Varpaaniemi, Heljanko)*

The project continued the development of PROD, a high level Petri net reachability analysis tool. A new model checking algorithm for the branching time temporal logic CTL was designed and implemented. Also some new features were implemented to help the Emma analyzer to more efficiently interface with the PROD tool.

An algorithm for computing very small stubborn sets was designed and programmed, and results obtained from that algorithm were published in ISCIS-XI.

Broadband intelligent network application protocol (BINAP) *(Blom, Junttila)*

The rapid development of communication networks during the last decade has enabled the construction of broadband networks. Compared to the traditional narrowband networks, like the telephone network, more diversified services can be offered in the broadband networks. These services include especially different video-based services and other multimedia services. However, the broadband network alone is not sufficient to provide broadband services, but various enabling functions are needed. The broadband service enabling functions include e.g. navigation, charging and billing, restrictions and security functions. This work considers these most common broadband service enabling functions. One of the planned broadband service environments, the Digital Audio-Visual Council's DAVIC-architecture, is also introduced.

The Emma project *(Husberg, Jyrinki, Malmqvist, Penttinen)*

A dynamic analyzer Emma (Extendible Multi-Method Analyzer) was developed for TNSDL programs (TeleNokia SDL). It supports the detection of some errors related to parallelism and the investigation of their causes. The Emma analyzer is designed on top of Nokia's TNSDL translator and the PROD Pr/T net analyzer of the Digital Systems Laboratory. The user of Emma is working only on the the level of TNSDL.

Performance analysis of a video on demand system using stochastic Petri nets *(Pyssysalo, Ojala, Penttinen)*

The performance of an adaptive video on demand (VOD) system was studied using stochastic Petri nets. In this system channel resources are allocated more efficiently than well-known full VOD or near VOD systems. In adaptive VOD a video server does not notify users immediately it receives the requests, but after a time delay (delayed notification). This enables the server to accept more requests, because it can allocate one channel for several users (bunching property). The efficiency can be improved even more by using a proper rejecting strategy, where some requests are rejected, although there are channel resources available (refusal by choice). We give a system model for this adaptive VOD system using stochastic Petri nets. Discrete event simulation is used to determine the performance of the system; numerical performance indicators are computer using the software toolkit TimeNET.

4 Examinations and theses

4.1 Licentiate in Technology

Pyssysalo, Tino:	An Induction Theorem for Ring Protocols of Processes described using Predicate/Transiton Nets

4.2 Master of Science in Engineering

Aura, Tuomas:	Time Processes of Time Petri Nets
Nykänen, Asko:	Suomen kielen lauseenjäsennysympäristön suunnittelu ja toteutus (in Finnish)
Helme, Jukka:	Yhteyspohjaisten tietoliikenneprotokollien mallintamisesta ja analysoimisesta (in Finnish)
Salmi-Saarinen, Mervi:	A Study of Wireless Communication
Rautiainen, Aapo:	Conference Testing in a Distributed Testing Architechture

5 Awards

Tuomas Aura was granted the annual Pro Gradu award of the Finnish Society for Computer Science for a distinguished master's thesis in Computer Science.

6 Conferences, tours, and visits

6.1 Conferences and tours

Aura, Tuomas	Eurocrypt'96, Zaragoza Spain, 12.–16.5.1996.
	Workshop on Information Hiding, Cambridge UK, 30.5.–1.6.1996. (Presentation: Practical invisibility in digital communication.)
Heljanko, Keijo	CONCUR'96, August 1996, Pisa, Italy. (Presentation: PROD 3.1 - An Advanced Tool for Efficient Reachability Analysis.)
	Workshop on Concurrency, Specification Programming, Berlin, 25.–27.9.1996. (Presentation: Implementing a CTL Model Checker.)
	3rd Advanced Course on Petri Nets, Schloss Dagstuhl, Germany, 7.–18.10.1996. (Presentation: PROD 3.1 - An Advanced Tool for Efficient Reachability Analysis.)
Husberg, Nisse	Workshop on Concurrency, Specification Programming, Berlin, 25.–27.9.1996. (Presentation: SDL Modelling with High Level Petri Nets)
	8th Nordic Workshop on Programming Theory", Oslo 4.–6.12.1996. (Presentation: Formal Models for Real Programs.)
Janhunen, Tomi	University of Koblenz, Germany, June 1996. (Presentation: From the Relationship of Autoepistemic and Default Logics to a Meta-Level Specification for Non-Monotonic Theories.)
	ECAI-96 Workshop on Intregrating Nonmonotonicity in Automated Reasoning Systems, Budapest, Hungary, August 1996. (Presentation: On Abstracting Decision Procedures for Non-Monotonic Reasoning.)
	12th European Conference on Artificial Intelligence, Budapest, Hungary, August 1996. (Presen-

