



510996

TYPES

Types for Proofs and Programs

Coordination Action  
FP6-2002-IST-C

Periodic activity report no 3  
revised version

**Period covered:** Aug 1, 2006 – Aug 31, 2007

**Date of preparation:** January 8, 2008

**Duration of project:** Sept 1, 2004 – April 30, 2008

**Coordinator:** Bengt Nordström, Chalmers University of Technology

# Contents

<b>1</b>	<b>Project objectives and major achievements</b>	<b>6</b>
1.1	Correctness of Computer Systems . . . . .	6
1.2	Formal Mathematics and Mathematics Education . . . . .	7
1.3	Proof Technology . . . . .	7
1.4	Foundational Research . . . . .	8
1.5	Relationship to other type-related research. . . . .	9
<b>2</b>	<b>Work-package progress and deliverables</b>	<b>10</b>
2.1	WP 1: Coordination and evaluation . . . . .	10
2.1.1	D3: periodic project reports . . . . .	10
2.2	WP 2: Types 2007 conference . . . . .	10
2.2.1	D6: The Udine meeting . . . . .	10
2.2.2	D9: Informal Types 2007 proceeding . . . . .	10
2.2.3	D11: Refereed Types 2006 Proceedings . . . . .	10
2.3	WP 3: Thematic workshops . . . . .	10
2.3.1	Small Workshop: CHIT/CHAT Nijmegen . . . . .	10
2.3.2	Small Workshop: Deep Inference Paris . . . . .	11
2.3.3	Small Workshop: Higher Order Rewriting (HOR '07) . . . . .	11
2.3.4	Small Workshop: Formal Topology . . . . .	11
2.3.5	Small Workshop: Proof Assistants and Types in Education . . . . .	11
2.3.6	Small Workshop: Type theory, proof theory and rewriting . . . . .	12
2.3.7	Small Workshop in honor of Gerard Huet . . . . .	12
2.4	WP4: Education . . . . .	13
2.4.1	Summer school . . . . .	13
2.4.2	Lecture notes of the summer school . . . . .	13
2.5	WP 5: Visits between sites . . . . .	14
2.6	WP 6: The Types web page and the mailing list . . . . .	21
2.6.1	D30 The www-site . . . . .	21
<b>3</b>	<b>Consortium management</b>	<b>22</b>
<b>4</b>	<b>Scientific collaboration inside the Types project</b>	<b>22</b>
<b>5</b>	<b>Involvement in other EU projects</b>	<b>28</b>
<b>6</b>	<b>Industrial cooperation</b>	<b>30</b>
<b>7</b>	<b>Coauthored papers and presentations</b>	<b>32</b>
<b>8</b>	<b>Major scientific results</b>	<b>35</b>
8.1	Chalmers . . . . .	35
8.2	Paris 7 . . . . .	36
8.3	Paris-Sud, Grenoble and France Telecom R&D . . . . .	37
8.4	TU München . . . . .	41
8.5	München LMU . . . . .	44
8.6	Nijmegen . . . . .	50
8.7	Białystok . . . . .	54
8.8	Royal Holloway, University of London . . . . .	55
8.9	Edinburgh . . . . .	57

8.10	Manchester	59
8.11	Torino	60
8.12	Udine and Padova	61
8.13	Warsaw	64
8.14	IoC Tallinn	66
8.15	Bergen	68
8.16	Helsinki	69
8.17	Savoie	70
8.18	Swansea	71
8.19	Toulouse	74
8.20	Birmingham	75
8.21	Nottingham	75
8.22	Kraków	77
8.23	Bamberg	78
8.24	Stockholm – Uppsala	78
8.25	Novi Sad - Belgrade	80
<b>A</b>	<b>Appendix 1 – Plan for using and disseminating the knowledge</b>	<b>81</b>
A.1	Exploitable knowledge and its Use	81
A.2	Dissemination of knowledge	81
A.3	Publishable results	82

## Summary of the Types project, 1.8.2006 – 31.8.2007

The aim of the research in the Types consortium is to develop the technology of formal reasoning and computer programming based on Type Theory. This is done by improving the languages and computerised tools for reasoning, and by applying the technology in several domains such as analysis of programming languages, certified software, formalisation of mathematics and mathematics education.

The funding for the Types project goes to coordination of and communications between research groups. The research itself is funded by other sources. The Types consortium receives funding for three annual meetings to communicate recent work throughout, at least six smaller thematic workshops on designated research themes, one summer school, short courses and short visits between sites. Thanks to a major redistribution of money during the previous reporting period, we have been able to prolong the action half a year. This has made it possible to arrange at least six additional small workshops, one extra summer school and one extra annual meeting.

The consortium is coordinated by Bengt Nordström (Chalmers University, Göteborg, Sweden) and consists of 35 research groups from universities and industries in Europe. It would have been unfeasible to let all groups be full participants in the action. In order to manage this, we have created a two-level hierarchy with 15 main sites (the contractors of the project) and 21 subsites (subcontractors). The following are the main sites: Chalmers, CNRS – Paris 7, INRIA-Futurs, INRIA-Sophia, Paris – Sud, München – LMU, München – TU, Nijmegen, Bialystok, Royal Holloway, Edinburgh, Manchester, Torino, Udine, Warsaw, Tallinn. The small sites are: Bergen, Helsinki, Stockholm/Uppsala, Minho, Padova, Bologna, Dassault-Aviation, Grenoble, France Telecom, Kent, Novi Sad, Krakow, Savoie, Swansea, Toulouse, Birmingham, Nottingham and Sheffield.

The main research areas of the consortium are the following:

- Correctness of Computer Systems: tools and techniques aimed specifically at application of formal methods to system correctness, e.g. programming language specific tools and problem-specific automation of proof search.
- Formal Mathematics and Mathematics Education: this is the prototype example for *proof in the large*, including very high level *mathematical vernacular* languages, the construction and use of necessarily large libraries of previous work, and distributed working on long-term projects.
- Proof Technology: the details of a proof checker, including unification, resolution, rewriting, general proof search, tactic languages and *declarative* proof languages.
- Foundational Research: underlying the previous three areas must be research on the expressiveness and relative correctness of the foundational logics, including syntax and semantics.

This is the third annual report. During this period we organized the Types 2007 Conference, a summer school, six small workshops and had many short visits between the sites.

**Types 2007 Conference.** The meeting took place in Udine, Italy. It attracted more than 100 participants and there were more than 60 regular presentations.

**Summer school.** The summer school took place in Bertinoro outside Bologna during two weeks in August 2007. There were 78 students.

**Small workshops** The following workshops were given:

- Small Workshop CHIT/CHAT Nijmegen, 18 -22 December, 2006
- Small Workshop on Deep Inference Paris, 1 - 2 December, 2006
- Higher Order Rewriting (HOR '07) Paris, June 25, 2007
- Small Workshop on Formal Topology Padova, 7 - 12 May, 2007
- Small Workshop Proof Assistants and Types in Education Paris, 25 June, 2007
- Small Workshop Type theory, proof theory and rewriting Paris, June 29, 2007
- Small Workshop in honor of Gerard Huet, Paris, June 22 – 23.

**Cooperation, visits and coauthored papers** The full report describes briefly 36 different cooperation activities inside the Types project. There were 15 refereed scientific papers with coauthors from different sites produced during the reporting period. In addition to this, there were 10 refereed coauthored conference contributions. There were around 90 visits between the sites (60 paid by the project). More than 60 talks were given.

**Industrial cooperation** There are at least 11 projects where the different research groups cooperates in industrial projects.

**The Types web page** The home page of the Types project can be found at [www.cs.chalmers.se/Cs/Research/Logic/Types/](http://www.cs.chalmers.se/Cs/Research/Logic/Types/)

**The Types mailing list** The types mailing list has now 271 members.

# 1 Project objectives and major achievements

The funding for the Types project goes to coordination of and communications between research groups. The research itself is funded by other sources.

We have divided our work in the following research areas:

1. Correctness of Computer Systems: tools and techniques aimed specifically at application of formal methods to system correctness, e.g. programming language specific tools and problem-specific automation of proof search.
2. Formal Mathematics and Mathematics Education: this is the prototype example for *proof in the large*, including very high level *mathematical vernacular* languages, the construction and use of necessarily large libraries of previous work, and distributed working on long-term projects.
3. Proof Technology: the details of proof, including unification, resolution, rewriting, general proof search, tactic languages and *declarative* proof languages.
4. Foundational Research: underlying the previous three areas must be research on the expressiveness and relative correctness of the foundational logics, including syntax, semantics, definitional mechanisms, allowed computation and sub-typing.

We will here briefly describe the most important results, a more detailed description of our work in these areas is found in section 8.

## 1.1 Correctness of Computer Systems

The "Why tool", is a generic tool developed by the Coq group that generates verification conditions in the logics of many proof tools (Coq, PVS, Isabelle/HOL, HOL 4, HOL Light and Mizar) and automated decision procedures (Simplify, Ergo, Yices, Z3, CVC Lite and haRVey). There are specialized front-ends for Why: "Krakatoa" to support verification of Java programs and "Caduceus" to support verification of C programs. These tools are freely available. There is an Eclipse plugin user environment for using Why/Caduceus/Krakatoa. Use of these tools has been taught at the TYPES Summer School 2007, and there is a web page with lecture notes, exercises and technical articles. New work on a more efficient intermediate language for translation into Why was reported in a workshop Programming Languages meets Program Verification 2007.

Coq is also being used in the MOBIUS project (IST-15905, including many TYPES sites, directed by INRIA Sophia-Antipolis) as the foundation for a system of proof carrying code (PCC) for Java. This is a large project, developing significant infrastructure to support resource, security and functional correctness of transmitted byte code. This is ongoing work, which is expected to lead to a feasible prototype PCC system for Java. This work was also presented at the TYPES Summer School 2007.

There were several talks on formally guaranteed correctness at the TYPES annual meeting (May 2007) including a Java Virtual Machine programmed in Coq, and ongoing work on a certified compiler for the language Lustre.

## 1.2 Formal Mathematics and Mathematics Education

Significant progress was made in Isabelle/HOL on formalizing Hales' proof of the Kepler conjecture. This work reduced the number of graphs that must be checked from 5128 to 2771, exemplifying the power of formal reasoning to be precise and concise as well as correct.

A team from INRIA, collaborating with Microsoft research is working on a general platform for mathematical components, based on the Coq "ssreflect" extension that was used to carry out the formalization of the Four Colour Theorem. This application of reflective proof is especially suited to type theory, and is also being pursued by the Isabelle group.

Correctness of efficient algorithms on triangular matrices in Coq was reported at TYPES 2007.

Both Mizar and Isabelle support archives of mathematical developments; Mizar's Mathematical Library, and its journal, Formalized Mathematics, is a serious start on an open-ended foundational formal development of mathematics.

In the area of type theory to support mathematics education, we have at least two prototype web interfaces to Coq, both designed specifically to support student use, and in use by students at Nijmegen and Nice. We held a workshop on Proof Assistants and Types in Education (June 2007) and another on web interfaces to proof tools, focusing on large scale distributed development, as required to construct a significant formalized curriculum in mathematics.

## 1.3 Proof Technology

Isabelle's declarative proof language "Isar" has made striking improvement this year. This is a formal language, inspired by the proof language of Mizar, designed to be readable by humans, and also to support human-style proof steps: "by induction", "case Successor", etc. This makes it easier to read, write, and maintain proofs. Mizar and Isar have been so successful that a similar language is in development for Coq. Both Coq and Isabelle/Isar use the generic Proof General interface, and there is ongoing work to implement a new Proof General as an Eclipse plugin, providing a modern interface environment with many new features supported by Eclipse.

The team of "Matita", a new proof tool from Bologna have done much work on modularity of proof developments, and construction, maintenance and searching of proof libraries. Matita has its own user-level proof language, but is foundationally largely compatible with Coq: compiled proof "object" files are interchangeable between Coq and Matita. Use of Matita was taught at the TYPES 2007 Summer School, and there is a Matita web page with a tutorial and examples. The Matita group research on modularity and subtyping was presented at TYPES 2007.

The Coq module system (inspired by the OCaml module system) has been in widespread use for several years. It is the most sophisticated module system in any prover, having functors as well as module structures, and was recently re-implemented for greater efficiency. Isabelle/Isar has also improved the modularity that it can express by improvements to its "locale" and "axiomatic type-class" notions.

There is extremely useful recent proof technology to support reasoning about programming languages, program semantics, and other systems with variable

binding. This has been a hot topic in the programming language community for about 3 years. (We held a TYPES topical workshop on binding in 2005.) The nominal logic package for Isabelle/HOL supports a notion of "datatypes with binding", having equality up-to alpha conversion. This package also automatically proves strong induction principles that are needed for reasoning about these datatypes, and conveniently provides other useful facilities. This is no longer experimental, but part of mainstream Isabelle/HOL distribution. There is also new work on representing binding in Coq (this also works in Isabelle and Matita) that depends on clever use of existing datatype technology. In fact these two new approaches to working with binding work well together, and this joint work has been reported in recent workshops and conferences. There is a challenge problem set on binding (the POPLmark Challenge) proposed by a group of programming language researchers in the USA; several solutions to the challenge problems have been submitted using the TYPES approaches mentioned, and checked in Coq, Isabelle and Matita.

Correct typechecking in the presence of meta-variables (like logic variables from logic programming) has been an outstanding problem in dependent types for years. The Chalmers group presented a re-implementation of the Agda proof tool with several new features, including a module system that is simple by design, and a proof of correct typechecking with meta-variables.

The group in Savoie is developing a new proof tool for a higher order logic over an ML-like programming language.

We held a TYPES topical workshop on type theory implementation techniques and interfaces for proof tools (Nov 2007).

## 1.4 Foundational Research

The relationship between intensional type theory and extensional type theory, and how to get the best of both in a single type theory, has long been an important problem for the use of type theory in programming and proving. (This problem is mentioned in our technical annex.) Recent work by the Nottingham group (reported at TYPES 2007) has made interesting progress on this very hard topic. This work includes the use of "universes" to provide generic programming in the type theory.

Our type theories support only total functions, and use some syntactic schema to capture the class of datatypes and functions that are acceptable. These syntactic schemas are more restrictive than semantically necessary, so the extension of such schemas, and the use of more general rewriting technology with sophisticated termination proofs has long been of interest. There were several talks on this topic at TYPES 2007, including a Coq library on rewriting and termination (invited talk from LORIA) and work from Warsaw on justifying new computation rules.

Another foundational topic that has received attention from TYPES is constructive analysis and exact real arithmetic. This is particularly relevant for computer programming, as computer programs inherently follow constructive logic, as in our type theories, not classical logic. Our work in this field goes back several years, and several talks at TYPES 2007 addressed this topic.

The group at Royal Holloway have been working with Aczel's notion of logic-enriched type theory: a type theory in which the mechanism for representing mathematical objects, and the mechanism for reasoning about those objects, are



rigidly separated. It is therefore possible to choose the logic and the collection of mathematical objects independently. The goal is to support type theory for different foundational schemes, including classical logic. Other work on logical frameworks with improved expressiveness was presented by the Udine group at TYPES 2007.

### **1.5 Relationship to other type-related research.**

The project has a strong focus on computer-assisted reasoning, this is clearly expressed in our project proposal and also clear from the full title of our project (Types for Proofs and Programs). The aim of the project is *not* to represent all major activities of “types” in Europe. There is a lot of work on types for conventional programming languages, concurrency, security, linguistics etc which is very interesting but not represented in this project. We want to keep our project focussed and relatively small.

We think it is important that we have an open atmosphere, this should hold for all scientific enterprises. All our meetings are widely announced and open to everybody, this includes our summer schools, the annual Types meetings, small workshops and individual visits.

## 2 Work-package progress and deliverables

All deliverables proposed for the third year are completed. The proceedings of the Types 2006 proceedings (D11) was sent to Brussels in October 2007, just in time for the review meeting. The current status of all deliverables for each work-package is described below.

### 2.1 WP 1: Coordination and evaluation

#### 2.1.1 D3: periodic project reports

This deliverable consists of this report and the project management report.

### 2.2 WP 2: Types 2007 conference

#### 2.2.1 D6: The Udine meeting

The annual conference of the Types project <http://users.dimi.uniud.it/types07> took place in Udine in the beginning of May 2007. There were 50 talks and 109 participants.

#### 2.2.2 D9: Informal Types 2007 proceeding

The electronic proceedings are available from the homepage of the meeting and also directly from <http://users.dimi.uniud.it/types07/programme.html>.

#### 2.2.3 D11: Refereed Types 2006 Proceedings

The Post-Proceedings of the Types 2006 Workshop were edited by Thorsten Altenkirch and Conor McBride. It is now published as the volume 4502 of the Lecture Notes in Computer Science (LNCS) series. The publishing house has sent out copies to the participants. Previous Types post-workshop proceedings include LNCS volumes 3839, 3085, 2646, 2277, 1657, 1512, 1158, 996 and 806.

More information about this volume can be found online at the web page [www.springer.com/978-3-540-74463-4](http://www.springer.com/978-3-540-74463-4).

### 2.3 WP 3: Thematic workshops

In the Description of Work, we promised to organize at least 6 workshops during the three years (deliverables D12 – D23). These workshops took place during the first two periods of the project and have been reported. During this period we organized seven additional workshops.

#### 2.3.1 Small Workshop: CHIT/CHAT Nijmegen

The workshop took place at the campus of the Radboud University in Nijmegen 18 -22 December, 2006. A programme with abstracts and slides is available at <http://hair-dryer.cs.ru.nl/typeschitchat/>.

This meeting consisted of two workshops. The CHIT Workshop aimed at gathering implementers of Curry-Howard based Theorem provers/Programming environments to discuss implementation issues. Its aim was to share isolated experience of development teams of those systems. The CHAT workshop focussed

on interaction between users and proof environments, graphical interfaces, and on network-based interaction.

### **2.3.2 Small Workshop: Deep Inference Paris**

This workshop gathered people interested in structural proof theory and especially in Deep Inference. Deep inference systems are deduction systems with rules applying directly to connectives arbitrary deep inside formulas, unlike sequent calculus or natural deduction where rules apply only to the main connectives. The programme with abstract and slides are available from the homepage <http://www.pps.jussieu.fr/eleph/swodi.html>. There were 26 participants and 11 presentations. The workshop took place in Paris 1 - 2 December, 2006.

### **2.3.3 Small Workshop: Higher Order Rewriting (HOR '07)**

HOR 2007 was a forum to present work concerning all aspects of higher-order rewriting. The following is a non-exhaustive list of topics for the workshop:

- Applications: proof checking, theorem proving, generic programming, declarative programming, program transformation.
- Foundations: pattern matching, unification, strategies, narrowing, termination, syntactic properties, type theory.
- Frameworks: term rewriting, conditional rewriting, graph rewriting, net rewriting, comparisons of different frameworks.
- Implementation: explicit substitution, rewriting tools, compilation techniques.
- Semantics: semantics of higher-order rewriting, higher-order abstract syntax.

The meeting took place in Paris June 25, 2007 and the program can be found at <http://www.lsv.ens-cachan.fr/rdp07/hor.html>

### **2.3.4 Small Workshop: Formal Topology**

This meeting took place in Padova 7 - 12 May, 2007. The workshop was preceded by two days of introductory lectures. The invited speakers were Peter Aczel (Manchester), Giovanni Curi (Padua), Nicola Gambino (Montreal), Hajime Ishihara (Kanazawa), Andre Joyal (Montreal), Martin Hyland (Cambridge), Maria Emilia Maietti (Padua), Per Martin-Löf (Stockholm), Christopher Mulvey (Sussex), Erik Palmgren (Uppsala), Giuseppe Rosolini (Genoa), Bas Spitters (Nijmegen), Paul Taylor (Manchester) and Steve Vickers (Birmingham). The programme can be found at <http://www.3wftop.math.unipd.it/>

### **2.3.5 Small Workshop: Proof Assistants and Types in Education**

This workshop took place in Paris on June 25 2007. The topics were

- type theory as a language for (teaching) mathematics and programming;

- computer assisted informal reasoning;
- tools and languages for teaching math and logic;
- experience in using proof assistants in class.

The programme can be found at <http://www.rdp07.org/pate.html>.

### **2.3.6 Small Workshop: Type theory, proof theory and rewriting**

The "Type theory, proof theory, and rewriting" was held in Paris on June 29th just after the conference "Rewriting Techniques and Applications". It aimed at being a place where researchers coming from the Types community and the rewriting community could meet.