	tation: Representing Autoepistemic Introspection in Terms of Default Rules.)
	European Workshop, JELIA' 96, Evora, Portugal, September/October 1996.
Junttila, Tommi	Forte/PSTV'96 Joint International Conference Kaiserslautern, Germany, 8.–11.10.1996.
Jyrinki, Tero	8th Nordic Workshop on Programming Theory, Oslo 4.–6.12.1996.
Lassila, Eero	HeCSE Winter School. Stockholm, Sweden, 8.–10.1.1996. (Presentation: Code generation for embedded special-purpose processors.)
	The Second International Symposium on High-Performance Computer Architecture. San Jose, California, USA, 3.–7.2.1996.
	Workshop on Interaction between Compilers and Computer Architectures. San Jose, California, USA, 4.2.1996. (Presentation: A macro expansion approach to embedded processor code generation.)
	22nd Euromicro Conference. Prague, Czech Republic, 2.–5.9.1996 (Presentation: A macro expansion approach to embedded processor code generation.)
Lilius, Johan	Second Workshop on Object-Oriented Programming and Models of Concurrency, 24.6.1996, Osaka, Japan. (Presentation: OOB(PN)^2: An Object-Oriented Petri Net Programming Notation.)
	ICATPN-96, 23.6.–1.7.1996, Osaka, Japan
	Euro-Par'96, 26.–29.8.1996, Lyon, France. (Presentation: OB(PN)^2: An Object Based Petri Net Programming Notation.)
	Workshop on Concurrency, Specification Programming, Berlin, 25.–27.9.1996. (Presentation: Modelling Actors with M-Nets.)
	11th International Symposium on Computer and Information Sciences, Antalya, Turkey, 6.–8.11.1996. (Presentation: An M-Net Semantics for B(PN)^2 with Procedures.)

	20.11.1996, “OOB(PN)^2”, PROCOPE Project POEM (No. 95102) Workshop, LRI, University of Paris Sud, Orsay, France.
Malmqvist, Markus	8th Nordic Workshop on Programming Theory", Oslo 4.–6.12.1996.
Niemelä, Ilkka	Rheinische Friedrich-Wilhelms-Universität Bonn, Institut für Informatik, Bonn, Germany, 13.2.1996. (Presentation: Implementing Circumscription Using a Tableau Method)
	Fifth Workshop on Theorem Proving with Analytic Tableaux and Related Methods, Terrasini, Italy, 15.–17.5.1996. (Presentation: A Tableau Calculus for Minimal Model Reasoning)
	6th International Workshop on Nonmonotonic Reasoning, Timberline, Oregon, USA, 10.–12.6.1996. (Presentation: Nonmonotonic Reasoning and Complexity Results)
	Dagstuhl Seminar 9627: Disjunctive Logic Programming and Databases: Non-monotonic Aspects, Schloß Dagstuhl, Germany, 1.–5.7.1996. (Presentations: Towards Implementing DLPs using Hyper Tableaux, and Efficient Implementation of the Well-founded and Stable Model Semantics)
	12th European Conference on Artificial Intelligence, Budapest, Hungary, 12.–16.8.1996. (Presentation: Implementing Circumscription Using a Tableau Calculus)
	State University of New York at Stony Brook, Department of Computer Science, Stony Brook, 4.11.1996. (Presentation: Efficient Implementation of the Well-founded and Stable Model Semantics)
	Universität Bern, Institut für Informatik und angewandte Mathematik, Bern, Switzerland, 28.11.1996. (Presentation: Automated Deduction in Nonmonotonic Logics)
Nurmela, Kari	11th Midwestern Conference on Combinatorics, Cryptography, and Computing, Las Vegas, Nevada, 31.10–2.11.1996. (Presentation: Heuristic algorithms for constructing constant weight codes)

Ojala, Leo	Theoretical Aspects of Rationality and Knowledge, March 17–20 1996, Renesse, Holland. FCRC Conference, 21.–26.5.1996, Philadelphia, USA ICATPN-96, 23.6.–1.7.1996, Osaka, Japan FLOC-1996, 22.7.–2.8.1996, New Jersey, USA 3rd Advanced Course on Petri Nets, 7.–18.10.1996, Schloß Dagstuhl, Germany.
Sandqvist, Sam	AISB conference, Brighton, England, 1.–3.4.1996. 2nd Nordic Workshop on Genetic Algorithms, Vasa, Finland, 23.–24.8.1996. (Presentation: Some Aspects of Time in Genetic Algorithms.)
Schmidt, Karsten	Workshop on Concurrency, Specification & Programming, Berlin, 25.–27.9.1996. (Presentation: Siphons and Traps of algebraic Petri nets) Algorithmen und Werkzeuge für Petrinetze, Karlsruhe, 4.–5.10.1996. (Presentation: Ein Verfahren zur Verifikation von 'Immer Moeglich' und 'moeglich, dass immer'-Eigenschaften) Technische Universität Dresden, Institut für Informatik, 9.–13.11.1996. (Presentation: Wie ein symbolisches Analyseverfahren fuer algebraische High-Level-Netze entsteht)
Simons, Patrik	Joint International Conference and Symposium on Logic Programming, Bonn, September 1996 (Presentation: Efficient Implementation of the Well-founded and Stable Model Semantics)
Varpaaniemi, Kimmo	11th International Symposium on Computer and Information Sciences, Antalya, Turkey, 6.–8.11.1996. (Presentation: Finding Small Stubborn Sets Automatically.)
Östergård, Patric	8th Quadrennial International Conference on Graph Theory, Combinatorics, Algorithms, and Applications, Kalamazoo, Michigan, 3.–7.6.1996. (Presentation: Optimal packings of equal circles in a square.)

6.2 Visiting scholars

Nebel, Bernhard — Prof. Dr. Institut für Informatik, Albert-Ludwigs-Universität Freiburg. 19.–21.12.1996.

Schmidt, Karsten — Dr. Institut für Informatik, Humboldt-Universität zu Berlin. 1.5.–31.10.1996.

6.3 Visits

Niemelä, Ilkka — Acting Professor and visiting researcher, Universität Koblenz, Institut für Informatik, 1.1.–31.12.1996.

Rintanen, Jussi — Visiting reseracher, University of Texas at Austin, Department of Computer Sciences, 1.1.–31.5.1996.

Östergård, Patric — Visiting researcher, Discrete Mathematics group, Department of Mathematics and Computing Science, Eindhoven University of Technology, 1.1.–17.12.1996.

7 Documents

7.1 Journal articles

I. Niemelä: Autoepistemic Logic as a Basis for Automating Nonmonotonic Reasoning; Partiality, Modality and Non-monotonicity, Stanford, CA, 1996; pp. 251–289.

P. R. J. Östergård: A combinatorial proof for the football pool problem for six matches; Journal of Combinatorial Theory. Series A, 76(1996); pp. 160–163.

P. R. J. Östergård: The football pool problem; Congressus Numerantium, 114(1996); pp. 33–43.

P. R. J. Östergård and *M. K. Kaikkonen*: New single-error-correcting codes; IEEE Transactions on Information Theory, 42(1996); pp. 1261–1262.

7.2 Articles in collections

I. Niemelä: Autoepistemic Logic as a Basis for Automating Nonmonotonic Reasoning; Partiality, Modality and Non-monotonicity, Stanford, CA, 1996; pp. 251–289.

7.3 Edited books

I. Niemelä (ed): Proceedings of the ECAI'96 Workshop on Integrating Nonmonotonicity into Automated Reasoning Systems; Universität Koblenz-Landau, Fachbericht Informatik 18–96, August 1996.

7.4 Conference papers

C. Aravindan, *P. Baumgartner*, *J. Dix*, *U. Furbach*, *G. Neugebauer*, *I. Niemelä*, *D. Schäfer* and *F. Stolzenburg*: On Merging Theorem Proving and Logic Programming Paradigms; Proceedings of the Joint International Conference and Symposium on Logic Programming, Bonn, Germany, September 1996; 546 p.

C. Aravindan, *P. Baumgartner*, *J. Dix*, *U. Furbach*, *G. Neugebauer*, *I. Niemelä*, *D. Schäfer* and *F. Stolzenburg*: On Merging Theorem Proving and Logic Programming Paradigms; Proceedings of the Poster Session at JICSLP'96, Bonn, Germany, September 1996; pp. 99–122.

T. Aura: Practical invisibility in digital communication; Proc. 1st International Workshop on Information Hiding, Cambridge, England, May 1996.

P. Baumgartner, *U. Furbach* and *I. Niemelä*: Hyper Tableaux; Proceedings of the European Workshop on Logics in Artificial Intelligence (JELIA'96), Èvora, Portugal, September/October 1996; pp. 1–17.

K. Heljanko: Implementing a CTL Model Checker; Proceedings of the Fifth International Workshop on Concurrency, Specification & Programming (CSP), Berlin, Germany, September 25–27, 1996, Berlin, 1996; pp. 75–84.

N. Husberg: SDL Modelling with High Level Petri Nets; Proceedings of the Fifth International Workshop on Concurrency, Specification & Programming (CSP), Berlin, Germany, September 25–27, 1996, Berlin, 1996; pp. 85–96.