The program committee was mixed including people from Types community (Negri, Dowek) and from the rewriting and the proof theory communities (Blanqui, Lipton, Okada). It included talks of Jim Lipton, Frédéric Blanqui, Jean-Pierre Jouannaud, Albert Rubio, Olivier Hermant, Michele Pagani, Lorenzo Tortora de Falco, Makoto Hamana, Thorsten Altenkirch, James Chapman, Ross Duncan, Nicolas Oury, Bruno Barras and Bruno Bernardo.

About thirty people attended the workshop and we are planning to organize a second workshop next year.

The program can be found at [www.lix.polytechnique.fr/~dowek/tpr.html](http://www.lix.polytechnique.fr/~dowek/tpr.html).

### **2.3.7 Small Workshop in honor of Gerard Huet**

The colloquium in Honor of Gérard Huet was held in École Normale Supérieure, in Paris on June 22th and 23th 2007. Thirteen talks were give by Robin Milner, Larry Paulson, Jean-Jacques Levy, Dominique Bolignano, Jean-Marie Hullor, Gordon Plotkin, Jean Vuillemin, Andre Hirschowitz, Rod Burstall, Aarne Ranta, Philippe de Groot and Christian Retoré. Gérard Huet has been one of the founders of the types community and several talks were given by people coming from various Type sites. The colloquium was organized by five former students of Gérard Huet : Thierry Coquand, Gilles Dowek, Francois Fages, Xavier Leroy, Christine Paulin, Didier Rémy. The audience was mixed and included people coming from various Type sites such as Cambridge, Edinburgh, Göteborg and Paris.

## 2.4 WP4: Education

### 2.4.1 Summer school

The Types Summer School 2007 took place at Bertinoro, Italy, on August 19-31, 2007. The two weeks' course was designed for postgraduate students, researchers and industrials with interest in interactive proof development. The present school followed the format of previous TYPES summer school (in Båstad 1993, Giens 1999, Giens 2002 and Göteborg 2005). There were introductory and advanced lectures on type theory, constructive topology, semantics, realizability, and proof carrying-code. Several talks were devoted to applications.

Most state-of-the-art proof assistants were presented during the school: Agda, Coq, Epigram, Isabelle, Matita and Mizar. Participants were given extensive opportunities to use and compare the tools, discovering their different features. A live-cd, containing pre-installed versions of all these systems has been produced and distributed to participants, and is still available for free downloading at the school home page (<http://typessummerschool07.cs.unibo.it/>).

The school had 75 students from 19 different countries all over the world (see the following table) confirming the high interest for the subject.

France	23
Italy	11
UK	11
Germany	9
USA	3
Poland	2
Portugal	2
Serbia	2
Argentina	1
Canada	1
Korea	1
Estonia	1
Finland	1
India	1
Ireland	1
Norway	1
Netherlands	1
Romania	1
Russia	1

There were 14 lecturers, among the top specialists in the world.

44 students received partial support for their expenses, mostly paid by money from the Types project (which also paid part of the expenses for a few lecturers).

### 2.4.2 Lecture notes of the summer school

The entire program, including material for the students like slides of the talks, lecture notes and proof systems are available from the home-page of the school (<http://typessummerschool07.cs.unibo.it/>).

## 2.5 WP 5: Visits between sites

We have had at least 81 visits between the sites, these are summarized in the tables on page 14 and 15. The tables do not include visits to workshops organized by Types. The visits marked (\*) have been paid by Types.

Table 1: List of visits between sites, part I:

From	To	Who
Bergen	Paris-Sud & INRIA Futurs	Bezem
Birmingham	Bamberg	Eike Ritter *
Birmingham	Padova	Vickers
Birmingham	Padova	Eike Ritter *
Birmingham	Padova	Escardo
Chalmers	Nijmegen	Bove*
Chalmers	Nottingham	Danielsson*
Chalmers	Nottingham	Dybjær
Chalmers	Nottingham	Norell*
Chalmers	Nottingham	Danielsson *
Edinburgh	Chalmers	Pollack
Edinburgh	TU München	Aspinall *
Edinburgh	Chambéry	Aspinall*
Edinburgh	INRIA Sophia-Antipolis	Aspinall
Edinburgh	INRIA Sophia-Antipolis	Jaroslav Ševčík
Edinburgh	Nijmegen	Stirling
Edinburgh	TU München	David Aspinall*
Edinburgh	TU München	James Cheney*
INRIA-Sophia	Chalmers	Yves Bertot*
LMU	Chalmers	Abel(August 07)
LMU	Chalmers	Abel (March 07) *
LMU	Chalmers	Abel (May 07)
LMU	Edinburgh	Urban (May 07)
LMU	Nijmegen	Schuster (June 07)
LMU	Nijmegen	Urban (Sep 06)
LMU	Swansea	Ratiu 3 visits, *
Manchester	LMU München	Aczel*
Minho	Tallinn	Pinto *
Minho	Tallinn	Pinto *
Nijmegen	Chalmers	Capretta *
Nijmegen	Chalmers	Spitters
Nijmegen	Chalmers	Wiedijk *
Nijmegen	INRIA Futurs	O'Connor *
Nijmegen	INRIA Sophia Antipolis	Niqui *
Nijmegen	TU München	Kaliszyk *
Nijmegen	Tallinn	Capretta *

The following is a list of talks given during some of the short visits:

1. Eike Ritter gave a talk in October 2006 in Padova entitled “Reductive Logic and proof-search: Proof Theory, Semantics and Control”. He also gave a talk in August 2007 in Bamberg entitled “A games model for classical proofs”.
2. Tarmo Uustalu visited Nijmegen 29 Oct.-4 Nov. 2006 and gave a talk “The many facets of structured (co)recursion” 30 Oct 2006.
3. Tarmo Uustalu visited Udine 18-25 Nov. 2006 and gave a talk “Type-systematic and foundational data-flow analysis” 23 Nov. 2006

Table 2: List of visits between sites, part II:

From	To	Who
Nottingham	Chalmers	Conor McBride *
Nottingham	Chalmers	James Chapman *
Nottingham	Paris-Sud & INRIA Futurs	Altenkirch
Nottingham	Tallinn	Altenkirch *
Novi Sad	Udine	Ghilezan *
Novi Sad	Udine	Ivetić *
Sheffield	Bamburgh	Stannett
Stockholm	Padova	Martin-Lof *
Swansea	Bergen	O'Reilly
Swansea	Bergen	Roggenbach *
Swansea	Bergen	Seisenberger
Swansea	LMU München	Berger *
Swansea	LMU München	Seisenberger *
Swansea	LMU München	Setzer *
Swansea	Nottingham	Setzer (*, Sept 2007)
Swansea	Royal Holloway	Setzer *
Swansea	TU München	Kahsai *
TU München	Paris-Sud & INRIA Futurs	Narboux
TU München	Swansea	Nipkow *
Tallinn	Nijmegen	Uustalu *
Tallinn	Nijmegen	Vene *
Tallinn	Nottingham	Uustalu*
Tallinn	Udine	Uustalu (twice)*
Tallinn	Nijmegen	Vene *
Torino	London	Dezani *
Torino	Paris	Coppo *
Torino	Paris	Dezani *
Torino	Paris	Fossati *
Torino	Paris	Gaboardi *
Torino	Paris	Giachino *
Torino	Paris	Piccolo *
Torino	Paris	de' Liguoro *
Torino	Paris	Giovannetti *
Torino	Udine	Berardi *
Torino	Warsaw	Bono *
Torino	Warsaw	Viviana Bono*
Toulouse	Braga (Minho)	Ralph Matthes *
Toulouse	Helsinki	Sergei Soloviev *
Toulouse	Paris	Ralph Matthes *
Toulouse	Royal Holloway	Sergei Soloviev *
Toulouse	Uppsala and Chalmers	Sergei Soloviev *
Toulouse	München	Ralph Matthes *
Udine	Bergen	Honsell
Udine	Bergen	Lenisa
Udine	Edinburgh	Honsell
Udine	Edinburgh	Lenisa
Udine	Padova	Di Gianantonio
Udine	Tallinn	Miculan
Uppsala	Padova	Palmgren *
Warsaw	Paris-Sud	Chrzęszcz
Warsaw	Paris-Sud	Walukiewicz
Warsaw	Chalmers	Marcin Benke*

4. Tarmo Uustalu visited Nottingham 13-22 May 2007, taught a 10 h course “Monads and more” 14-18 May 2007 and gave a talk “How to be firmly antifounded?” in Cambridge 17 May 2007
5. Tarmo Uustalu visited Udine 30 June-9 July 2007 and taught a 10 h course “Monads and more” 2-6 July 2007
6. Varmo Vene visited Nijmegen 2-8 July 2007 and gave a talk “Comonadic notions of computation” 3 July 2007
7. Marino Miculan visited Tallinn 11-18 March 2007 and gave a talk “From reactions to observations: the directed bigraphical model” 15 March 2007
8. Venanzio Capretta visited Tallinn 18-26 April 2007 and gave a talk “The path to computer mathematics” 19 April 2007
9. Thorsten Altenkirch visited Tallinn 22-27 April 2007 and gave a talk “Indexed containers” 26 April 2007
10. Luis Pinto visited Tallinn 29 July-3 Aug 2007 and gave a talk “Sequent calculus and extensions of lambda-calculus” 2 Aug 2007
11. David Aspinall from Edinburgh visited TU München; talk “The Future of Proof Engineering with Proof General”.
12. David Aspinall visited Chambéry; talk “The Future of Proof Engineering with Proof General”.
13. Peter Aczel visited LMU München, June 22 - 27, 2007 and gave a talk: ‘Type setups and logic-enriched type theories’
14. Yves Bertot gave a short course at Chalmers on June 4 – June 8, 2007. The title of the course was Programming Language Semantics in the Calculus of Inductive Constructions. There were around 20 students attending the lectures and around 10 of them passed the exam. The home page of the course is <http://groups.google.com/group/chalmers-cs-semantics-in-coq>
15. During his visit at Chalmers in August 2007, Venanzio Capretta gave a talk with the title “Common Knowledge as a Coinductive Modality”.
16. JavaMIP - Java with a modular initialization protocol: its core and a prototype. Viviana Bono, Warsaw, 26 Jan 2007.
17. "Termination checker for Agda 2", Marcin Benke, Chalmers, 29.9.2006
18. "Agda Compiler", Marcin Benke, Chalmers, 25.5.2007
19. During his visit to Tallin in April, Thorsten Altenkirch from Nottingham gave a talk on *Indexed Containers* at the Institute of Cybernetics in Tallinn.
20. Tarmo Uustalu (Tallinn) visited Nottingham in May 2007 and gave an intensive course on *Monads and more* to postgraduates and researchers in Nottingham.



21. During his visit to Paris Universite Denis Diderot in July 2007, Thorsten Altenkirch gave a talk at INRIA Futurs on *Normalisation by Completeness*.
22. Nils Anders Danielsson gave a talk with the title “A Well-typed Interpreter for a Dependently Typed Language” during his visit at Nottingham in February 2007.
23. M.E. Maietti gave a talk titled “Proofs as programs via logical principles”, at the University of Torino, on 18 October 2006.
24. Marino Miculan gave a talk titled “From reactions to observations: the directed bigraphical model”, during a visit at the Institute of Cybernetics, Tallinn, 11-18 March 2007.
25. Ralph Matthes gave the talk *On the importance of normalization for typed rewrite systems* in Univ. of Minho in the Seminar of the Centre of Mathematics.
26. In May 29 he gave the talk *Substitution - surprising challenges with inductive families* at the same place.
27. On June 23 in München (Workshop Proof and Computation II) he gave the talk *Continuation-passing style and strong normalisation for sequent calculi*.
28. A similar talk with 50 % overlap was also given on July 6 in Chambéry (Séminaires de logique du LAMA).
29. Sergei Soloviev gave the talk *Non-standard reductions in typed lambda-calculus with inductive types and normalization properties*. at LOGIK-SEMINARIET STOCKHOLM-UPPSALA, and at the seminar in Gotheborg, Chalmers University.
30. In June 2007, he gave the talk *Axiomatics and Evidence* at the University of Helsinki.
31. Henk Barendregt – Non-left linear reductions via infinitary lambda calculus. Symposium from Type Theory to Morphologic Complexity: 28-29 June 2007
32. Venanzio Capretta – Common Knowledge as a Coinductive Modality. Gotheborg August 2007
33. Venanzio Capretta – The path to Computer Mathematics, Tallin, April 2007.
34. Cezary Kaliszyk – Automating side conditions in formalized partial functions, TYPES Annual Meeting, Cividale del Friuli, Italy
35. Cezary Kaliszyk – Towards Wikis for Formalized Mathematics, PGIP meeting March 2007.
36. Ugo de’ Liguoro, Mariangiola Dezani and Mario Coppo from Torino visited Paris from March, 6 to March, 8 2007, and worked with Chantal Berline on types for mobiles and session types.

37. Piccolo from Torino visited Paris VII from April, 2 to April, 7 2007 to work with Claudia Faggian. By building on a previous work by Varacca and Yoshida, they interpreted processes of the Pi-calculus in typed linear strategies, that is the strategies introduced by Girard within the setting of Ludics. Then they proved that this model is fully complete and fully abstract w.r.t. the calculus. The output was a paper which was later accepted by TLCA 2007: Ludics is a Model for the Finitary Linear Pi-Calculus (pages 148-162 of the proceedings).
38. Luca Fossati from Torino visited Paris VII from February, 16 to February, 20 2007 to work with Pierre Louis-Curien to study the semantics of asynchronous typed processes using different approaches: Game Semantics, Typed Process Calculi, Petri Nets and Categories. The output was a paper "Automatic Parallelization of Sequential Specifications for Symmetric MPSoCs", published on IESS 2007 (pages 179-192).
39. Mariangiola Dezani visited London from March, 23 to March, 2007 to work with Steffen van Bakkel to work on the foundational properties of intersection type assignment.
40. Marco Gaboardi (Torino) visited Paris VII from April, 25 to May, 16 2007 and from May, 21 to June, 6 2007 to start a PhD thesis with Patrick Baillet. They studied a subsystem of second-order linear logic with restricted rules for exponentials, which is correct and complete for PTIME, designing a type assignment system in such a way that typable terms inherit subject reduction and normalization properties from the logical system. The output of this research work has been a paper "A Soft Type Assignment System for lambda -Calculus" published on CSL 2007.
41. Giovannetti Elio (Torino) visited Paris from June, 27 to July, 2 2007, , and worked with Chantal Berline on a mobility calculus with local and dependent types.
42. Dezani Mariangiola (Torino) visited Paris from June, 20 to June 24 2007, visited Giuseppe Castagna working on variants of the lambda calculus and the pi-calculus, characterized by rich typing and subtyping systems with union, negation, and intersection types.
43. Andreas Abel visited Chalmers from the 12th to the 21st of March and gave a talk on *Syntactical Normalization Proofs*.
44. James Cheney from Edinburgh visited TU München. Feb. 5–10 2007; talk on nominal techniques.
45. Bono Viviana from Torino visited Warsaw from 1/23 to 02/04/2007 and worked with Pawel and Jaroslaw about typing in Featherweight Java. They developed a modular way of initializing objects in Featherweight Java, avoiding duplication of code and unnecessary code dependencies. The output has been a paper with D. M. Kusmirek; "FJMIP: A Calculus for a Modular Object Initialization" in the proceedings of FCT 2007, pages 100-112.

46. Giachino Elena from Torino visited Nice and the University of Paris VII to develop her PhD thesis with Giuseppe Castagna on typing assignment for languages for the Web, from Jan., 22 to Jan., 27 2007. They developed a mechanism for dynamically extending object behaviors, by instantiating wrapper objects which are attached to basic entities dynamically at runtime. The output has been a paper published in SAC 2007, pages 1094-1100.
47. Ana Bove (Chalmers) – In the way of formalising the Odd-Even merge-sort algorithm, Nijmegen, November 2006.
48. Monika Seisenberger from Swansea visited LMU München June 22 - July 2, 2007 and gave two talks: “Applied Program Extraction” and “Coinduction and formalizing exact real numbers”.
49. Ulrich Berger from Swansea visited LMU München 22 - 23 June 2007 and gave a talk on “Forty years of provable recursion Applications of domain theory to termination problems”.
50. Anton Setzer from Swansea visited Royal Holloway 2 - 5 June 2007 and gave a talk on “Object-oriented programming in dependent type theory”.
51. Anton Setzer from Swansea visited Birmingham 1 - 2 June 2007 and gave a talk on “Inductive-recursive definitions and partial-recursive functions”.
52. Anton Setzer from Swansea visited Nottingham 6 - 11 September 2007 and gave on 7 September 2007 a talk on “Partial recursive functions and the recursion theorem in Martin-Löf Type Theory”.
53. Temesghen Kahasi from Swansea visited the TU München 13. - 16. August 2007. He was working on formalising the spi-calculus done under the supervision of Marino Miculan.
54. M Roggenbach from Swansea visited Magne Haveran in Bergen in August 2007. They collaborated on “Specifying with Theory Functors”.
55. Helmut Schwichtenberg from LMU München visited Swansea 12 - 15 April 2007 and gave a talk on “Computational content of indirect existence proofs”.
56. Trifon Trifonov from LMU München visited Swansea 12 - 15 April 2007 and gave a talk on “Finding Dialectica realizers for axioms”.
57. Tobias Nipkow from TU München visited Swansea 21 - 23 February 2007 and gave a talk on “Verifying a Hotel Key Card System”.
58. Olov Wilander from Uppsala visited Swansea and gave a talk on 19 June 2007 on “Universal algebras with lazy and partial functions”.
59. Diana Ratiu from LMU München visited Swansea 12 - 15 April 2007 and gave a talk on “Searching for Algorithms in Proofs of Existence of Groebner Bases”. She visited Swansea 13 - 27 November 2006 and gave a talk on 16 November 2006 on A-Translation - From Theory to Practice and Back.

60. Paul Taylor from Manchester visited Swansea and gave a talk on 28 November 2006 on "The definitive axiomatisation for ASD (maybe)".
61. Peter Schuster (LMU München) – Problems As Solutions, Swansea, June 2007
62. Varmo Vene (Tartu Estonia) – Comonadic notions of computation, Swansea, July 2007
63. Anton Setzer visited Royal Holloway in July 2007, giving a talk titled "Object-Oriented Programming in Dependent Type Theory".
64. Sergei Soloviev visited Royal Holloway in December 2006 and talked about coercive subtyping.

## 2.6 WP 6: The Types web page and the mailing list

### 2.6.1 D30 The www-site

The web page of the project is:

`www.cs.chalmers.se/Cs/Research/Logic/Types/`.

The page contains a short description of all research groups, a link to downloadable software, tutorials and lectures from the summer school. It also contains links to previous and coming events of the community and finally links to organizational matters.

The page is regularly updated to reflect the activities in the project. New activities are announced before they happen and reported after they happened.

The types mailing list is mainly used for announcements of types related activities and can be found at

`https://lists.chalmers.se/mailman/listinfo/types`

The mailing list now has 271 members.

### 3 Consortium management

Project management and coordination has been conducted without any friction. The steering group and the coordinator have regular exchange of emails and also meet during the Types conferences. During the Types conference there is an open business meeting discussing various organizational matters (such as suggestions for small workshops and the next Types meeting).

There have been no conflicts within the consortium.

The project has been extended 8 months, the final date is now April 30 2008.

### 4 Scientific collaboration inside the Types project

One of the main objectives of the Types project is to facilitate smooth cooperation between the entire Types community. The regular Types meetings and the small workshops are an important initial stimulus for this. In this section we will give some examples of further cooperation. The research has been partially supported by Types, either it was reported at a Types event or a Types-sponsored talk, meaning that Types supported the dissemination, or the results arose from work done during the visits between Types sites that took place during this or the previous period. The Types money has been essential for this kind of cooperation.

**Joint PhD supervision: INRIA – Chalmers, Savoie – Chalmers:** Arnaud Spiwack is a joint PhD student of Benjmain Werner (INRIA Futurs) and Thierry Coquand (Chalmers). He has written a joint paper with Thierry Coquand on algebraic topology in type theory, and another one on applying intersection types and domain theory to normalisation proofs (following U. Berger’s original insight).