T. Janhunen: On Abstracting Decision Procedures for Non-Monotonic Reasoning; Proceedings of the ECAI'96 Workshop on Integrating Nonmonotonicity into Automated Reasoning Systems, Koblenz-Landau, August 1996; pp. 29–31.

T. Janhunen: Representing Autoepistemic Introspection in Terms of Default Rules; Proceedings of the 12th European Conference on Artificial Intelligence, ECAI-96, Budapest, Hungary, August 1996; pp. 70–74.

E. Lassila: A Macro Expansion Approach to Embedded Processor Code Generation; Proceedings of the 22nd EUROMICRO Conference, Prague, Czech Republic, September 1996; pp. 136–142.

J. Lilius: Modelling Actors with M-Nets; Workshop on Concurrency, Specification & Programming, Berlin, 1996.

J. Lilius: OB(PN)^2: An Object Based Petri Net Programming Notation; Proceedings of Euro-Par'96, Berlin, 1996; pp. 660–663.

J. Lilius: OOB(PN)^2: An Object-Oriented Petri Net Programming Notation; Proceedings of the Second Workshop on Object-Oriented Programming and Models of Concurrency, Osaka, June 24 1996.

J. Lilius and *E. Pelz*: An M-Net Semantics for B(PN)^2 with Procedures; Proceedings of the Eleventh International Symposium on Computer and Information Sciences, Antalya, Turkey, 1996; pp. 365–374.

I. Niemelä: Implementing Circumscription Using a Tableau Method; Proceedings of the European Conference on Artificial Intelligence, Budapest, Hungary, August 1996; pp. 80–84.

I. Niemelä: A Tableau Calculus for Minimal Model Reasoning; Proceedings of the Fifth Workshop on Theorem Proving with Analytic Tableaux and Related Methods, Terrasini, Italy, May 1996; pp. 278–294.

I. Niemelä and *P. Simons*: Efficient Implementation of the Well-founded and Stable Model Semantics; Proceedings of the 1996 Joint International Conference and Symposium on Logic Programming, Bonn, Germany, September 1996; pp. 289–303.

T. Pyssysalo and *L. Ojala*: Causal Modeling of a Video-on-Demand System Using Predicate/Transition Net Formalism; Proceedings of the 22nd EUROMICRO Conference, Prague, Czech Republic, September 1996; pp. 625–632.

K. Varpaaniemi: Finding Small Stubborn Sets Automatically; Proceedings of the Eleventh International Symposium on Computer and Information Sciences, Antalya, Turkey, 1996; pp. 133–142.

K. Varpaaniemi, *J. Lilius* and *K. Heljanko*: PROD 3.1 - An Advanced Tool for Efficient Reachability Analysis; Demos at Concur96, Technical Report, TR-96-29, Pisa, 1996; pp. 18–19.

7.5 Other Publications

P. Baumgartner, *U. Furbach* and *I. Niemelä*: Hyper Tableaux, Fachbericht Informatik 8–96, Universität Koblenz-Landau, 1996.

S. Brass, *J. Dix*, *I. Niemelä* and *T. C. Przymusinski*: A Comparison of STATIC Semantics with D-WFS, Fachbericht Informatik 2–96, Universität Koblenz-Landau, 1996.

I. Niemelä and *P. Simons*: Efficient Implementation of the Well-founded and Stable Model Semantics, Forschungsbericht 7–96, Universität Koblenz-Landau, 1996.

I. Niemelä: Implementing Circumscription Using a Tableau Method, Fachbericht Informatik 6–96, Universität Koblenz-Landau, 1996.

I. Niemelä: A Tableau Calculus for Minimal Model Reasoning, Fachbericht Informatik 5–96, Universität Koblenz-Landau, 1996.

7.6 Laboratory reports

J. Lilius (ed.): Annual Report for the Year 1995, August 1996, 18 p.

Series A: Research Reports

A38 *Tuomas Aura*: Time Processes of Time Petri Nets, 58 p.

A39 *Karsten Schmidt*: How to Calculate Symbolically Siphons and Traps for some Algebraic Petri nets, 40 p.

A40 *Tino Pyssysalo*, *Leo Ojala* and *Olli-Matti Penttinen*: Performance Analysis of a video on demand system using stochastic Petri nets, 11 p.

A41 *Jussi Rintanen*: Lexicographic Ordering as a Basis of Priorities in Default Reasoning, 187 p.

Series B: Technical Reports

B15 *Eero Lassila*: ReFlEx—An Experimental Tool for Special-Purpose Processor Code Generation, 79 p.