Muhammad Humayoun started a PhD in February 2007 which is co-directed by C. Raffalli from Savoie and Aarne Ranta from Chalmers. The subject of the PhD is to use the GF grammatical framework of A. Ranta to be able to validate mathematical proofs or software specifications written in natural language. This is very important when teaching mathematics and when we writing norms, API or RFC for software, because we must use natural language and our text in natural language should be correct when compared with a formal version written using a specific proof assistant.

**Coq development: Paris Sud – Warsaw, Paris – Nijmegen – INRIA Sophia:** Jacek Chrząszcz and Daria Walukiewicz-Chrząszcz from Warsaw use Coccinelle and Cime (a Coq rewriting library and termination prover respectively) developed by the Paris-Sud site to propose a new way of proving inductive theorems in Coq, based on completeness of rewriting.

Roland Zumkeller from Inria Paris uses Russel O’Connor’s (Nijmegen) and Yves Bertot’s (Sophia) implementations of real numbers in Coq for his work on Hales’ proof of the Kepler conjecture. Also Niqui (Nijmegen) and Bertot cooperate on exact real arithmetic. More generally there is a deep interaction between these three teams on several cutting edge formal proofs efforts. O’Connor has visited Zumkeller in Paris. Niqui has visited Bertot in Sophia Antipolis.

Corbineau and Mamane from Nijmegen cooperate with the Coq team (Herbelin) on the further development of Coq and adding specific features. Both have made several contributions to the cvs version of Coq.

**Agda: Chalmers – Nottingham – Warsaw – LMU:** Marcin Benke (Warsaw) and Abel (LMU) cooperates with Norell and others from Chalmers on the development of the Agda proof assistant.

Conor McBride and James Chapman from Nottingham attended the Agda Implementors meeting in Göteborg in April 2007, exchanging ideas on implementing type-theoretic languages with implementors from Göteborg and Japan.

**Normalization by evaluation: Chalmers – LMU:** Andreas Abel and Klaus Aehlig (München LMU) have been collaborating with Peter Dybjer and Thierry Coquand (Chalmers) on normalization-by-evaluation for dependent types. Abel visited Chalmers twice for working meetings on this topic (March 12-21 and August 21-27), the first visit was paid by TYPES. The work resulted in two conference publications (MFPS XXIII and LiCS 2007).

**Type theory monograph: Chalmers – Uppsala – Swansea:** Collaboration of Anton Setzer (Swansea) with Peter Dybjer, Thierry Coquand (Göteborg, Chalmers) and Erik Palmgren (Uppsala) on writing a two volume monograph on dependent type theory. A draft version of volume 1 has been completed and sent to a publisher.

**Inductive recursive definitions 1: Nottingham – Swansea:** Collaboration of Anton Setzer (Swansea) with Peter Hancock, (Nottingham) on inductive-recursive definitions. Two research visit of A. Setzer at Nottingham were carried out as part of this project, apart from this the collaboration worked by email. This research has resulted up to now in 2 refereed and 3 non-refereed conference publications.

Another collaboration concerns categorical foundations of inductive-recursive definitions between Setzer and Peter Hancock and Neal Ghani (Nottingham). Two research visit of A. Setzer at Nottingham were carried out as part of this project, apart from this the collaboration was carried out by email. A joint larger EPSRC grant proposal is in preparation.

**Inductive recursive definitions 2: Chalmers – Uppsala – Swansea:** Collaboration of Anton Setzer (Swansea) with Peter Dybjer (Göteborg, Chalmers) on the theory and extensions of inductive-recursive definitions. This collaboration took place during two visits in Chalmers. It has resulted up to now in 2 journal publications and 3 refereed conference proceedings.

**General recursion: Chalmers – Nijmegen:** Venanzio Capretta (Nijmegen) and Ana Bove (Chalmers) continue working on how to represent partial and general recursive functions in Type Theory, which resulted in a joint paper presented at TLCA'07 with the title “Computation by Prophecy”. The work combines the advantages of the method based on inductive domain predicates and Venanzio’s work on general recursion via co-inductive types.

**Proof General: Edinburgh – TU München – Nijmegen Savoie:** The *Proof General* interface (David Aspinall et. al.) is widely used in the TYPES community. It is now redeveloped in *Eclips*, a modern framework for user interfaces, with many powerful new features. Markus Wenzel (TU) organized a workshop about the future development of the Proof General Interaction Protocol (PGIP), which took place on March 8 – 10, 2007 at TU München. At this workshop, David Aspinall and Christoph Lüth presented the latest version of Proof General based on the Eclipse Framework. Moreover, Cezary Kaliszyk gave a demonstration of his newly-developed, lightweight web interface for Isabelle.

David Aspinall visited Savoie from June the 14th to the 23rd to work on the possible use of the new version of Proof General with the new proof assistant PML which is currently being developed by Christophe Raffalli.

**Formalization of Mathematics: Manchester – Royal Holloway:** Peter Aczel from the Manchester site and Zhaohui Luo from the Royal Holloway site have collaborated in the UK EPSRC project Pythagoras (references GR/R84108 and GR/R84092), a three-year research project on formalisation of mathematics.

**Cryptography: Grenoble – INRIA – Paris Sud:** The sites in Grenoble, INRIA Sophia and Paris Sud are starting a new collaborative project on formal proofs of properties of computational cryptography. The platform will be based on the Coq proof assistant and in particular will use a modeling of randomized algorithms in Type Theory.

**Swansea – Chalmers:** Ulrich Berger from Swansea collaborated via email and discussions at the TYPES meeting, Udine 2007 with Thierry Coquand and Arnaud Spiwack from Chalmers (Göteborg) about domain theoretic methods for proving strong normalisation for lambda-calculi extended by rewriting and pattern matching.

**Swansea – LMU München:** Collaboration of Monika Seisenberger and Ulrich Berger from Swansea with Helmut Schwichtenberg and Diana Ratiu from LMU München on proof formalisation and program extraction in the areas of computable analysis, infinite combinatorics and Groebner base theory. This collaboration took place during a visit of Monika Seisenberger and Ulrich Berger at LMU München (22 June - 2 July 2007), a visit of Helmut Schwichtenberg and Diana Ratiu in Swansea, 13-14 April 2007, and two other visits (16 - 27 November 2006 and 16 - 21 September 2007) of Diana Ratiu in Swansea.

A second collaboration between these groups takes places between Ulrich Berger, Helmut Schwichtenberg, Pierre Letouzey (LMU München) and Stefan Berghofer (TU München) on program extraction from normalisation proofs (joint paper in *Studia Logica*, see below). This collaboration took place via email and during the visits of Ulrich Berger at LMU München and the visit of Schwichtenberg at Swansea mentioned in the previous paragraph.

**Swansea – Royal Holloway:** Collaboration of Anton Setzer (Swansea) with Z. Luo (Royal Holloway) on the integration of object-oriented concepts into dependent type theory. One research visit of A. Setzer at Royal Holloway was carried out as part of this project, apart from this the collaboration worked by



email. This research has resulted in 2 refereed conference proceedings. A larger joint EPSRC grant proposal is in preparation.

**Partiality: Nottingham – Tallinn – Nijmegen:** Collaboration with Thorsten Altenkirch (Nottingham), Tarmo Uustalu (Tallinn) and Venanzio Capretta (Nijmegen) on *Partiality as an effect*, facilitated by a joint visit of Capretta and Altenkirch to Tallinn in April 2007.

**Torino – Paris VII:** Mauro Piccolo, Luca Fossati, Marco Gaboardi and Elena Giachino started a PhD thesis in several topics of Type Theory, including Featherlight Java, typing mobiles, session types, light types of linear logic and dynamic re-typing for computation over the Web. They collaborated with a number of people including Patrick Baillot, Claudia Faggian, Giuseppe Castagna and P.L. Curien of Paris VII.

**Novi Sad – Torino:** M. Dezani-Ciancaglin, S. Ghilezan, J. Pantović work on a type system for the  $Xd\pi$  calculus, a calculus a distributed network of locations, where each location consists of both a data tree and a process. The type system is based on types for locations, data and processes, expressing security levels. It enjoys type preservation under reduction (subject reduction). They explore the use of types to model safe communication between processes and data.

**Novi Sad – INRIA:** H. Herbelin, S. Ghilezan design a  $\lambda\mu tp$ -calculus as a uniform framework for representing different calculi of delimited continuations. The type system proposed for  $\lambda\mu tp$ -calculus enjoys subject reduction. A classification of four calculi of delimited continuation is in focus of this work.

**Novi Sad – Braga:** J. Espirito-Santo (Minho), S. Ghilezan, J. Ivetić - An intersection type system is proposed for characterising strong normalisation in a term calculi for intuitionistic sequent logic.

**Birmingham – Bamberg:** Together with Michael Mandler from Bamberg Eike Ritter is investigating the completeness of certain Kripke models for modal logic. This work is relevant to the verification of hardware where the modal logic is used to model time constraints.

**Birmingham – Padova:** Ritter and Maietti from Padova are working on a Curry-Howard correspondence for a variant of linear type theory with double contexts, which is used in functional programming to model resource control. A fibrational semantics is the most natural way of modelling these double contexts.

**Chalmers – Bergen:** Marc Bezem and Thierry Coquand (Chalmers) have an ongoing cooperation on Coherent Logic with type-theoretic proof objects. This collaboration has resulted in a project called Automating Coherent Logic, funded by the Norwegian Science Council (NFR 177562).

**Warsaw – Torino:** Jarosław Kuśmierk (Warsaw) collaborates with Viviana Bono (Torino) on advanced features of object-oriented languages: mixin modules, better class initialization mechanisms, etc.

**Bergen – Paris Sud:** Marc Bezem was ‘rapporteur’ for the PhD thesis of Julien Narboux (Paris Sud, temporarily TU München). He was opponent at the graduation of Narboux on 26 September 2006.

**Manchester – LMU München:** Collaboration by email and during visits to München of Peter Aczel from Manchester with Peter Schuster from LMU München on the joint paper "Binary Refinement Implies Discrete Exponentiation", by Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren and Peter Schuster, in *Studia Logica* 84 (2006) 361-368.

**Manchester – Padova:** Collaboration by email and during various meetings of Peter Aczel from Manchester with Giovanni Curi from Padova on the joint paper “On the  $T_1$  Axiom and Other Separation Properties in Constructive Topology”, submitted to APAL, September, 2007.

**Udine – Padova – Tallinn – INRIA:** People in Udine and Padova have continued the collaborations with other sites, initiated in the previous periods. In particular, this was supported by a visit by Miculan to Tallinn, and two visits of Uustalu to Udine, in this reporting period. Also the collaboration with Luigi Liquori, from the site of INRIA Sophia-Antipolis, has been endorsed. The workshop organized in Padova during this reporting period has been an occasion for strengthening the collaborations with Eike Ritter, Steve Vickers (University of Birmingham), P. Martin-Löf (University of Stockholm), and others. Also the collaboration with Edinburgh has been strengthened by the visits of Honsell and Lenisa; moreover, their visit to Bergen can be seen as a first step towards a new collaboration.

**Toulouse – Minho – Helsinki:** The group in Toulouse has a collaboration with Minho site (Braga, Portugal) facilitated by visits by R. Matthes (resulting in joint publication) and S. Soloviev (financed by another project, but presenting a talk on non-standard reduction related to main directions of foundational research within “Types”). They have also a collaboration with Jan von Plato and Sara Negri (Helsinki) facilitated by a visit of Sergei Soloviev to Helsinki in June 2007.

**Toulouse – Royal Holloway:** The Toulouse group also has a collaboration with Zhaohui Luo (Royal Holloway) facilitated by a visit of Sergei Soloveiv to Egham (Royal Holloway) in December 2006. (This is a continued collaboration on the subject of coercive subtyping.)

**Chalmers – LMU:** Peter Schuster (München LMU) is developing constructive mathematics with Thierry Coquand (Chalmers) and Erik Palmgren (Uppsala).

**Chalmers – Bergen:** Marc Bezem (Bergen) and Thierry Coquand (Chalmers) have an ongoing cooperation on Coherent Logic with type-theoretic proof objects.

**Chalmers – Nijmegen:** Spitters (Nijmegen) and Coquand (Chalmers) have also a cooperation which has resulted in a joint publication.

**Edinburgh – TU München :** Randy Pollack (Edinburgh) and Christian Urban (TU München) are collaborating on using Isabelle to formalise binding syntax. They have a joint workshop paper at “Workshop on Mechanizing Metatheory, 2007”.

**Royal Holloway – Toulouse:** Zhaohui Luo from the Royal Holloway site and Sergei Soloviev from the Toulouse site have worked collaboratively on application of coercive subtyping to linguistic semantics.

**Tallinn – Nijmegen:** T. Uustalu, V. Vene, V. Capretta worked on antifounded corecursion.

**Tallinn – Udine:** T. Uustalu, M. Miculan collaborated on the categorical theory of contexts and variable binding.

**Tallinn – Minho:** T. Uustalu and L. Pinto collaborated on the structural proof theory of bi-intuitionistic logic.

Several sites within Types (Nijmegen, INRIA, Bologna, Edinburgh, TU München, Chambéry, Białystok) are working on a joint EU Strep proposal.

## 5 Involvement in other EU projects

The sites are also participating in other European projects. The Types money is not used for this activity, but it is an important part of the overall activity of the Types consortium.

1. *MOBIUS, Mobility Ubiquity and Security* (Chalmers, Edinburgh, LMU – München, Tallinn, INRIA, Nijmegen, Warsaw) - an integrated project to develop the technology for establishing trust and security for the next generation of global computers, using the Proof Carrying Code paradigm. The Coq type theory proof assistant (from Types partner INRIA) is the main proof system for this project, although Isabelle (from Types partner TUM – München) is also being used. This is related to our research area Correctness of Computer Systems.
2. *EmBounded* (München LMU) The aims of the EmBounded Project are to identify, to quantify and to certify resource-bounded code in Hume, a domain-specific high-level programming language for real-time embedded systems. Using formal models of resource consumption as a basis, the project will develop static analyses for time and space consumption and assess these against realistic applications for embedded systems. The work is novel in combining analyses of both source and machine code into a single framework.
3. Manchester participates in Mathlogapps (MATHematical LOGic and APplicationS), <http://www.maths.manchester.ac.uk/logic/mathlogaps/>. MATHLOGAPS is an Early Stage Research Training project involving the Universities of Leeds, Manchester, Lyon (Lyon 1 and the Ecole Normale Supérieure) and München (LMU). Mathlogapps shares with Types the sites Manchester and München and is used to finance research visits of PhD and MSc Research students between the Types sites München and Manchester.
4. *CiE* (München LMU) Computability In Europe, a network of mathematicians, logicians, computer scientists, philosophers, theoretical physicists and others interested in new developments in computability. This is also related to our area Foundational Research.
5. Nottingham participates in the STREP on *Quantum Information and Computation* (QUICS) as a subsite of Oxford. Nottingham's emphasis is on using type-theoretic methods to provide a high-level interface to a hypothetical quantum computer, the Quantum IO monad.
6. *ALFA/LerNet* (Chalmers) The group is involved in the ALFA (Latin America Academic Training) network LerNet (Language Engineering and Rigorous Software Development). ALFA is a programme of cooperation between higher education institutions of the European Union and Latin America.
7. *EmBounded* (München LMU) The aims of the EmBounded Project are to identify, to quantify and to certify resource-bounded code in Hume, a domain-specific high-level programming language for real-time embedded

systems. Using formal models of resource consumption as a basis, the project will develop static analyses for time and space consumption and assess these against realistic applications for embedded systems. The work is novel in combining analyses of both source and machine code into a single framework.

8. *MATHLOGAPS* (LMU – München) - a multi-participant Early Stage Research Training program between universities in Leeds, Manchester, Lyon and München to fund young researchers in the area of the mathematical logic and its applications. This is related to our area Foundational Research.
9. *CiE* (LMU – München) - Computability In Europe, a network of mathematicians, logicians, computer scientists, philosophers, theoretical physicists and others interested in new developments in computability. This is also related to our area Foundational Research. The annual CiE conference has been hosted by the Types site Swansea in 2006.

## 6 Industrial cooperation

The different sites have cooperation with industry of varying degree. This cooperation is never paid by the Types project, but it is an important part of our activity.

The site in *Paris-Sud* is collaborating with Dassault Aviation and France Telecom R&D in the area of proofs of C programs. They also have a collaboration with the Gemalto company (a smart-cards manufacturer) on proofs of Java and C programs, Java card applets. Th. Hubert (Dassault), N. Rousset (Axalto), Y. Moy (France telecom R&D) are studying for their PhD part-time in the industry and part-time in the university. The tools designed for verification of imperative programs use type theory both as a foundational model for the semantics of programs and also as a back-end for solving proof obligations which cannot be solved automatically.

*Warsaw* collaborates with Comarch Research Center of Comarch SA (a Polish software company), on the introduction of extended typing tools to the industrial software engineering process. The collaboration resulted in several research papers so far. The results were also used by Comarch in the tools employed in the development of an experimental GenRap Report Generator application, integrated recently with the Comarch CDN Opt!ma industrial ERP system.

The Coq proof assistant has been used by Gemalto in a Common Criteria (CC) evaluation on a Java Card based commercial product. This evaluation will lead to the world's first CC certificate of a Java product involving EAL7 components.

The site in *Toulouse* participate in the project "TOPCASED" (collaboration with "Airbus", "Astrium" and other industrial partners) as part of the research team "Acadie" at IRIT. The project uses Type Theory (in particular, the language Coq) in its specification and verification tools.

The site in *Bergen* has industrial cooperation in the Norwegian project SHIP (NFR 176853) which has a subproject devoted to the application of type theory to software correctness and security issues. The companies involved are Intelinet AS and Cellvision AS.

*Chalmers* cooperates with Japan's National Institute of Advanced Industrial Science and Technology (AIST) on the development and application of the proof environment Agda. AIST, in turn, is strongly focused on industrial cooperation. The Agda system is the latest of the proof assistants developed in Chalmers inside the Types project. Anton Setzer from Swansea visited AIST in November 2006 twice and participated at the Agda implementors meeting, 23 - 30 May 2007 in Göteborg and the Agda review meeting, 26 - 27 September 2007. He is supervising on PhD student who is working on the implementation of coalgebras in Agda.

The *München LMU* site is cooperating with AbsInt GmbH, Saarbrücken, in order to provide time bounds of machine code on the M32C embedded system processor. These low-level bounds are input to the high-level program analysis for Hume developed by the München LMU site. The aim of this cooperation is to obtain sharp worst-case estimations of resource usage of embedded computer systems.

The *TU München* site is involved in the project *Verisoft* funded by the German Ministry of Education and Research (BMBF). The main goal of the

project is the pervasive formal verification of computer systems (such as those used e.g. in automotive engineering). We are closely cooperating with *OneSpin Solutions* (the former hardware verification division of Infineon), which is one of the industry partners involved in the project. As a part of this cooperation, the Isabelle/Isar proof language has been extended with additional specification methods that allow to formalize large proofs about properties of microprocessors in a modular way.

In *Swansea*, Anton Setzer has together with Faron Moller, started a collaboration with the Invensys Rail System (<http://www.invensysrail.com/>) on the verification of railway interlocking systems. After a visit of Invesys to Swansea the company agreed to fund two MRes Studentships at Swansea in the academic year 2007/08, of which one will be supervised by Anton Setzer.

Also in *Swansea*, Markus Roggenbach and Andy Gimblett are contuing their collaborating with Holger Schlingloff (Berlin) and the company Zuehlke (Zürich, Switzerland). They are working on formalizing the electronic payment standard EP2, a new international standard for which first terminals are just beeing installed, in the formal specification language CSP-CASL.

*Belgrad* cooperates with Telekom Srbija in the area of proofs and security.

## 7 Coauthored papers and presentations

Collaborations between researchers in the consortium are taking place in many forms. People are visiting each other, meeting in workshops and exchanging emails. Some of this activity leads to joint publications. Here is a list of some cooperations between people from different groups in the Types project. These papers are also included in section 8, which contains all Types-related publications for each site. Here, we do not list articles and talks given at a meeting organized by Types.

### Books

1. Peter Schuster, ‘Trends in Constructive Mathematics.’ Selected papers (with J. Berger, D. Pattinson, J. Zappe, eds.). *Math. Log. Quart.* (2008) [special issue], accepted

### Refereed journal papers

1. Venanzio Capretta, Tarmo Uustalu, and Varmo Vene. Recursive coalgebras from comonads. *Information and Computation*, 204(4):437–468, April 2006
2. Andreas Abel and Thierry Coquand. Untyped algorithmic equality for Martin-Löf’s logical framework with surjective pairs. *Fundamenta Informaticae*, 77(4):345–395, 2007. TLCA’05 special issue
3. Peter Schuster, ‘Apartness and formal topology’ (with E. Palmgren). *New Zealand J. Math.* 35 (2006) 77-84
4. Peter Schuster, ‘Binary refinement implies discrete exponentiation’ (with P. Aczel, L. Crosilla, H. Ishihara, E. Palmgren). *Studia Logica* 84 (2006) 361–368
5. Peter Schuster, ‘The projective spectrum as a distributive lattice’ (with T. Coquand, H. Lombardi). *Cah. Topol. Géom. Différ. Catég.*, accepted
6. Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, 82:27–51, 2006
7. Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren and Peter Schuster. Binary Refinement Implies Discrete Exponentiation. *Studia Logica* 84 (2006) 361-368.
8. F. Kamareddine et K. Nour A completeness result for a realisability semantics for an intersection type system. *Annals of Pure and Applied Logic*, vol 146, pp. 180-198, 2007.
9. Franco Barbanera, Michele Bugliesi, Mariangiola Dezani-Ciancaglini and Vladimiro Sassone: "Space-Aware Ambients and Processes" *Theoretical Computer Science* Vol. 373 N. 1-2 p. 41–69, 2007.



10. Mario Coppo, Mariangiola Dezani-Ciancaglini and Elio Giovannetti: "Types for Ambient and Process Mobility" *Mathematical Structures in Computer Science*, 2007, to appear.
11. Pablo Garralda, Eduardo Bonelli, Adriana Compagnoni and Mariangiola Dezani-Ciancaglini: "Boxed Ambients with Communication Interfaces" *Journal MSCS Volume 17* p. 1–59, 2007
12. Davide Ancona, Christopher Anderson, Ferruccio Damiani, Sophia Drossopoulou, Paola Giannini and Elena Zucca: "A provenly correct translation of Fickle into Java" *Journal ACM Transactions On Programming Languages and Systems* Vol. 29 N. 2 Page(s), 2007
13. M.Dezani-Ciancaglini, S. Ghilezan, J. Pantović: "Security types for dynamic web data", *Trustworthy Global Computing TGC 2006*, (R. Bruni, U. Montanari, D. Sannella, eds) *Lecture Notes in Computer Science* 4661 (2007) pp 263–280.
14. V. Bono, J. Kuśmierek, Modularizing constructors, *Journal of Object Technology*, vol. 6, no. 9, Special Issue. *TOOLS EUROPE 2007*, October 2007, pp. 297-317.
15. J. Kuśmierek, V. Bono, Introducing HygJava, *Journal of Object Technology*, vol. 6, no. 9, Special Issue. *TOOLS EUROPE 2007*, October 2007, pp. 209-229.

#### Refereed conference papers

1. Ana Bove and Venanzio Capretta. Computation by prophecy. In *Typed Lambda Calculi and Applications, TLCA 2007*, volume 4583 of *LNCS*, pages 70–83. Springer, 2007
2. A. Bove and V. Capretta. Computation by prophecy. In *Typed Lambda Calculi and Applications TLCA '07*, *LNCS* 4583, pages 70–83, June 2007
3. Patrik Jansson, Johan Jeuring, and students of the Utrecht University Generic Programming class. Testing properties of generic functions. In Zoltan Horvath, editor, *Proceedings of IFL 2006*, volume 4449 of *LNCS*, pages 217–234. Springer-Verlag, 2007
4. Andreas Abel, Thierry Coquand, and Peter Dybjer. Normalization by evaluation for martin-löf type theory with equality judgements. In *Proceedings of 22nd IEEE Annual Symposium on Logic in Computer Science, Wroclaw, Poland, July 2007.*, 2007
5. Andreas Abel, Klaus Aehlig, and Peter Dybjer. Normalization by evaluation for martin-löf type theory with one universe. In *Mathematical Foundations of Programming Semantics, New Orleans, LA, USA, April 2007. Ed. M. Fiore. Electronic Notes in Theoretical Computer Science, Elsevier.*, volume 173, pages 17–40, 2007
6. Christian Urban and Randy Pollack. Strong induction principles in the locally nameless representation of binders (preliminary notes). Presented at (ACM) Workshop on Mechanizing Metatheory, 2007

7. Andreas Abel, Thierry Coquand, and Peter Dybjer. Normalization by evaluation for Martin-Löf Type Theory with typed equality judgements. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12 July 2007, Wrocław, Poland, Proceedings*, pages 3–12. IEEE Computer Society Press, 2007
8. Andreas Abel, Klaus Aehlig, and Peter Dybjer. Normalization by evaluation for Martin-Löf type theory with one universe. In Marcelo Fiore, editor, *Proceedings of the 23rd Conference on the Mathematical Foundations of Programming Semantics (MFPS XXIII), New Orleans, LA, USA, 11-14 April 2007*, volume 173 of *Electronic Notes in Theoretical Computer Science*, pages 17–39. Elsevier, 2007
9. C. Urban and R. Pollack. Strong Induction Principles in the Locally Nameless Representation of Binders (Preliminary Notes). In *Proc. of the Workshop on Mechanizing Meta-Theory, 2007*
10. V. Bono, J. Kuśmierek "FJMIP: a calculus for a modular objectinitialization", In Proc. FCT 2007 pp. 100-112, LNCS 4639

## Talks

1. Ana Bove and Venanzio Capretta, Computation by Prophecy, TLCA 2007, Paris 2007.
2. Andreas Abel, Thierry Coquand, and Peter Dybjer, Normalization by Evaluation for Martin-Löf Type Theory with Typed Equality Judgements, 10 July 2007. Logic in Computer Science, LiCS 2007, Wrocław, Poland.
3. Eike Ritter. Reductive Logic and Proof-search: Proof Theory, Semantics and Control. Talk given in Padova, 2006.
4. Eike Ritter. A games model for classical proofs. Talk given in Bamberg, August 2007.
5. V. Bono and J. Kuśmierek gave a talk “Hygienic methods - Introducing HygJava” at TOOLS EUROPE 2007 conference in Zürich
6. V. Bono and J. Kuśmierek gave a talk “Modularizing constructors” at TOOLS EUROPE 2007 conference in Zürich
7. T. Uustalu, talk How to be firmly antifounded (coauthors V. Capretta, V. Vene), Fun in the afternoon, Cambridge, 18 May 2007

## 8 Major scientific results

We have asked each site to briefly describe their main scientific results, divided into the the main topics of our research:

- Correctness of Computer Systems
- Foundational Research
- Formal Mathematics and Mathematics Education
- Proof Technology

The sites have also included a list of published papers in a Types-related area. Papers with authors from more than one site have also been reported in section 7.

### 8.1 Chalmers

Ulf Norell defended his PhD thesis "Towards a practical programming language based on dependent type theory". The thesis describes the new version of the Agda language geared towards dependently typed programming. A main feature is a flexible treatment of pattern matching over inductive families.

Nils Anders Danielsson showed how a dependently typed language can be encoded in a well-typed way, without raw terms. The work was published in the TYPES 2006 proceedings.

#### Publications

##### Refereed journal papers

1. Thierry Coquand and Henri Lombardi. A logical approach to abstract algebra. *Mathematical Structures in Computer Science*, 16(5):885–900, 2006
2. Thierry Coquand. On seminormality. *Journal of Algebra*, 305(1):577–584, 2006

##### Refereed conference papers

1. Nils Anders Danielsson. A formalisation of a dependently typed language as an inductive-recursive family. In *Types for Proofs and Programs, International Workshop, TYPES 2006, Revised Selected Papers*, volume 4502 of *LNCS*, pages 93–109. Springer-Verlag, 2007
2. Nils Anders Danielsson. Lightweight semiformal time complexity analysis for purely functional data structures. Accepted for publication in POPL '08: Conference record of the 35th ACM SIGPLAN-SIGACT symposium on Principles of programming languages, 2008
3. Alexandre Buisse and Peter Dybjer. Towards formalizing categorical models of type theory in type theory. In *Second International Workshop on Logical Frameworks and Metalanguages: Theory and Practice (LFMTP'07)*, *Electronic Notes in Theoretical Computer Science*, Elsevier, pages 72–85, 2007

4. Fredrik Lindblad. Higher-order proof construction based on first-order narrowing. In *Second International Workshop on Logical Frameworks and Metalanguages: Theory and Practice (LFMTP'07)*, *Electronic Notes in Theoretical Computer Science*, Elsevier, 2007

## Dissertations

1. Ulf Norell. *Towards a practical programming language based on dependent type theory*. PhD thesis, Department of Computer Science and Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden, September 2007
2. David Wahlstedt. *Dependent Type Theory with Parameterized First-Order Data Types and Well-Founded Recursion*. PhD thesis, Chalmers University of Technology, 2007. ISBN 978-91-7291-979-2

## 8.2 Paris 7

**Correctness of Computer Systems** J.L. Krivine et Y. Legrandg erard introduced a new method for specifying network protocols, using games on valid first-order formulas. It is more compact and powerful than usual languages based on automata and allows to obtain correct protocols. The protocol is described as a game between two players - sender and receiver - associated to a formula, which constitutes the specification of the protocol.

**Foundational Research** M. Parigot introduced a logic of constructivity K which, unlike intuitionistic logic, allows to deal with constructivity in a classical setting. The logic K is an extension of classical logic with constructive connectives - a constructive disjunction and a constructive existential quantifier - whose statements freely mix constructive and classical connectives. It allows to use classical reasoning for proving constructive properties.

V. Mogbil gave a proofs-as-programs correspondence between proof nets and deterministic as well as non-deterministic Boolean circuits with a uniform depth-preserving simulation of each other and obtained a Curry-Howard characterization of the complexity class NC (the efficiently parallelizable functions), P and NP in term of proof nets classes based on Multiplicative and Additive Linear Logic.

V. Atassi and P. Baillot have continued with Terui (Tokyo) the study of type inference in a system derived from linear logic (DLAL) and ensuring polynomial time bounds on system F lambda terms. Together with Coppola (Udine) and Dal Lago (Bologna / Paris 13), Baillot has also studied optimal reduction (in the sense of L avy-Lamping) for the lambda terms typable in Light linear logic (or DLAL) and shown that it could be performed in polynomial time .

C. Berline proved with G. Manzonetto important particular cases of a general conjecture she made before: the equational theory of a model of pure of lambda-calculus living in a Scott semantics or in a refinement of it can not be recursively enumerable.

Delia Kesner revisited the theory of explicit substitutions. She used a very simple technology to establish a general theory of explicit substitutions for the

lambda-calculus which enjoys fundamental properties such as simulation of one-step beta-reduction, confluence on metaterms, preservation of beta-strong normalisation, strong normalisation of typed terms and full composition.

### **Formal Mathematics and Mathematics Education**

**Proof technology** P. Letouzey contributed to the Coq proof assistant with extension of the standard libraries (finite sets, rational numbers, etc.) He also contributed to the study of the extraction mechanism.

### **Publications**

#### **Refereed journal papers**

1. C. Berline, A. Salibra. Easiness in graph models, *Theor. Comput. Science* 354 (2006) 4-23.
2. C. Berline. Graph models of lambda-calculus at work, and variations, *Math. Struct. for Comput. Sci.* (2006), vol.16, pp. 185-221.

#### **Refereed conference papers**

1. Paulin Jacobé de Naurois and Virgile Mogbil. Correctness of multiplicative (and exponential) proof structures in NL-complete. *proceedings CSL'07*, LNCS 4646, pp. 435-450, 2007.
2. Virgile Mogbil and Vincent Rahli. Uniform circuits & Boolean proof nets. *proceedings LFCS'07*, LNCS 4514, pp. 401-421, 2007.
3. Patrick Baillot, Paolo Coppola, Ugo Dal Lago. Light Logics and Optimal Reduction: Completeness and Complexity. *Proceedings LICS 2007*, pp 421-430, 2007.
4. Patrick Baillot. From Proof-Nets to Linear Logic Type Systems for Polynomial Time Computing. *Proceedings TLCA'07*, LNCS 4583, pp. 2-7, 2007.
5. Vincent Atassi, Patrick Baillot, Kazushige Terui. Verification of Ptime Reducibility for system F Terms via Dual Light Affine Logic. *Proceedings CSL'06*, LNCS 4207, pp.150-166, 2006.
6. Delia Kesner. The Theory of Explicit Substitutions Revisited. *Proceedings CSL'07*, LNCS 4646, pages 238-252, 2007.

### **8.3 Paris-Sud, Grenoble and France Telecom R&D**

The Paris-Sud, Grenoble and France telecom R& D are mainly working on the topics of Correctness of Computer Systems and automated deduction.

## Correctness of Computer Systems

**Proving C or Java programs** Paris-Sud designs a general platform "Why" [68] (see <http://why.lri.fr>) for analysing imperative sequential programs in particular written in C (see <http://caduceus.lri.fr>) and Java (see <http://krakatoa.lri.fr>) using deductive verification. This platform uses type theory for modeling programs and specifications and also for proving proof obligations. The verification conditions can be generated for several existing provers, including interactive proof assistants (Coq, PVS, HOL Light, Mizar) and automatic provers (Simplify, haRVey, CVC Lite).

France Telecom R& D is mainly interested by a automatic analysis of memory properties in C code [108, 107].

**Reasoning on functional programs** M. Sozeau supervised by C. Paulin, designed a language with a subset type (in the spirit of the PVS language) which is convenient for programming with dependent types. He proposed a translation of a term in this language to a Coq term containing existential variables corresponding to type-checking conditions. This feature is integrated in the Coq distribution and has been used for the development of a certified library on finger trees [129, 131, 130].

**Reasoning on randomized programs** C. Paulin together with Ph. Audebaud proposed a method for representing randomized algorithms in Coq using a monadic interpretation translating randomized expressions into distributions [22]. A Coq library has been designed in Coq for representing the interval  $[0, 1]$ , probabilistic distributions and randomized algorithms [117]. This library is used in a collaboration between INRIA, Paris-Sud, CNAM, ENS Lyon and Grenoble for the formal verification in Coq of proofs in computational cryptography.

**Compiler certification for synchronous data-flow languages** A new project has been started on the formal development of a certified compiler for the synchronous language Lustre (used for critical software in embedded systems). A formalisation of static analysis has been designed and presented at the conference TYPES 2007 [31]. A library for the formalisation of Kahn's networks has been designed which contains constructive representation of domain theory [116].

**Floating-point arithmetic** Numeric computations use floating-point numbers to approximate exact arithmetic. Unfortunately, this use can falsify a program correct on real numbers. Proof assistants are especially useful as floating-point arithmetic may have unexpected behaviors [33, 35]. A method has been designed and implemented for the specification of errors related to floating numbers computation in C programs [34].

## Foundational Research

**Automatic deduction** Integrating automatic deduction into type theory is a long term research.

S. Conchon and E. Contejean designed an automatic proof procedure Ergo [52] (<http://ergo.lri.fr>) for first-order logic with equality and arithmetic in order to solve proof obligations generated by checking correctness of programs. A trace mechanism for a subset of the procedure has been designed which generates proof scripts in Coq.

S. Lescuyer and J.-F. Couchot designed a method for translating a problem defined in a multi-sorted polymorphic theory into a formula adapted to automatic provers based on mono-sorted logic [61] which is integrated in the WHY platform.

E. Contejean continues her long-term project of cross-fertilizing rewriting techniques and type theory. She designed a large Coq library COCCINELLE (<http://www.lri.fr/~contejea/Coccinelle/coccinelle.html>) on rewriting, using an efficient representation of terms, similar to the one used in rewriting tools like CiMe. This library can be applied to the certification of automated termination proofs [55].

**Dependent types** N. Oury defended his PhD thesis [114] on the theory of equality and pattern matching with dependent types.

**Formal Mathematics and Mathematics Education** Ideas coming from the TYPES community were extensively used for teaching the basis of logic reasoning in a new course for first year undergraduate (L1) students of the university of Grenoble (UJF). The emphasis is put on deduction rules instead of truth tables. Attendees: 300 students in computer science, mathematics, biology, chemistry and physics. Lecturer: JF Monin.

**Proof technology** Most of our research results are integrated in the Coq proof assistant as publicly available libraries and extensions of the system. We develop the WHY platform for the analysis of imperative programs. WHY can also be used as a multi-prover interface for theorem proving.

## Publications

### Refereed journal papers

1. Philippe Audebaud and Christine Paulin-Mohring. Proofs of randomized algorithms in Coq. *Science of Computer Programming*, 2007. Accepted for publication
2. Sylvie Boldo and Guillaume Melquiond. Emulation of fma and correctly-rounded sums: proved algorithms using rounding to odd. *IEEE Transactions on Computers*, 2007. Accepted for publication

### Refereed conference papers

1. Malgorzata Biernacka and Dariusz Biernacki. Formalizing Constructions of Abstract Machines for Functional Languages in Coq. In *7th International Workshop on Reduction Strategies in Rewriting and Programming (WRS 2007)*, Paris, France, June 2007

2. Sylvie Boldo, Marc Daumas, William Kahan, and Guillaume Melquiond. Proof and certification for an accurate discriminant. In *12th IMACS-GAMM International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*, Duisburg, Germany, sep 2006
3. Sylvie Boldo and Jean-Christophe Filliâtre. Formal Verification of Floating-Point Programs. In *18th IEEE International Symposium on Computer Arithmetic*, pages 187–194, Montpellier, France, June 2007
4. Sylvain Conchon, Evelyne Contejean, and Johannes Kanig. CC(X): Efficiently Combining Equality and Solvable Theories without Canonizers. In Sava Krstic and Albert Oliveras, editors, *SMT 2007: 5th International Workshop on Satisfiability Modulo*, 2007
5. Sylvain Conchon, Jean-Christophe Filliâtre, and Julien Signoles. Designing a Generic Graph Library using ML Functors. In *The Eighth Symposium on Trends in Functional Programming*, New York, USA, April 2007
6. Sylvain Conchon and Jean-Christophe Filliâtre. Type-Safe Modular Hash-Consing. In *ACM SIGPLAN Workshop on ML*, Portland, Oregon, September 2006
7. Evelyne Contejean, Pierre Courtieu, Julien Forest, Olivier Pons, and Xavier Urbain. Certification of automated termination proofs. In Frank Wolter, editor, *6th International Symposium on Frontiers of Combining Systems (FroCos 07)*, Lecture Notes in Artificial Intelligence, Liverpool, UK, September 2007. Springer Verlag
8. Jean-François Couchot and Stéphane Lescuyer. Handling polymorphism in automated deduction. In *21th International Conference on Automated Deduction (CADE-21)*, volume 4603 of *Lecture Notes in Artificial Intelligence*, pages 263–278, Bremen, Germany, July 2007
9. Jean-Christophe Filliâtre. Backtracking iterators. In *ACM SIGPLAN Workshop on ML*, Portland, Oregon, September 2006
10. Jean-Christophe Filliâtre and Claude Marché. The Why/Krakatoa/Caduceus platform for deductive program verification. In Werner Damm and Holger Hermanns, editors, *19th International Conference on Computer Aided Verification*, Lecture Notes in Computer Science, Berlin, Germany, July 2007. Springer Verlag
11. Claude Marché and Nicolas Rousset. Verification of Java Card applets behavior with respect to transactions and card tears. In *4th IEEE International Conference on Software Engineering and Formal Methods (SEFM'06)*, Pune, India, September 2006
12. Yannick Moy and Claude Marché. Inferring local (non-)aliasing and strings for memory safety. In *Heap Analysis and Verification (HAV'07)*, Braga, Portugal, March 2007
13. Yannick Moy. Union and cast in deductive verification. In *Proceedings of the C/C++ Verification Workshop*, volume ICIS-R07015. Radboud University Nijmegen, July 2007



14. Matthieu Sozeau. Subset coercions in Coq. In Thorsten Altenkirch and Conor Mc Bride, editors, *TYPES 2006*, volume 4502 of *Lecture Notes in Computer Science*, pages 237–252. Springer Verlag, 2007
15. Matthieu Sozeau. Program-ing finger trees in Coq. In Ralf Hinze and Norman Ramsey, editors, *12th ACM SIGPLAN International Conference on Functional Programming, ICFP 2007*, Freiburg, Germany, 2007. ACM

### Talks

1. Alexandre Bertails. A certified compiler for the synchronous language Lustre. TYPES 2007, talk, May 2007
2. Matthieu Sozeau. A journey with Russell. TYPES 2007, talk, May 2007

### Dissertations

1. Nicolas Oury. *Égalités et filtrages avec types dépendants dans le Calcul des Constructions Inductives*. Thèse de doctorat, Université Paris-Sud, September 2006

## 8.4 TU München

### Correctness of Computer Systems

#### Foundational Research

- Christian Urban from the LMU München site, Michael Norrish from NICTA Canberra, Australia, and Stefan Berghofer from TU München have developed a method for strengthening induction rules for predicates involving *nominal datatypes*. Examples of such predicates include evaluation relations or typing judgements for  $\lambda$ -calculi. When conducting a proof using strengthened induction rules, the user may assume that names of bound variables introduced during the proof are “fresh” with respect to a given context, a convention often used in pencil-and-paper proofs. A paper on this subject has appeared in the proceedings of CADE 2007.

### Formal Mathematics and Mathematics Education

#### Proof technology

- Florian Haftmann and Markus Wenzel have refined the notion of axiomatic type classes in Isabelle towards a “constructive reading” with explicit dictionary parameters. At the same time, classes and Isabelle *locales* have been explained in a uniform setting. As a side-effect, Isabelle now comes with a satisfactory meta-theory of overloading and supports code generation involving type-classes in a Haskell-like manner. This work has been presented at the Types Workshop in April 2007.

- Amine Chaieb and Markus Wenzel have developed techniques for proof methods depending on abstract mathematical structures; this has been demonstrated by significant examples of (semi)ring normalization via Gröbner Bases (Buchberger’s algorithm) and dens linear orders. A paper on this subject has appeared in the proceedings of CALCULEMUS 2007 and MKM 2007.
- Markus Wenzel and Amine Chaieb have refined the idea of “LCF-style” programming of proof tools by means of context-sensitive antiquotations holding references to the formal logical context. Thus the Isabelle/Isar proof language and plain SML have been integrated more tightly, while leaving the meaning of the logic and the programming language untouched. A paper on this subject has appeared in the proceedings of the Workshop on Programming Languages for Mechanized Mathematics.
- In the Festschrift in Honour of Andrzej Trybulec, as well as in the proceedings of TPHOLs 2007, Markus Wenzel has published papers that explain the Isabelle/Isar framework both as a logical framework for structure proof texts, and as a system framework for building formal method tools.

## Publications

### Refereed journal papers

1. Gerwin Klein and Tobias Nipkow. A machine-checked model for a Java-like language, virtual machine and compiler. *ACM Transactions on Programming Languages and Systems*, 28(4):619–695, 2006

### Refereed conference papers

1. Florian Haftmann and Markus Wenzel. Constructive type classes in Isabelle. In Thorsten Altenkirch and Conor McBride, editors, *Types for Proofs and Programs (TYPES 2006)*, volume 4502 of *Lecture Notes in Computer Science*. Springer-Verlag, 2007
2. Tobias Nipkow and Gertrud Bauer. Flyspeck I: Tame graphs. In U. Furbach and N. Shankar, editors, *Automated Reasoning (IJCAR 2006)*, volume 4130 of *Lecture Notes in Computer Science*, pages 21–35. Springer-Verlag, 2006
3. Daniel Wasserrab, Tobias Nipkow, Gregor Snelting, and Frank Tip. An operational semantics and type safety proof for multiple inheritance in C++. In *OOPSLA ’06: Object oriented programming, systems, languages, and applications*. ACM Press, 2006
4. Lukas Bulwahn, Alexander Krauss, and Tobias Nipkow. Finding lexicographic orders for termination proofs in Isabelle/HOL. In K. Schneider and J. Brandt, editors, *Theorem Proving in Higher Order Logics (TPHOLs 2007)*, volume 4732 of *Lecture Notes in Computer Science*, pages 38–53. Springer-Verlag, 2007

5. Amine Chaieb and Markus Wenzel. Context aware calculation and deduction — ring equalities via Gröbner Bases in Isabelle. In M. Kauers, M. Kerber, R. Miner, and W. Windsteiger, editors, *Towards Mechanized Mathematical Assistants (CALCULEMUS 2007 and MKM 2007)*, volume 4573 of *Lecture Notes in Artificial Intelligence*. Springer-Verlag, 2007
6. Markus Wenzel and Burkhart Wolff. Building formal method tools in the Isabelle/Isar framework. In *Theorem Proving in Higher Order Logics (TPHOLs 2007)*, Lecture Notes in Computer Science. Springer-Verlag, 2007
7. Christian Urban, Stefan Berghofer, and Michael Norrish. Barendregt’s variable convention in rule inductions. In Frank Pfenning, editor, *21st International Conference on Automated Deduction (CADE-21)*, volume 4603 of *Lecture Notes in Artificial Intelligence*, pages 35–50. Springer-Verlag, 2007

#### Invited conference papers

1. Tobias Nipkow. Verifying a hotel key card system. In K. Barkaoui, A. Cavalcanti, and A. Cerone, editors, *Theoretical Aspects of Computing (ICTAC 2006)*, volume 4281 of *Lecture Notes in Computer Science*, pages 1–14. Springer-Verlag, 2006. Invited paper
2. Markus Wenzel. Isabelle/Isar — a generic framework for human-readable proof documents. In R. Matuszewski and A. Zalewska, editors, *From Insight to Proof — Festschrift in Honour of Andrzej Trybulec*, Studies in Logic, Grammar, and Rhetoric 10(23). University of Białystok, 2007

#### Workshop papers

1. Markus Wenzel and Amine Chaieb. SML with antiquotations embedded into Isabelle/Isar. In J. Carette and F. Wiedijk, editors, *Programming Languages for Mechanized Mathematics Workshop (CALCULEMUS 2007)*, RISC-Linz Report 07-10, 2007

#### Talks

- Tobias Nipkow. Verification of an electronic hotel key card system. *Theoretical Aspects of Computing (ICTAC 2006)*, Tunis, Tunisia, 20-24 November 2006.
- Stefan Berghofer. An overview of the nominal datatype package in Isabelle/HOL. Workshop on Mathematical Theories of Abstraction, Substitution and Naming in Computer Science, May 26 – 28, 2007, ICMS Edinburgh.
- Christian Urban. Formalizations using the nominal datatype package. Workshop on Mathematical Theories of Abstraction, Substitution and Naming in Computer Science, May 26 – 28, 2007, ICMS Edinburgh.
- Markus Wenzel. Local proofs, local theories, and local everything. *The second Isabelle users workshop (CADE)*, July 15th 2007, Bremen.

## 8.5 München LMU

**Correctness of Computer Systems** In joint work with the University of St Andrews, Hofmann and Loidl have developed a program analysis for inferring upper bounds of heap consumption, stack consumption and execution time in the embedded systems language Hume.

Hofmann and Beringer, in joint work with Benton and Kennedy (Cambridge), have given a relational semantics to effect type systems (APLAS 2006, PPDP 2007). It is used to verify program optimizations in the presence of references.

**Foundational Research** Hofmann, Schoepp, and Schimanski are exploring programming languages and type systems for computational complexity classes (polynomial time, logarithmic time) and connections between different languages for the same class. Schimanski has embedded LFPL into LLL (talk at TYPES 2007).

Schwichtenberg has developed a constructive theory of computable functionals, based on the partial continuous functionals as their intended domain.

**Formal Mathematics and Mathematics Education** Schuster has advanced the development of constructive mathematics. Recently, he has clarified why uniqueness forces constructive existence: the completion of a metric space is isomorphic to the set of all the equations satisfying a certain uniform uniqueness condition for the solutions.

**Proof technology** Schwichtenberg is developing the MINLOG proof assistant and has implemented extraction of programs from proofs with computational content.

Abel and Mehlretter have implemented a termination checker for Agda theorem prover developed at Chalmers. Abel and Aehlig have in cooperation with Coquand and Dybjer (Chalmers) extended the normalization-by-evaluation technique to dependent types (publications MFPS XXIII and LiCS 2007), giving a theoretical justification of equality and type checking in Agda.

Urban and Berghofer have developed the nominal datatype package, a package built on top of the theorem prover Isabelle/HOL and designed to easy proofs about the meta-theory of programming languages.

### Publications

#### Books

1. Martin Hofmann and Matthias Felleisen, editors. *Proceedings of the 34th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2007, Nice, France, January 17-19, 2007*. ACM, 2007
2. Peter Schuster, ‘Trends in Constructive Mathematics.’ Selected papers (with J. Berger, D. Pattinson, J. Zappe, eds.). *Math. Log. Quart.* (2008) [special issue], accepted
3. Peter Schuster, ‘Proceedings of the Third Workshop on Formal Topology (3WFTop), Padova, May 2007’ (with A. Bauer, T. Coquand, G. Sambin, eds.). *Ann. Pure Appl. Logic* [special issue], agreed with journal

4. Peter Schuster, ‘Formal Topology, Program Types, and Constructive Algebra. Lecture Notes of 3WFTop Tutorials.’ Polimetrica, Monza, agreed both with the publisher and the contributors
5. H. Schwichtenberg and K. Spies, editors. *Proof Technology and Computation. Proc. NATO Advanced Study Institute, Marktoberdorf, 2003*, volume 200 of *Series III: Computer and Systems Sciences*. IOS Press, 2006

#### Refereed journal papers

1. Andreas Abel and Thierry Coquand. Untyped algorithmic equality for Martin-Löf’s logical framework with surjective pairs. *Fundamenta Informaticae*, 77(4):345–395, 2007. TLCA’05 special issue
2. Klaus Aehlig. A finite semantics of simply-typed lambda terms for infinite runs of automata. *Logical Methods in Computer Science*, 3(3), 2007
3. Martin Hofmann, Jaap van Oosten, and Thomas Streicher. Well-foundedness in realizability. *Arch. Math. Log.*, 45(7):795–805, 2006
4. Martin Hofmann and Hans-Wolfgang Loidl. Preface. *Theor. Comput. Sci.*, 364(3):271–272, 2006
5. A. Al Zain, P.W. Trinder, G.J. Michaelson, H-W. Loidl. "Evaluating a High-Level Parallel Language (GpH) for Computational GRIDs" In IEEE Transactions on Parallel and Distributed Systems. To appear.
6. Peter Schuster, ‘Formal Zariski topology: positivity and points’. *Ann. Pure Appl. Logic* 137 (2006) 317–359
7. Peter Schuster, ‘The fan theorem and unique existence of maxima’ (with J. Berger, D. Bridges). *J. Symbolic Logic* 71 (2006) 713–720
8. Peter Schuster, ‘Quasi-apartness and neighbourhood spaces’ (with H. Ishihara, R. Mines, L. Viță). *Ann. Pure Appl. Logic* 141 (2006) 296–306
9. Peter Schuster, ‘Apartness and formal topology’ (with E. Palmgren). *New Zealand J. Math.* 35 (2006) 77-84
10. Peter Schuster, ‘Finitely generated Banach algebras and local Nullstellensätze: a constructive treatment’ (with D. Bridges, R. Havea). *Publ. Math. Debrecen* 69/1–2 (2006) 171–184
11. Peter Schuster, ‘Classifying Dini’s theorem’ (with J. Berger). *Notre Dame J. Formal Logic* 47 (2006) 253–262
12. Peter Schuster, ‘A simple constructive proof of Kronecker’s density theorem’ (with D. Bridges). *Elem. Math.* 61 (2006) 152–154
13. Peter Schuster, ‘Unique solutions’. *Math. Log. Quart.* 52 (2006) 534–539. Corrigendum: 53 (2007) 214
14. Peter Schuster, ‘Binary refinement implies discrete exponentiation’ (with P. Aczel, L. Crosilla, H. Ishihara, E. Palmgren). *Studia Logica* 84 (2006) 361–368

15. Peter Schuster, ‘Ideals in constructive Banach algebra theory’ (with D. Bridges, R. Havea). *J. Complexity* 22 (2006) 729–737
16. Peter Schuster, ‘Almost locatedness in uniform spaces’ (with D. Bridges, H. Ishihara, R. Mines, F. Richman, L. Vîță). *Czechoslovak Math. J.* 57 (2007) 1–12
17. Peter Schuster, ‘Spatiality for formal topologies’ (with N. Gambino). *Math. Structures Comput. Sci.* 17 (2007) 65–80
18. Peter Schuster, ‘The shrinking principle and the axiom of choice’ (with B. Banaschewski). *Monatshefte Math.* 151 (2007) 263–270
19. Helmut Schwichtenberg. Minlog. In Freek Wiedijk, editor, *The Seventeen Provers of the World*, volume 3600 of *Lecture Notes in Computer Science*, pages 151–157. Springer, 2006
20. Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, 82:27–51, 2006
21. Helmut Schwichtenberg. An arithmetic for polynomial-time computation. *Theor. Comput. Sci.*, 357(1-3):202–214, 2006
22. G. Bellin, M. Hyland, E. Robinson, and C. Urban. Proof Theory of Classical Propositional Calculus. *Theoretical Computer Science*, 364(2):143–170, 2007

#### Refereed conference papers

1. Andreas Abel. Mixed inductive/coinductive types and strong normalization. In *The Fifth ASIAN Symposium on Programming Languages and Systems (APLAS 2007)*, 2007
2. Andreas Abel, Thierry Coquand, and Peter Dybjer. Normalization by evaluation for Martin-Löf Type Theory with typed equality judgements. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12 July 2007, Wrocław, Poland, Proceedings*, pages 3–12. IEEE Computer Society Press, 2007
3. Andreas Abel. Strong normalization and equi-(co)inductive types. In Simona Ronchi Della Rocca, editor, *Typed Lambda Calculi and Applications, 8th International Conference, TLCA 2007, Paris, France, June 26-28, 2007, Proceedings*, volume 4583 of *Lecture Notes in Computer Science*, pages 8–22. Springer-Verlag, 2007
4. Andreas Abel. Syntactical normalization for intersection types with term rewriting rules. In *Fourth International Workshop on Higher-Order Rewriting, HOR’07, Paris, France, 25 June 2007*, 2007
5. Andreas Abel, Klaus Aehlig, and Peter Dybjer. Normalization by evaluation for Martin-Löf type theory with one universe. In Marcelo Fiore,

- editor, *Proceedings of the 23rd Conference on the Mathematical Foundations of Programming Semantics (MFPS XXIII), New Orleans, LA, USA, 11-14 April 2007*, volume 173 of *Electronic Notes in Theoretical Computer Science*, pages 17–39. Elsevier, 2007
6. Andreas Abel. Semi-continuous sized types and termination. In Zoltán Ésik, editor, *Computer Science Logic, 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 21-24, 2006, Proceedings*, volume 4207 of *Lecture Notes in Computer Science*, pages 72–88. Springer-Verlag, 2006
  7. Klaus Aehlig. A finite semantics of simply-typed lambda terms for infinite runs of automata. In Zoltan Esik, editor, *Proceedings of the 20th international Workshop on Computer Science Logic (CSL '06)*, volume 4207 of *Lecture Notes in Computer Science*, pages 104–118. Springer Verlag, September 2006
  8. Klaus Aehlig and Arnold Beckmann. Propositional logic for circuit classes. In Jacques Duparc and Thomas Henzinger, editors, *Proceedings of the sixteenth Annual Conference on Computer Science and Logic (CSL '07)*, volume 4646 of *Lecture Notes in Computer Science*, pages 512–526. Springer Verlag, September 2007
  9. Klaus Aehlig, Stephen A. Cook, and Phuong Nguyen. Relativizing small complexity classes and their theories. In *Proceedings of the sixteenth Annual Conference on Computer Science and Logic (CSL '07)*, volume 4646 of *Lecture Notes in Computer Science*, pages 374–388. Springer Verlag, September 2007
  10. Nick Benton, Andrew Kennedy, Lennart Beringer, and Martin Hofmann. Relational semantics for effect-based program transformations with dynamic allocation. In Michael Leuschel and Andreas Podelski, editors, *Proceedings of the 9th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, July 14-16, 2007, Wroclaw, Poland*, pages 87–96. ACM, 2007
  11. Nick Benton, Andrew Kennedy, Martin Hofmann, and Lennart Beringer. Reading, writing and relations. In Naoki Kobayashi, editor, *Programming Languages and Systems, 4th Asian Symposium, APLAS 2006, Sydney, Australia, November 8-10, 2006, Proceedings*, volume 4279 of *Lecture Notes in Computer Science*, pages 114–130. Springer, 2006
  12. Lennart Beringer and Martin Hofmann. A bytecode logic for jml and types. In Naoki Kobayashi, editor, *Programming Languages and Systems, 4th Asian Symposium, APLAS 2006, Sydney, Australia, November 8-10, 2006, Proceedings*, volume 4279 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2006
  13. Christian Dax, Martin Hofmann, and Martin Lange. A proof system for the linear time  $\mu$ -calculus. In S. Arun-Kumar and Naveen Garg, editors, *FSTTCS 2006: Foundations of Software Technology and Theoretical*

*Computer Science, 26th International Conference, Kolkata, India, December 13-15, 2006, Proceedings*, volume 4337 of *Lecture Notes in Computer Science*, pages 273–284. Springer, 2006

14. Abyd Al Zain, Phil W. Trinder, Hans-Wolfgang Loidl, Greg J. Michaelson. "Supporting High-Level Grid Parallel Programming: the Design and Implementation of Grid-GUM2" Proceedings of the All Hands Meeting 2007 (AHM2007) to the UK e-Science Programme, Nottingham 10 - 13 Sept 2007.
15. Armelle Bonenfant, Kevin Hammond, Christoph A. Herrmann, Steffen Jost, Hans-Wolfgang Loidl, Robert Pointon. "Automatic Amortised Worst-Case Execution Time Analysis" In 7th Int'l Workshop on Worst-Case Execution Time (WCET) Analysis, Pisa, Italy, July 3, 2007.
16. A. Al Zain, K. Hammond, P.W. Trinder, S. Linton, H-W. Loidl, and M. Costanti. "SymGrid-Par: Designing a Framework for Executing Computational Algebra Systems on Computational Grids " Fourth International Workshop on Practical Aspects of High-level Parallel Programming (PAPP 2007), part of The International Conference on Computational Science (ICCS07), May 27-30, 2007, University of Beijing, China.
17. Peter Schuster, 'Problems as solutions'. In: S. B. Cooper, B. Löwe, A. Sorbi, eds., *Computation and Logic in the Real World*. Third Conference on Computability in Europe, CiE 2007. Siena, Italy, June 2007. Springer, Berlin and Heidelberg. *Lect. Notes Comput. Sci.* 4497 (2007) 676–684
18. Peter Schuster, 'Dini's theorem in the light of reverse mathematics' (with Josef Berger). In: S. Lindström, E. Palmgren, K. Segerberg, V. Stoltenberg-Hansen, eds., *Logicism, Intuitionism, and Formalism—What has become of them?* Workshop on the Philosophy of Mathematics, Uppsala, Sweden, August 27–29, 2004
19. Helmut Schwichtenberg. Inverting monotone continuous functions in constructive analysis. In Arnold Beckmann, Ulrich Berger, Benedikt Löwe, and John V. Tucker, editors, *Logical Approaches to Computational Barriers, Second Conference on Computability in Europe, CiE 2006, Swansea, UK, June 30-July 5, 2006, Proceedings*, volume 3988 of *Lecture Notes in Computer Science*, pages 490–504. Springer, 2006
20. Helmut Schwichtenberg. Recursion on the partial continuous functionals. In C. Dimitracopoulos, L. Newelski, D. Normann, and J. Steel, editors, *Logic Colloquium '05*, volume 28 of *Lecture Notes in Logic*, pages 173–201. Association for Symbolic Logic, 2006
21. Helmut Schwichtenberg. Constructive analysis with witnesses. In H. Schwichtenberg and K. Spies, editors, *Proof Technology and Computation. Proc. NATO Advanced Study Institute, Marktoberdorf, 2003*, volume 200 of *Series III: Computer and Systems Sciences*, pages 323–353. IOS Press, 2006
22. C. Urban, S. Berghofer, and M. Norrish. Barendregt's Variable Convention in Rule Inductions. In *Proc. of the 21th International Conference on Automated Deduction (CADE)*, volume 4603 of *LNAI*, pages 35–50, 2007



23. J. Narboux and C. Urban. Formalising in Nominal Isabelle Crary's Completeness Proof for Equivalence Checking. In *Proc. of the International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP)*, 2007
24. C. Urban and R. Pollack. Strong Induction Principles in the Locally Nameless Representation of Binders (Preliminary Notes). In *Proc. of the Workshop on Mechanizing Meta-Theory*, 2007

## Talks

1. Andreas Abel, Normalization by Evaluation for Martin-Löf Type Theory with Typed Equality Judgements, 10 July 2007. Logic in Computer Science, LiCS 2007, Wroclaw, Poland.
2. Andreas Abel, Strong Normalization for Equi-(Co)inductive Types 27 June 2007. International Conference on Typed Lambda Calculi and Applications, TLCA 2007, Paris, France.
3. Andreas Abel, Syntactical Strong Normalization for Intersection Types with Term Rewriting Rules 25 June 2007. International Workshop on Higher-Order Rewriting, HOR 2007, Paris, France.
4. Andreas Abel, Strong Normalization for Equi-(Co)inductive Types 2 May 2007. International Workshop on Types for Proofs and Programs, TYPES 2007, Cividale, Udine, Friuli, Italy.
5. Andreas Abel, Syntactical Normalization Proofs 14 March 2007. Programming Logics Group, Department of Computer Science, Chalmers University of Technology, Göteborg, Sweden.
6. Andreas Abel, Type-Based Termination 9 March 2007. Copenhagen Programming Language Seminar, ITU, Copenhagen, Denmark.
7. Andreas Abel, Normalization by Evaluation and Dependent Types 27 February 2007. Protheo Seminar, LORIA, Nancy, France.
8. Andreas Abel, Semantical Type-Checking Normalization by Evaluation Techniques and Abstract Values December 19, 2006. TYPES Workshop Curry-Howard Implementation Techniques - Connecting Humans And Theorem provers CHIT-CHAT, Radboud University, Nijmegen, The Netherlands.
9. Andreas Abel, Normalization by Evaluation for Martin-Löf Type Theory with One Universe December 7, 2006. Arbeitstreffen Bern-München, Department of Mathematics, University of München.
10. Andreas Abel, Semi-continuous Sized Types and Termination September 26, 2006. 15th Annual Conference of the EACSL, Computer Science Logic, CSL '06, Szeged, Hungary, September 25-29, 2006.
11. Stefan Schimanski, *An embedding of LFPL into LLL*, Types 2007 Conference, Cividale

12. Peter Schuster, Séminaire de l'Equipe Algèbre et Théorie des Nombres, Université de Franche-Comté, Besançon, France (28 Sep 2006)
13. Peter Schuster, Laboratory of Foundational Aspects of Computer Science Seminar, University of Cape Town, South Africa (Mar 2007)
14. Peter Schuster, Radboud Universiteit, Nijmegen, The Netherlands (Jun 2007, invited)
15. Peter Schuster, *Colloquium Logicum 2006*, Bonn, Germany (Sep 2006)
16. Peter Schuster, *Mathematics: Algorithms and Proofs*, Lorentz Center, Leiden, The Netherlands (Jan 2007)
17. Peter Schuster, *Methods of Proof Theory in Mathematics*, Max-Planck-Institut für Mathematik, Bonn, Germany (invited, not attended) (Jun 2007)
18. Peter Schuster, *Computation and Logic in the Real World*. Third Conference on Computability in Europe, CiE 2007, Siena, Italy (Jun 2007)
19. Christian Urban, Lecture course at the International School on Rewriting in Nancy (2 - 6 July)
20. Christian Urban, Talk at LFCS in Edinburgh (29th May, host: Randy Pollack)
21. Christian Urban, Talk at ICMS Workshop on Substitution and Naming in Computer Science (26 - 28 May, Edinburgh)
22. Christian Urban, Talk at St Andrews University (13th February, host: Dr Roy Dyckhoff)
23. Christian Urban, Talk in London (1st November, host: Prof. Edmund Robinson)
24. Christian Urban, Talk in Amsterdam (15th September, hosts: Prof. Jan Klop and Dr Femke van Raamsdonk)

## 8.6 Nijmegen

**Correctness of Computer Systems** Geuvers, Synek and Tveretina have started research in correctness of Hybrid Systems. The plan is to prove properties of Hybrid Systems by modelling these in the Coq proof assistant.

**Foundational Research** Geuvers and Loeb have studied further the notion of 'deduction graph', extending it with universal quantification.

Wiedijk has studied and described the type system of the Mizar proof system and published it in TPHOLs 2007.

Barendregt and Dekkers have continued the work on the overview book on typed lambda calculus.

O'Connor and Niqui have both worked on exact real arithmetic, formalising various approaches to real number computation in Coq.

Spitters has studied topics in formal topology and constructive functional analysis.

**Formal Mathematics and Mathematics Education** Kaliszyk has developed a web interface for Coq that has been used in various classes in Nijmegen and Amsterdam, teaching students logic. This has been done in a Dutch SURF funded project “Web deduction”, lead by Wiedijk, where this Coq interface has been turned into a web-based tool for doing natural deduction.

**Proof technology** Kaliszyk and Corbineau have developed a first version of a “Mathwiki” that provides web access to a variety of proof assistants (Coq, Isabelle, ...) and thereby supports the web-based development of a distributed of formalized mathematics. The plan is to work out these ideas into a EU Strep proposal, together with other Types partners.

## Publications

### Refereed journal papers

1. Herman Geuvers, Milad Niqui, Bas Spitters, and Freek Wiedijk. Constructive analysis, types and exact real numbers (overview article). *Mathematical Structures in Computer Science*, 17(1):3–36, 2007
2. H. Geuvers and I. Loeb. Natural deduction via graphs: Formal definition and computation rules. *Mathematical Structures in Computer Science*, 17(3):485–526, 2007
3. H. Barendregt and F. Wiedijk. The Challenge of Computer Mathematics. *Transactions A of the Royal Society*, 363(1835):2351–2375, 2006
4. F. Wiedijk. Is ZF a hack? comparing the complexity of some (formalist interpretations of) foundational systems for mathematics. *Journal of Applied Logic*, 4:622–645, 2006
5. Venanzio Capretta, Tarmo Uustalu, and Varmo Vene. Recursive coalgebras from comonads. *Information and Computation*, 204(4):437–468, April 2006
6. Bas Spitters. A constructive view on ergodic theorems. *J. Symbolic Logic*, 71(2):611–623, 2006

### Refereed conference papers

1. Ana Bove and Venanzio Capretta. Computation by prophecy. In *Typed Lambda Calculi and Applications, TLCA 2007*, volume 4583 of LNCS, pages 70–83. Springer, 2007
2. Venanzio Capretta, Bernard Stepien, Amy Felty, and Stan Matwin. Formal correctness of conflict detection for firewalls. In *The 5th ACM Workshop on Formal Methods in Security Engineering: From Specification to Code*. ACM, 2007. in print
3. Lionel Elie Mamane. Surreal numbers in coq. In Jean-Christophe Filli tre, Christine Paulin-Mohring, and Benjamin Werner, editors, *Types*

for Proofs and Programs: International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers, volume 3839 of *Lecture Notes in Computer Science*, pages 170–185. TYPES network, Springer Verlag, January 2006

4. Herman Geuvers and Lionel Elie Mamane. A document-oriented coq plugin for texmacs. In Paul Libbrecht, editor, *MathUI workshop at the MKM 2006 conference*, <http://www.activemath.org/paul/MathUI06/>, August 2006. MKM Interest Group
5. Herman Geuvers and Iris Loeb. From deduction graphs to proof nets: Boxes and sharing in the graphical presentation of deductions. In *Mathematical Foundations of Computer Science 2006, 31st International Symposium, MFCS 2006, Stará Lesná, Slovakia, August 28-September 1, 2006, Proceedings*, volume 4162 of *Lecture Notes in Computer Science*, pages 39–57, 2006
6. H. Geuvers and F. Wiedijk. A logical framework with explicit conversions. In Carsten Schürmann, editor, *Proceedings of the Fourth International Workshop on Logical Frameworks and Meta-Languages, Cork, Ireland*. ENTCS, 2007
7. H. Geuvers and I. Loeb. Deduction graphs with universal quantification. In I. Mackie and D. Plump, editors, *Proceedings of TERMGRAPH 2007*. ENTCS, 2007
8. F. Wiedijk. Introduction. In F. Wiedijk, editor, *The Seventeen Provers of the World*, volume 3600 of *LNCS*. Springer, 2006
9. Milad Niqui. Coinductive field of exact real numbers and general corecursion. *Electronic Notes in Theoretical Computer Science*, 164(1):121–139, October 2006
10. C. Kaliszyk. Web interfaces for proof assistants. In S. Autexier and C. Benzmüller, editors, *Proceedings of the FLoCs Workshop on User Interfaces for Theorem Provers (UITP-06), Seattle*, pages 53–64, 2006. To be published in ENTCS
11. P. Corbineau. A declarative language for the Coq proof assistant. In Klaus Schneider and Jens Brandt, editors, *Theorem Proving in Higher Order Logics: Emerging Trends Proceedings*, number 364/07 in Technical Report, Department of Computer Science, University of Kaiserslautern, 08 2007
12. P. Corbineau and C. Kaliszyk. Cooperative repositories for formal proofs – a wiki-based solution. In *Towards Mechanized Mathematical Assistants*, volume 4573 of *LNCS*, pages 221–234. Springer, 2007
13. P. Corbineau. Deciding equality in the constructor theory. In Thorsten Altenkirch and Conor McBride, editors, *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers*, volume 4502 of *Lecture Notes in Computer Science*, pages 78–92. Springer, 2007

14. M. Hendriks C. Kaliszyk, F. Wiedijk and F. van Raamsdonk. Teaching logic using a state-of-the-art proof assistant. In H. Geuvers and P. Courtieu, editors, *PATE'07, International Workshop on Proof Assistants and Types in Education*, pages 37–50. CNAM, 2007
15. F. Wiedijk. The qed manifesto revisited. In R. Matuszowski and A. Zalewska, editors, *From Insight to Proof, Festschrift in Honour of Andrzej Trybulec*, pages 121–133. 2007
16. C. Kaliszyk and F. Wiedijk. Certified computer algebra on top of an interactive theorem prover. In R. Miner M. Kauers, M. Kerber and W. Windsteiger, editors, *Towards Mechanized Mathematical Assistants, Calculemus 2007, Hagenberg*, volume 4573 of *LNAI*, pages 94–105, 2007
17. J. Carette and F. Wiedijk, editors. *Programming Languages for Mechanized Mathematics Workshop, Informal Proceedings*, number 07-10 in RISC-Linz Report Series, 2007

### Popular

1. Freek Wiedijk. On the usefulness of formal methods. *Nieuwsbrief van de NVTI*, pages 14–23, 2006
2. H. Geuvers. Computer-ondersteund redeneren: de boekhouder steunt de denker (Dutch), inaugural speech, March 9 2007. Radboud University Nijmegen, ISBN 978-90-9021687-4
3. B. Mols. *Opgelost, Toepassingen van Wiskunde en Informatica*, chapter 14, Wiskunde om de wiskunde. De deskundige: Henk Barendregt, pages 163–166. Veen Magazines, Diemen, 2006
4. H.P. Barendregt. Hoofdstuk. In John Brockman, editor, *Ik geloof dat ... maar heb geen bewijs. De belangrijkste denkers over wat zij zeker menen te weten*, pages 201–205. Spectrum, Utrecht, 2006

### Talks

1. Freek Wiedijk – Do not take natural language too seriously, Seminar Formal Mathematics, University of Bonn 2007-04-17,
2. Freek Wiedijk – Formalization of mathematics, Nederlands Mathematisch Congres, Leiden University, 2007-04-12,
3. Freek Wiedijk – How to implement a typechecker?, CHIT/CHAT workshop, University of Nijmegen, 2006-12-19,
4. Herman Geuvers – Course “Introduction to Type Theory” at the Bertinoro Summer school.
5. H. Geuvers – Formalising Hybrid Systems in Coq. Talk at the annual Types Conference, Cividale Italy, May 2007.

6. H. Geuvers MathWiki, a first proposal for a Strep project. Talk at the annual Types Conference, Cividale Italy, May 2007.
7. Henk Barendregt – Non-left linear reductions via infinitary lambda calculus. Symposium from Type Theory to Morphologic Complexity: 28-29 June 2007
8. Venanzio Capretta – Common Knowledge as a Coinductive Modality. Gotheborg August 2007
9. Venanzio Capretta – The path to Computer Mathematics, Tallin, April 2007.
10. Cezary Kaliszyk – Automating side conditions in formalized partial functions, TYPES Annual Meeting, Cividale del Friuli, Italy
11. Cezary Kaliszyk – Towards Wikis for Formalized Mathematics, PGIP meeting March 2007.
12. Milad Niqui – Certified exact real arithmetic in arbitrary integer radix using co-induction TYPES Annual Meeting, Cividale del Friuli, Italy
13. Bas Spitters – Computable sets: located and overt locales, Third Workshop on Formal Topology, Padova, Italy 2007

### Dissertations

1. Iris Loeb – Natural Deduction, Sharing By Presentation, PhD thesis Radboud University Nijmegen, June 2007.

## 8.7 Białystok

**Formal Mathematics and Mathematics Education** In the last academic year, three MIZAR-based courses (*Introduction to Logic and Set Theory*, *Formalizing Mathematics* and *Software Verification*) were carried out with computer science students at the University of Białystok. Two additional courses have been designed and the names of undergraduate courses have been changed, so that from this year on the obligatory curriculum will include one one-semester MIZAR-aided course during each year of study.

Undergraduate courses:

- *Introduction to Formal Methods*
- *Constructive Methods in Computer Science*
- *Abstract Methods in Computer Science*

Graduate courses:

- *Software Verification*
- *Proof Verification*

Since September 2006, the MIZAR Mathematical Library (MML) has been extended with 39 new articles.

**Proof technology** The strength of the MIZAR checker has been improved by redesigning the mechanism of adjective registrations. This new implementation required extensive revisions to MML.

The MIZAR language has been extended with several new features, including the `identify` construct which adds more automation to some aspects of redefinitions.

Two new articles of the Encyclopedia of Mathematics in Mizar (EMM) have been extracted from MML (*On the Arithmetic of Boolean Values* and *Basic Properties of Extended Real Numbers*) - encyclopedic articles are supposed to comprehensively cover selected areas of mathematics.

## Publications

### Refereed journal papers

1. Adam Grabowski and Artur Kornilowicz - "Computer-Assisted Reasoning about Algebraic Topology", in R. Matuszewski and A. Zalewska (Eds.): From Insight to proof. Festschrift in Honour of Andrzej Trybulec, *Studies in Logic, Grammar and Rhetoric* 10 (23), pp. 179–189, 2007.
2. Adam Naumowicz - "Evaluating Prospective Built-in Elements of Computer Algebra in Mizar", in R. Matuszewski and A. Zalewska (Eds.): From Insight to proof. Festschrift in Honour of Andrzej Trybulec, *Studies in Logic, Grammar and Rhetoric* 10 (23), pp. 191–200, 2007.

### Refereed conference papers

1. Ewa Borak and Anna Zalewska - "Mizar Course in Logic and Set Theory", in M. Kauers et al. (Eds.): MKM/Calculemus 2007, LNAI 4573, pp. 191–204, 2007.
2. Adam Grabowski and Christoph Schwarzweller - "Revisions as an Essential Tool to Maintain Mathematical Repositories", in M. Kauers et al. (Eds.): MKM/Calculemus 2007, LNAI 4573, pp. 235–249, 2007.

## Talks

1. Adam Naumowicz - "How to Teach to Write a Proof", in proceedings of RDP 2007 affiliated TYPES Workshop on Proof Assistants and Types in Education, pp. 69-76, Paris, June 25, 2007.

## 8.8 Royal Holloway, University of London

The TYPES-related main scientific work includes:

## Foundational Research

- Z Luo and R Adams have worked on the development of the “Framework Approach” to formalisation and verification. Along this line, a type-theoretic framework for formalisation and verification with different logical foundations has been developed (and implemented in Plastic, thanks to Paul Callaghan). A paper concerning this has been published in LNCS 4435.
- Z Luo and R Adams have worked on structural subtyping for parameterised inductive types in coercive subtyping for dependent type theories. A paper on this has been submitted to and accepted by Mathematical Structures in Computer Science.
- Z Luo has worked on coercions in a polymorphic type system and a paper on this has been submitted.

## Formal Mathematics and Proof technology

- R Adams and Z Luo have used the type-theoretic framework (see above) to formalise Weyl’s predicative mathematics in the proof assistant Plastic. A paper on this has been published in TYPES’07, LNCS 4502.

The TYPES-related publications/presentations in the last year include

## Refereed journal papers

1. Z. Luo and R. Adams. *Structural Subtyping for inductive types with functorial equality rules*. Mathematical Structures in Computer Science. 2006. Accepted and to appear.

## Refereed conference papers

1. Z. Luo. A type-theoretic framework for formal reasoning with different logical foundations. Proc of the 11th Annual Asian Computing Science Conference. LNCS 4435. 2007.
2. R. Adams and Z. Luo. *Weyl’s predicative classical mathematics as a logic-enriched type theory*. In Types for Proofs and Programs, Proc. of Inter. Conf. of TYPES’06. LNCS 4502. 2007.

## Talks

1. R. Adams. Coercive Subtyping in a Lambda-Free Logical Framework. TYPES’07, 2007.



## 8.9 Edinburgh

**Correctness of Computer Systems** Jaroslav Ševčík and David Aspinall have formalised the Java Memory Model in Isabelle/HOL. As well as filling in missing details of the published semi-formal presentation, they show how to fix known bugs, and find several previously unknown bugs.

Robert Atkey has formalised an executable Java Virtual Machine in Coq, along with a linear logic of resource usage for reasoning about bytecode programs for this machine.

**Foundational Research** James Brotherston completed his PhD on "Complete Sequent Calculi for Induction and Infinite Descent". This is strongly related to inductive definitions and inductive reasoning in type theory.

Rasmus Møgelberg and Alex Simpson have extended the theory of relational parametricity from pure functional languages to a general theory of relational parametricity for computational effects (nondeterminism, probabilistic choice, input/output, exceptions, etc.).

In related work, Robert Atkey generalised Moggi's computational monads to capture computational effects with parameters, such as composable continuations and side effects where the type of the state varies.

**Formal Mathematics and Mathematics Education** Randy Pollack continued work on formal representation of mathematical languages with binding, and joint work with Christian Urban (TU München) on using the nominal Isabelle package to support the *locally nameless* representation of binding.

**Proof technology** The *Proof General* interface (David Aspinall et. al.) is widely used in the TYPES community. Aspinall and others are completely redeveloping Proof General in Eclipse, a modern framework for user interfaces, with many powerful new features.

Work on proof automation through *proof planning* (a high-level tactic mechanism) continued by Lucas Dixon, Priya Gopalan and Moa Johansson.

### Publications

#### Refereed journal papers

1. Robert Atkey. Parameterised notions of computation. *Journal of Functional Programming*, 2007. To appear. Expanded from a version at TYPES workshop MSFP'06

#### Refereed conference papers

1. James Cheney and Alberto Momigliano. Mechanized metatheory model-checking. In Michael Leuschel and Andreas Podelski, editors, *Proceedings of the 9th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, July 14-16, 2007, Wrocław, Poland*, pages 75–86. ACM, 2007

2. Alberto Momigliano, Alan Martin, and Amy Felty. Two-level hybrid: A system for reasoning using higher-order abstract syntax. Presented at Logical Frameworks and Meta-Languages (LFMTP'07), July 2007
3. Rasmus Møgelberg and Alex Simpson. Relational parametricity for computational effects. In *LICS*, pages 346–355. IEEE Computer Society, 2007
4. Rasmus Møgelberg and Alex Simpson. Relational parametricity for control considered as a computational effect. *Electr. Notes Theor. Comput. Sci.*, 173:295–312, 2007. Presented at Mathematical Foundations of Programming Semantics, (MFPS'07)
5. D. Aspinall, P. Maier, and I. Stark. Monitoring external resources in Java MIDP. In *REM 2007: Proceedings of the First International Workshop on Run Time Enforcement for Mobile and Distributed Systems*, September 2007. To appear
6. D. Aspinall and J. Ševčík. Formalising Java’s data-race-free guarantee. In *Theorem Proving in Higher Order Logics: Proceedings of the 20th International Conference TPHOLs 2007*, Lecture Notes in Computer Science 4732, pages 22–37. Springer-Verlag, 2007
7. D. Aspinall and J. Ševčík. Java memory model examples: Good, bad and ugly. In *VAMP 2007: Proceedings of the 1st International Workshop on Verification and Analysis of Multi-threaded Java-like Programs*, 2007. To appear
8. David Aspinall and Piotr Hoffman. Datatypes in memory. In Till Mossakowski, Ugo Montanari, and Magne Haveraaen, editors, *CALCO*, volume 4624 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 2007
9. David Aspinall, Christoph Lüth, and Daniel Winterstein. A framework for interactive proof. In Manuel Kauers, Manfred Kerber, Robert Miner, and Wolfgang Windsteiger, editors, *Calculemus/MKM*, volume 4573 of *Lecture Notes in Computer Science*, pages 161–175. Springer, 2007
10. James Brotherston and Alex Simpson. Complete sequent calculi for induction and infinite descent. In *Proceedings of LICS-22*, pages 51–60. IEEE Computer Society, July 2007

## Talks

1. Randy Pollack: invited talk at Logical Frameworks and Meta Languages (LFMTP, July 2007).
2. Randy Pollack: talk at Chalmers “Local Representations of Binding” (Feb. 2007).
3. Randy Pollack: talk at TYPES workshop Curry Howard Implementation Techniques (CHIT) “The Constructive Engine”. (Nov 2006).
4. David Aspinall: talk at TYPES annual meeting (May 2007) on “Proof Engineering with Proof General”.

5. David Aspinall: talk at Isabelle Workshop (July 2007) “Isabelle with Proof General Eclipse”.
6. Rasmus Møgelberg: talk at TYPES annual meeting (May 2007) on “A logic for parametric polymorphism with effects”.
7. Lucas Dixon: talk at TYPES annual meeting (May 2007) on “Deeply Embedded Datatype Morphisms”.
8. Lucas Dixon: talk at TYPES CHIT/CHAT workshop (Nov 2006) “Issues for Proof-Centric Proof Interfaces”.
9. Lucas Dixon: talk at ITU Copenhagen (Nov 2006) “Proof Planning in Twelf”
10. Robert Atkey: talk at TYPES annual meeting (May 2007) on “Implementing a JVM with Dependent Types”.
11. Priya Gopalan: talk at Isabelle Workshop (July 2007) “Concurrent/Distributed theorem proving in Isabelle/IsaPlanner”.
12. Moa Johansson: talk at Isabelle Workshop (July 2007) “Proof critics for IsaPlanner”.
13. James Cheney: tutorial on nominal logic and logic programming at the ICMS workshop on abstraction, naming, and substitution (May 2007).
14. James Cheney: talk at PPDP (July 2007) “Mechanized Metatheory Model-Checking”.

### Dissertations

1. James Brotherston. *Complete Sequent Calculi for Inductive Definitions*. PhD thesis, University of Edinburgh, November 2007

## 8.10 Manchester

### Correctness of Computer Systems

**Foundational Research** Peter Aczel and his PhD student, Joao Belo, are working on a generalisation of many-sorted logic, Dependently Sorted Logic where sorts may depend on individual variables, as types do in dependent type theory. Belo has generalised the metatheory of predicate logic to dependently sorted logic including syntax and semantics with completeness and interpolation results for both classical and intuitionistic versions. Peter Aczel is working on a notion of *type setup* that abstracts away from the details of the syntax of a dependent type theory.

Peter Aczel continues to work on Constructive Set Theory and constructive topology.

### Formal Mathematics and Mathematics Education

## Proof technology

## Publications

### Refereed journal papers

1. Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren and Peter Schuster. Binary Refinement Implies Discrete Exponentiation. *Studia Logica* 84 (2006) 361-368.

### Talks

1. Peter Aczel (Manchester): “Local Constructive Set Theory”, talk given at the Annual meeting of the Swiss Society for Logic and Philosophy of Science, on "Foundational Theories of Mathematics". Freiburg, Switzerland, October 11,12, 2006.
2. Peter Aczel (Manchester): “On avoiding dependent choices in Formal Topology”, talk given at the 3rd Formal Topology workshop, Padova, Italy, 7-12 May, 2007.
3. Peter Aczel (Manchester): “Type setups and logic-enriched type theories”, talk given at the meeting on Proofs and Computation II, München, 23 June 2007.
4. Joao Belo (Manchester): “Interpolation for Dependently Sorted Logic”, talk given at Types 2007, Udine, Italy, 2-5 May 2007.

## 8.11 Torino

**Foundational Research** Resource control and types for ambient and process mobility have attracted increasing interest in Torino site, as part of a foundational research on distributed systems. Our aim was to obtain an analysis of space usage in the context of an ambient-like calculus with bounded capacities and weighed processes, where migration and activation require space. This was achieved by using a type system complementing the dynamics of the calculus and providing static guarantees that the intended capacity bounds are preserved throughout the computation. The calculus comes equipped with a labeled transition system in which types play a major role: this system allows us to show interesting algebraic laws. Types also express, as usual in this setting, the communication, access and mobility properties of the modeled system; inferred types express the minimal constraints required for the system to well behave. We obtained a language flexible enough to allow different topics of conversation between an ambient and different parents of it, without compromising type-safety: we used port names for communication and ambient names for mobility. We defined a behavioral semantics a we proved type-soundness for all calculi we studied or defined (MA, M, BACI).

## 8.12 Udine and Padova

The Udine site organized the final general TYPES meeting, in Cividale, May 2-5, 2007. <http://users.dimi.uniud.it/types07/>, with more than 100 participants. The invited speakers (funded by TYPES) were Frédéric Blanqui (INRIA-Loria), Peter Sewell (University of Cambridge), Amy Felty (University of Ottawa).

The Padova subsite organized the “Third workshop in Formal Topology”, Padova, May 7-12, 2007 <http://www.3wftop.math.unipd.it/>. Invited speakers funded by Types: Peter Aczel (University of Manchester), Thierry Coquand (University of Goteborg), Per Martin-Loef (University of Stockholm), Erik Palmgren (University of Uppsala), Bas Spitters (University of Nijmegen).

**Correctness of Computer Systems** The Udine site has continued the study of methods and techniques for supporting the verification of correctness of programs, especially for object-oriented languages. Honsell, Lenisa and Redamalla extended Reichel-Jacobs coalgebraic account of objects and classes in Object Oriented Programming, where classes are modeled as bialgebras, to cover also binary methods. Class types include products, sums and powerset type constructors.

Ciaffaglione, Liquori and Miculan illustrated a methodology for formalizing and reasoning about Abadi and Cardelli’s object-based calculi, in (co)inductive type theory, such as the Calculus of (Co)Inductive Constructions, by taking advantage of Natural Deduction Semantics and coinduction in combination with weak Higher-Order Abstract Syntax and the Theory of Contexts. This methodology allows to implement smoothly the calculi in the target metalanguage; moreover, it suggests novel presentations of the calculi themselves.

**Foundational Research** Honsell, Lenisa and Liquori have introduced a General Logical Framework, called GLF, for defining Logical Frameworks, based on dependent types, in the style of the well known Edinburgh Logical Framework LF. The framework GLF subsumes, by simple instantiation, LF as well as a large class of generalized constrained-based lambda calculi, ranging from well known restricted lambda calculi, such as Plotkin’s call-by-value lambda calculus, to lambda calculi with patterns. But it suggests also a wide spectrum of new calculi which have intriguing potential as Logical Frameworks.

In the area of constructive mathematics, Valentini has provided some constructive characterizations of the notion of bar subset for the complete binary tree, alias Cantor space, for the complete countable spreading tree, alias Baire Space, and, more generally, for an inductively generated formal topology. Moreover, by using a completeness theorem for inductively generated formal topologies, he proved that such characterizations are classically equivalent to the standard one.

M.E. Maietti and G. Sambin studied the meaning of a “proofs-as-programs” foundation for constructive mathematics, usually identified with a type theory, like that introduced by Martin-Loef or the Calculus of Constructions by T. Coquand, by characterizing it via mathematical logical principles. Following previous work by Sambin, they argued that a proofs-as-programs foundation for constructive mathematics should be equipped with two levels: an intensional level of programs represented by a type theory, and an extensional level where to

introduce extensional concepts and to develop mathematical proofs. To this end, they have introduced an extensional version, called  $qmTT$ , of the intensional Minimal Type Theory  $mTT$ , introduced in a previous paper with G. Sambin, enriched with proof-irrelevance of propositions and effective quotient sets. Then, by using the construction of total setoid à la Bishop we build a model of  $qmTT$  over  $mTT$ .

**Formal Mathematics and Mathematics Education** Ciaffaglione and Di Gianantonio constructed exact Real Numbers in the proof assistant Coq using streams (i.e. infinite sequences) of ternary signed digits  $\{0, 1, -1\}$ . Then they certified the implementation working with coinductive types, corecursive functions and constructive logic.

## Publications

### Refereed journal papers

1. G. Boniolo and S. Valentini. Vagueness, kant and topology: a study of formal epistemology. *Journal of Philosophical Logic*, 2007
2. A. Ciaffaglione and P. Di Gianantonio. A certified, corecursive implementation of exact real numbers. *Theoretical Computer Science*, 351:39–51, 2006
3. Alberto Ciaffaglione, Luigi Liquori, and Marino Miculan. Reasoning about object-based calculi in (co)inductive type theory and the theory of contexts. *J. Autom. Reasoning*, 39(1):1–47, 2007
4. Giovanni Curi. Exact approximations to stone Čech compactification. *Annals of Pure and Applied Logic*, 2-3(146):103–123, 2007
5. F. Honsell, M. Lenisa, and R. Redamalla. Coalgebraic description of generalized binary methods. *Mathematical Structures in Computer Science*, 4(17):647–673, 2007
6. G. Sambin. Molteplicità delle logiche e necessità delle traduzioni. logica intuizionistica e logica classica a confronto. *Lettera matematica, Pristem*, 62-63:41–59, 2007
7. S. Valentini. Constructive characterizations of bar subsets. *Annals of Pure and Applied Logic*, 3(145):368–378, 2007

### Refereed conference papers

1. Davide Grohmann and Marino Miculan. An algebra for directed bigraphs. In Ian Mackie and Detlef Plump, editors, *Pre-proceedings of TER-MGRAPH 2007*, ENTCS. Elsevier, 2007
2. Davide Grohmann and Marino Miculan. Directed bigraphs. In *Proc. XXIII MFPS*, volume 173 of *ENTCS*, pages 121–137. Elsevier, 2007

3. Davide Grohmann and Marino Miculan. Reactive systems over directed bigraphs. In L. Caires and V.T. Vasconcelos, editors, *Proc. CONCUR 2007*, volume 4703 of *Lecture notes in computer science*, pages 380–394. Springer-Verlag, 2007
4. F. Honsell, M. Lenisa, and L. Liquori. A framework for defining logical frameworks. *ENTCS*, 172:399–436, 2007. Special Volume in honour of Gordon Plotkin
5. M.E. Maietti. Quotients over Minimal Type Theory. In *Computation and Logic in the Real World - Third Conference of Computability in Europe, CiE 2007, Siena*, volume 4497, pages 517–531. Springer, 2007
6. G. Sambin. Doing without turing machines: Constructivism and formal topology. In *Computation and Logic in the Real World - Third Conference of Computability in Europe, CiE 2007, Siena*, volume 4497, pages 674–675. Springer, 2007

## Talks

1. “Proofs as programs via logical principles”. Talk given by M.E. Maietti on joint work with Giovanni Sambin Dipartimento di Informatica, Università di Torino, invited by Stefano Berardi, 18 October 2006.
2. “Intensionality vs.extensionality:a solution with two-levels of abstraction.” given by G. Sambin on joint work with M.E. Maietti at Workshop “Identity Types - Topological and Categorical Structure”, Uppsala (Sweden), 13-14 November 2006.
3. “From reactions to observations: the directed bigraphical model”. Talk given by Marino Miculan at the Institute of Cybernetics, Tallinn, 15 March 2007.
4. “An algebra for directed bigraphs”. Talk given by Davide Grohmann at TERMGRAPH 2007, 31 March 2007.
5. “Directed Bigraphs”. Talk given by Davide Grohmann at MFPS 2007, 14 April 2007.
6. P. Di Gianantonio, F. Honsell, and M. Lenisa. A type assignment system for game semantics, 2007. TYPES final workshop
7. “Origins and ideas of formal topology” and “The basic picture, a future for formal topology?” tutorial talks given by G. Sambin at “Third workshop in Formal Topology”, Padova, 7-12 May 2007
8. “A minimal two-level constructive foundation and its relevance to formal topology.” invited talk given by M. E. Maietti on joint work with G. Sambin at “Third workshop in Formal Topology”, Padova, 7-12 May 2007
9. "All the constructive compactifications of a frame" invited talk given by G. Curi at “Third workshop on Formal Topology”, Padova, 7-12 May 2007

10. "Bigraphical models of calculi with names". Talk given by Marino Miculan in Edinburgh, UK, May 2007.
11. "Proofs as programs via logical principles". given by M.E. Maietti on joint work with Giovanni Sambin al Dipartimento di Scienze dell'Informazione, Universita' di Bologna, invited by Claudio Sacerdoti Cohen, 30 May 2007.
12. "An algebraic road to predicativity" held by G. Sambin at PPS, Paris, France, invited by P. Curien, 5 June 2007.
13. "Two applications of dynamic constructivism: Brouwer's continuity principle and choice sequences in formal topology", talk given by G. Sambin at 1907-2007 : Cent ans d'intuitionnisme, Cerisy-La-Salle, France, 5-12 June, 2007
14. " Constructive foundation for mathematics as a two level theory: an example." invited talk given by M.E. Maietti on joint work with G. Sambin at Special session on "Doing without Turing Machines:Constructivism and Formal Topology" at the conference "Computability in Europe 2007: Computation and Logic in the Real World", Siena, 18-23 June 2007
15. "Doing without Turing Machines:Constructivism and Formal Topology" talk given by G. Sambin at Special session on "Doing without Turing Machines:Constructivism and Formal Topology" at the conference "Computability in Europe 2007: Computation and Logic in the Real World", Siena, 18-23 June 2007
16. "Completeness of temporal logic in a fully constructive metatheory" talk given by G. Sambin on joint work with F. Ciraulo at Algebraic and topological methods in non-classical logics III (TANCL'07) August 5-9, 2007, Oxford, England

### Dissertations

1. F. Ciraulo. *Constructive Satisfiability*. PhD thesis, Department of Mathematics, University of Palermo, March 2007. supervised by G. Sambin

### 8.13 Warsaw

**Correctness of Computer Systems** Jarosław Kuśmierek and Viviana Bono invented and developed an idea of a "modular object initialization" which, by replacing the classical constructor approach reduced code size, and complexity, while extending flexibility and composability of code pieces. The idea was evaluated as an extension of Java language called JavaMIP.

The same authors developed also a formal calculus named Featherweight-JavaMIP, which models the core of mentioned concept. They have proved that the calculus enjoys subject reduction property, as well as type soundness. Additionally, it was proven, that in this calculus all the null values are eliminated during the proces of initialization.

J. Kuśmierek with V. Bono introduced also the concept of "hygienic bindings" in object oriented languages, which removes many ambiguities. As a



result, this concept allows one to simplify the type system of such a "hygienic language", and extends the possibilities of code reuse and combination.

Aleksy Schubert together with Christian Haack, Erik Poll, Jan Schäfer proposed a type system to ensure immutability of objects in a Java-like language. An object is considered immutable if its internal state cannot be changed during its lifetime. This notion allows to find effective ways to verify correctness of certain Java programs.

Aleksy Schubert with Erik Poll did a verification of an SSH implementation. This verification was done using extended static checking tools which are related to the typing tools and methods investigated within the Types project.

**Foundational Research** Daria and Jacek Chrzęszcz investigated inductive consequences of a complete set of rewrite rules. They extended a standard lemma for the first-order rewriting to the higher-order rewriting on non-functional inductive types and presented a version of this lemma for rewriting involving terms of functional inductive types.

Aleksy Schubert proved that the existential fragment of the one-step parallel rewriting theory is undecidable.

Paweł Urzyczyn, together with Morten Heine Sørensen proved correctness of a syntactic translation from first-order to second-order propositional intuitionistic logic, proving in particular the undecidability of the  $\forall$ -free fragment of second-order propositional intuitionistic logic. These authors also proved cut-elimination for a system of sequent calculus representing Lorenzen dialogues for arbitrary connectives, and strong cut-elimination for a natural set of reductions for explicit substitutions (submitted).

**Formal Mathematics and Mathematics Education** Agnieszka Kozubek and Paweł Urzyczyn originated research of a naive type theory to be used in computer science education and everyday mathematics. This led to a study of a certain PTS system that was initiated with a strong normalization result (submitted).

**Proof technology** Based on their results about inductive consequences of rewriting in the Calculus of Constructions, Daria and Jacek Chrzęszcz presented a number of examples of Coq developments leading to novel technology of proving inductive lemmas in Coq. This can be further developed into a more general methodology. Our examples make extensive use of Coccinelle and Cime (a Coq rewriting library and termination prover respectively) developed by the Paris-Sud site.

## Publications

### Refereed journal papers

1. V. Bono, J. Kuřmerek, Modularizing constructors, Journal of Object Technology, vol. 6, no. 9, Special Issue. TOOLS EUROPE 2007, October 2007, pp. 297-317.
2. J. Kuřmerek, V. Bono, Introducing HygJava, Journal of Object Technology, vol. 6, no. 9, Special Issue. TOOLS EUROPE 2007, October 2007, pp. 209-229.

### Refereed conference papers

1. Christian Haack, Erik Poll, Jan Schäfer, Aleksy Schubert, Immutable Objects for a Java-like Language, *Proceedings of ESOP'2007*, Springer LNCS.
2. Jacek Chrząszcz and Daria Walukiewicz-Chrząszcz. "Towards rewriting in Coq", in Jouannaud Festschrift, Hubert Comon-Lundth, Claude Kirchner, and Hélène Kirchner, editors, LNCS 4600, Springer, 2007, pp. 113-131.
3. V. Bono, J. Kuśmierek "FJMIP: a calculus for a modular object initialization", In Proc. FCT 2007 pp. 100-112, LNCS 4639

### Talks

1. Daria Walukiewicz-Chrząszcz gave a talk "Inductive consequences in the Calculus of Constructions" (joint work with Jacek Chrząszcz) at Types meeting in Cividale, Italy in May 2007.
2. Daria Walukiewicz-Chrząszcz gave a talk "Inductive consequences in the Calculus of Constructions" at LRI, Université de Paris-Sud, France in June 2007.
3. Jacek Chrząszcz gave a talk "Proving inductive theorems in Coq" at LRI, Université de Paris-Sud, France in June 2007.
4. Jacek Chrząszcz gave a talk "Papuq: a Coq assistant" (joint work with Jakub Sakowicz) at PATE'07 workshop in Paris, France in June 2007.
5. Aleksy Schubert gave a talk "Verifying an implementation of SSH" (joint work with Erik Poll) at WITS'2007
6. Agnieszka Kozubek and Paweł Urzyczyn gave talks "In the search of a naive type theory" at the Types Conference in Cividale and at the PATE workshop in Paris.
7. V. Bono and J. Kuśmierek gave a talk "Hygienic methods - Introducing HygJava" at TOOLS EUROPE 2007 conference in Zürich
8. V. Bono and J. Kuśmierek gave a talk "Modularizing constructors" at TOOLS EUROPE 2007 conference in Zürich
9. Marcin Benke gave a talk "Agda Compiler" at 6th Agda Implementors Meeting in Goeteborg in June 2007.
10. Marcin Benke gave a talk "Alonzo — a Compiler for Agda" at Types meeting in Cividale in May 2007.

## 8.14 IoC Tallinn

**Correctness of Computer Systems** T. Uustalu, A. Saabas and M. J. Frade developed a foundational approach to certification of data-flow analyses where applied type systems are replaced with more foundational program logics.

**Foundational Research** T. Uustalu together with T. Altenkirch and V. Capretta worked on the monadic semantics of partiality from nontermination. T. Uustalu and V. Vene with T. Altenkirch studied the semantics of interactive input-output based on resumptions.

T. Uustalu, V. Vene and V. Capretta produced a preliminary account of the dual of wellfounded recursion, viz. antifounded corecursion.

T. Uustalu and V. Vene studied further certain aspects of the comonadic notions of computation.

M. Miculan and T. Uustalu worked on the general categorical theory of contexts and variable binding.

L. Pinto and T. Uustalu developed a novel proof search and countermodel construction procedure for bi-intuitionistic logic.

T. Uustalu and V. Vene gave a categorical semantics to an intuitionistic system of “circular proofs” and a higher-order sequent calculus reformulation. The first is a term calculus with guarded (co)recursion, the second is based on Mendler-style (co)recursion.

T. Uustalu, V. Vene and M. Hamana extended their previous work on representing cyclic datastructures via nested datatypes to representing datastructures with sharing via nested GADTs.

## Publications

### Refereed journal papers

1. T. Uustalu, V. Vene. Comonadic functional attribute evaluation. In M. van Eekelen, ed., *Trends in Functional Programming 6*, pp. 145-162. Intellect, 2007.

### Refereed conference papers

1. T. Uustalu, V. Vene. The essence of dataflow programming. In Z. Horváth, ed., *Revised selected lectures from 1st Central-European Functional Programming Summer School, CEFP 2005, Lect. Notes in Comput. Sci.*, v. 4164, pp. 135-167. Springer, 2006.
2. M. J. Frade, A. Saabas, T. Uustalu. Foundational certification of data-flow analyses. In *Proc. of 1st Joint IEEE/IFIP Symp on Theor Aspects of Software Engineering, TASE 2007*, pp. 107-116. IEEE CS Press, 2007.

**Talks** This is a selection only (only seminar talks and invited talks).

1. T. Uustalu, invited tutorial The many facets of structured (co)recursion, Coalgebra Miniworkshop, Radbound Univ. Nijmegen, 30 Oct 2006
2. T. Uustalu, talk Type-systematic and foundational data-flow analysis (coauthors M. J. Frade, A. Saabas), Univ. degli Studi di Udine, 23 Nov. 2006
3. T. Uustalu, talk Comonadic notions of computation (coauthor V. Vene), TRACES 2007, Ottawa, 28-30 April 2007

4. T. Uustalu, invited talk Circular proofs = Mendler in sequent form, HOR 2007, Paris, 25 June 2007
5. T. Uustalu, 10 h course Monads and more, School of CS & IT, Univ of Nottingham, 14-18 May 2007
6. T. Uustalu, talk How to be firmly antifounded (coauthors V. Capretta, V. Vene), Fun in the afternoon, Cambridge, 18 May 2007
7. T. Uustalu, 10 h course Monads and more, Univ. degli Studi di Udine, 2-6 July 2007
8. V. Vene, talk Comonadic notions of computation (coauthor T. Uustalu), Inst. of Comput. Sci., Radboud Univ. Nijmegen, 3 July 2007

## 8.15 Bergen

**Correctness of Computer Systems** We have finished the research on the abstract component languages and type systems which ensure that the number of simultaneously active instances of any component never exceeds a (sharp) bound expressed in the type. A final publication is under review.

**Foundational Research** Exponential behaviour has been found in an algorithm by Butkovič and Zimmermann for solving two-sided equations in max-algebra. The algorithm is therefore not polynomial. The question whether there is such a polynomial algorithm is (again) open. This has been an open problem for over 30 years.

**Proof technology** An Isabelle backend has been developed for our prover for Coherent Logic. Further experiments will be carried out in collaboration with Dr. S. Berghofer (TU München), who will visit Bergen 3-10 November.

**Formal Mathematics and Mathematics Education** We have finished the formal verification of Hessenberg's Theorem stating that Pappus' Axiom implies Desargues' Axiom in elementary projective plane geometry. Large parts of the verification have been automated. This research has been presented at the Sixth International Workshop on Automated Deduction in Geometry. The final publication is under review.

### Publications

#### Refereed conference papers

1. M.A. Bezem and D. Hendriks. *On the mechanization of the proof of Hessenberg's Theorem*. In F. Botana and E. Roanes-Lozano, editors, *Proceedings the Sixth International Workshop on Automated Deduction in Geometry*, pages 160-181, Universidad de Vigo, September 2006.

## Talks

1. M. Bezem, *On the mechanization of the proof of Hessenberg's Theorem in Coherent Logic*, Sixth International Workshop on Automated Deduction in Geometry, Universidad de Vigo, 02.09.2006

## 8.16 Helsinki

Work in the Helsinki subsite has been on proof theory and its applications. In the latter field, Sara Negri has worked on labelled systems for epistemic and tense logic, in particular, the logic of common knowledge, the logic of distributed knowledge, linear time logic and branching time logic. The research provides proof systems for the mentioned logics with decision algorithms that can be applied to knowledge databases. Part of this work has been done by students including Raul Hakli and Bianca Boretti.

A second main field has been proof systems for mathematics, especially such parts as elementary algebra, geometry, and arithmetic. The results include decision algorithms for various word problems for freely generated structures. In arithmetic, Annika Kanckos who studies with Jan von Plato has been able to solve an outstanding problem, namely a direct proof of the consistency of intuitionistic arithmetic within a system of natural deduction, where earlier proofs had used classical sequent calculi.

Sara Negri and Jan von Plato have almost finished a book-length presentation of their work on proof systems for mathematics.

Jan von Plato has also worked on the development of Gentzen's proof theory, especially his unpublished manuscripts. This topic is of interest for Types because Gentzen's proof systems have played an important role in the creation of constructive type theory.

## Publications

### Refereed journal papers

1. S. Negri, and B. Boretti, Equality in the presence of apartness: an application of proof analysis to intuitionistic axiomatics, *Philosophia Scientiae*, Cahier special 6, 2006, pp. 61-79.
2. J. von Plato, In the shadows of the Lowenheim-Skolem theorem: early combinatorial analyses of mathematical proofs, *The Bulletin of Symbolic Logic*, vol. 13, 2007, pp. 189-225.

### Refereed conference papers

1. S. Negri, Proof analysis in non-classical logics, in *Logic Colloquium '05*, ASL Lecture Notes in Logic, vol. 28, 2006, pp. 107-128.
2. S. Negri and R. Hakli, Proof theory for distributed knowledge, in *Computational Logic in Multi-Agent Systems (CLIMA VIII)*, Porto, Portugal.

## 8.17 Savoie

### Correctness of Computer Systems

**Foundational Research** R. David has given arithmetical proofs of the strong normalization for various calculi. The known proofs of such results generally use the so-called reducibility method and thus are not formalizable in Peano first-order arithmetic. Since the statement of strong normalization is a simple first-order formula, it was interesting to see whether or not the proof can be done in a simple theory.

In cooperation with K Nour, he has given such a proof for the simple typed  $\lambda$ -calculus with recursive equations on types. In cooperation with D Kesner, he has given such a proof for proof-nets of the MELL linear Logic.

He also has given a direct proof of the confluence of combinatory Logic, solving then an old problem appearing as the first problem of the TLCA list of open problems.

K. Kamareddine and K. Nour studied an intersection type system with a universal type in order to find a formal definition of abstract data types. They showed the soundness and completeness of a realizability semantics for their system and defined a class of types such that if a term inhabits a type in this class, then this term is normalisable and reduces to a closed term. Thus this class of types can be used to represent abstract data types.

### Formal Mathematics and Mathematics Education

**Proof technology** C. Raffalli (author of the PhoX proof assistant) started to develop a completely new proof assistant named PML. This proof assistant is based on an extension of the ML language with a type system based on a consistency check for some typing constraints (instead of a constraint solving algorithm) and extended with specifications. The key idea of the system is to use the power of our language to make the logical part of the system minimal. This results in a very original system (for instance one central piece of the proof-checking algorithm is a simplified but terminating version of the Knuth-Bendix completion algorithm for rewrite system). Moreover, the type system of our ML language seems powerful enough to handle the kind of modularity needed for a software library with formal proof or large developments of mathematics. Preliminary versions of the proof assistant is available from the web page <http://www.lama.univ-savoie.fr/~raffalli/pml> and a paper containing the consistency proof of the system is in preparation.

### Publications

#### Refereed journal papers

1. R. David et K. Nour, Arithmetical proofs of strong normalization results for symmetric lambda calculi. *Fundamenta Informaticae*, vol 77, num 4, pp. 489-510, 2007.
2. F. Kamareddine et K. Nour A completeness result for a realisability semantics for an intersection type system. *Annals of Pure and Applied Logic*, vol 146, pp. 180-198, 2007.

## 8.18 Swansea

**Correctness of Computer Systems** M. Roggenbach has made progress in the development of CSP-Prover (2 new releases). A new theorem prover CSP-CASL prover has been developed. As a new insight, CSP has been described in the logical framework of an institution. A complete semantics for the CSP stable failures model has been presented - it was an open question for 25 years, if there was such a semantics.

A. Setzer and U. Berger are working together with a PhD student (R. Abdul Rauf, Shah Alam, Malaysia) on an integration of functional concepts into object-oriented languages, in particular C++. They implemented a parser-translator program that embeds the simply typed lambda-calculus into C++ and proved its correctness. This research resulted in 3 refereed conference proceedings and 1 journal publication.

**Foundational Research** U. Berger is investigating the dependency of the truth of statements about higher type functionals (formulated in the language of  $HA^\omega$ ) on the model where the statement is interpreted. He was able to characterise the prefix classes of formulas where truth in the full type structure implies truth in other models like the continuous functionals and the hereditarily effective operations.

U. Berger has developed a domain-theoretic method for proving termination of lambda-calculi extended by rewrite systems. The results have been partially obtained in collaboration with T. Coquand and A. Spiewack from Chalmers, Gothenburg.

U. Berger is working in collaboration with an MSc student (Tie Hou, now in Amsterdam) on coinductive specifications and correctness proofs of exact real number algorithms.

### Formal Mathematics and Mathematics Education

**Proof technology** U. Berger and M. Seisenberger are investigating the machine assisted formalization and verification of cryptographic algorithms and security protocols.

A. Setzer has developed the integration of concepts from object-oriented programming into C++. This research resulted in 2 conference proceedings.

### Publications

#### Refereed journal papers

1. U. Berger. Continuous semantics for strong normalization. *Mathematical Structures in Computer Science*, 16:751–762, 2006
2. Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, 82:27–51, 2006

## Refereed conference papers

1. Anton Setzer. Object-oriented programming in dependent type theory. In *Conference Proceedings of TFP 2006*, 2006. Available from <http://www.cs.nott.ac.uk/nhn/TFP2006/TFP2006-Programme.html> and <http://www.cs.swan.ac.uk/csetzer/index.html>.
2. Rose H. Abdul Rauf, Ulrich Berger, and Anton Setzer. Functional concepts in C++. In *Conference Proceedings of TFP 2006.*, 2006. Available from <http://www.cs.nott.ac.uk/nhn/TFP2006/TFP2006-Programme.html> and <http://www.cs.swan.ac.uk/csetzer/index.html>.
3. Will Harwood, Faron Moller, and Anton Setzer. Weak bisimulation approximants. In Zoltán Ésik, editor, *Computer Science Logic. 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 25-29, 2006. Proceedings*, volume 4207, pages 365 – 379. Springer Lecture Notes in Computer Science, 2006.
4. Anton Setzer. Partial recursive functions in Martin-Löf Type Theory. In Arnold Beckmann, Ulrich Berger, Benedikt Löwe, and John V. Tucker, editors, *Logical Approaches to Computational Barriers: Second Conference on Computability in Europe, CiE 2006, Swansea, UK, June 30-July 5, 2006. Proceedings.*, pages 505 – 515. Springer Lecture Notes in Computer Science 3988, 2006.

## Talks

1. U. Berger, Swansea. Computational interpretations of subsystems of analysis. Lisbon, Portugal, September 2007.
2. U. Berger, Swansea. Truth in higher types. Dagstuhl, Germany, April 2007.
3. U. Berger, Swansea. A domain-theoretic strong normalisation theorem for non-deterministic higher-order rewrite systems. Max Planck Institute, Bonn, Germany, June, 2007.
4. U. Berger, Swansea. Applications of domain theory to termination problems. LMU München, Germany, June, 2007.
5. (September 2007) U. Berger, Swansea. A domain-theoretic characterisation of strong normalisation for the Lambda-R-calculus. Sobolev Institute, Novosibirsk, Russia, September, 2007.
6. Anton Setzer, Swansea. Proof theory and Martin-Löf Type Theory. Invited plenary talk at conference “1907 – 2007, cent ans d’intuitionnisme”, Cerisy, France, June 2007.
7. Anton Setzer, Swansea. Partial-recursive functions in Martin-Löf Type Theory. Invited talk at Workshop Proof and Computation II, held on occasion of Helmut Schwichtenberg’s 65 birthday, June 2007.
8. Anton Setzer, Swansea. Inductive-recursive definitions and partial-recursive functions. TYPES 2007, Udine, Italy, May 2007.



9. Anton Setzer, Swansea. Teaching Agda. Agda Implementor's Meeting 6, Gothenburg, Sweden, May 2007.
10. Anton Setzer, Swansea. Guarded recursion in dependent type theory. Agda Implementor's Meeting 6, Gothenburg, Sweden, May 2007.
11. Anton Setzer, Swansea. Inductive-recursive definitions and partial recursive functions. British Mathematical Colloquium, Swansea, April 2007.
12. Anton Setzer, Swansea. Weak bisimulation approximants. CSL 2006, Szeged, Hungary, September 2006.
13. Anton Setzer, Swansea. Partial recursive functions and the recursion theorem in Martin-Löf Type Theory. Informal Seminar talk, Nottingham, England, September 2007.
14. Anton Setzer, Swansea. Object-oriented programming in dependent type theory. Seminar Talk, Royal Holloway, England, September 2007.
15. Anton Setzer, Swansea. Inductive-recursive definitions and partial-recursive functions. Seminar Talk, Birmingham, England.
16. Anton Setzer, Swansea. Partial recursive functions in Martin-Löf Type Theory. Seminar talk, Graduate School of Science and Technology, Kobe, Japan, . November 2006.
17. Markus Roggenbach (Swansea), CSP-CASL: Semantics, Application, Tools. Algebraic Specification Seminar, Swansea, 28 September 2006.
18. Temesghen Kahsai (Swansea), Towards semi automated equivalence checking of spi calculus processes. Algebraic Specification Seminar, Swansea, 30 November 2006.
19. Markus Roggenbach (Swansea), CSP-Prover. IFIP WG 1.3 Meeting, Braga, Portugal, March 2007.
20. Liam O'Reilly (Swansea), Implementing CSP-CASL. BCTCS 2007, Oxford, UK, April 2007.
21. Temsghen Kahsai (Swansea). Resting from CSP-CASL Specification. BCTCS 2007, Oxford, UK, April 2007.
22. Gift Samuel (Swansea). Implementation of the Stable Revivals Model in CSP-Prover. BCTCS 2007, Oxford, April 2007.
23. Markus Roggenbach (Swansea). CSP - neue Einsichten in ein altes Paradigma. Humboldt University Berlin, Germany, July 2007.
24. Markus Roggenbach (Swansea). CSP-Prover. University of Pretoria, South Africa, July 2007.
25. Liam O'Reilly (Swansea). Implementing CSP-CASL. CALCO-Jnr 2007, Bergen, Norway, August 2007.
26. Markus Roggenbach (Swansea). Proof Principles for Process Algebra - CSP-Prover in Practice, LDIC, Bremen, Germany, August 2007.

## 8.19 Toulouse

**Foundational Research** Sergei Soloviev continued his work on non-standard reductions in typed lambda-calculi. Recently interesting progress was done in the study of such reductions in dependent type systems. Work in progress concerning in particular reductions related to finite types in dependent type systems was presented at HOR workshop (joint work by S. Soloviev and his ph.d. student L. Marie-Magdeleine).

Ralph Matthes continued his foundational research on normalization problems and developed a new collaboration with Minho site (Braga), which resulted in a publication.

**Formal Mathematics and Mathematical Education** The paper by S. Soloviev and L. Mehats using proof-theoretical methods for verification of commutativity of algebraic diagrams in non-free categorical models was revised and published in “Annals of Pure and Applied Logic” (the paper was mentioned as submitted in previous report).

In continuation of this work S. Soloviev and A. El-Khoury (ph.d. student of S. Soloviev) are studying the action of symmetry groups on derivations and related categorical diagrams.

S. Soloviev and Z. Luo (RHUL) were collaborating on the applications of coercive subtyping to linguistics.

S. Soloviev was working on problems of history of type theory and axiomatics (collaboration outside “Types”, with O. Antonova from S. Petersburg University). The results are of interest to “Types” community and were presented in Helsinki during the visit of S. Soloviev.

### Publications

#### Refereed journal papers

1. L. Mehats, S. Soloviev Coherence in SMCCs and equivalences on derivations in IMLL with unit. - *Annals of Pure and Applied Logic*, 147/3 pp. 127-179 (july 2007)
2. Olga Antonova, Sergei Soloviev. Axiomatics and Evidence. (in Russian) - In: *Logico-Philosophical Studies*, 4, p. 3-11, St. Petersburg University, 2006.

#### Refereed conference papers

1. José Espírito Santo, Ralph Matthes, Luís Pinto. Continuation-Passing Style and Strong Normalisation for Intuitionistic Sequent Calculi. In: *Typed Lambda Calculi and Applications*, Paris, France, 26/06/2007-28/06/2007, Volume 4583, Simona Ronchi Della Rocca (Eds.), Springer-Verlag, Lecture Notes in Computer Science, p. 133-147, juin 2007.
2. Sergei Soloviev, Olga Antonova. Axiomatics and its Model Interpretation from the Historical Perspective. In : *The Classical Model of Science*, Vrije University, Amsterdam, 10/01/2007-13/01/2007, Vrije Universiteit, p. 18-19, janvier 2007.

## Refereed workshop papers

1. Lionel Marie-Magdeleine and Serguei Soloviev. Non-standard reductions in simply-typed, higher order and dependently-typed systems. (Short abstract.) - In: Proceedings 4th International Workshop on Higher-Order Rewriting, Paris, 25/06/2007 - 25/06/2007, IRIT, juin 2007 (ed. R. Matthes).

## 8.20 Birmingham

**Correctness of Computer Systems** Ritter, Adetoye and Ryan continued their work on developing type systems to characterise information flow. We extended our policy framework for specifying the degree of permissible information flow to non-deterministic programs.

**Foundational Research** Together with Michael Mendler from Bamberg Eike Ritter is investigating the completeness of certain Kripke models for modal logic. This work is relevant to the verification of hardware where the modal logic is used to model time constraints. We are also investigating how proof search in such a logic may be modelled by games.

**Proof technology** Together with his PhD-student Derrick Newton Ritter is modelling information flow conditions in workflow systems by adding type systems to suitable process calculi.

## 8.21 Nottingham

### Foundational Research

#### Containers [Altenkirch, Ghani, Hancock, McBride, Morris, Swierstra

] Our growing team of researchers continues to develop this powerful treatment of the 'strictly positive' data structures which lie at the heart of programming. Our refined treatment of 'Indexed Containers' gives both a theoretical rationalisation and a practical generalisation of the datatypes to be found in systems like Agda, Coq and Epigram. This research forms the basis for the treatment of datatypes in Epigram 2. We continue to study aspects such as isomorphisms, differential structure, etc.

**Observational Equality [Altenkirch and McBride ]** Our quest for a type theory whose computational equality reflects the execution of programs and is decidable, but whose 'reasoning' equality reflects the intuitive notion of being 'the same as far as we can observe' is bearing fruit. A candidate system has been identified and implemented experimentally as part of Epigram 2. Its components have been analysed into a 'proof-relevant' core, which has been justified by a model construction, and a 'proof-irrelevant' extension, whose correctness remains subject to conjecture.

**Continuous Functions on Final Coalgebras [Ghani and Hancock ]** We have developed a presentation of 'live' processes which consume and produce infinite data structures, generalising from streams to arbitrary containers. The processes are themselves represented via datatypes which are

mutually coinductive (guaranteeing that writing will eventually start) and inductive (guaranteeing that reading will eventually stop).

**Correctness of Computer Systems** The development of the Epigram 2 dependently typed functional programming language and integrated development environment is now well under way at Nottingham. The team (Conor McBride, James Chapman, Peter Morris, Wouter Swierstra and Joel Wright) have been hard at work improving all aspects of the system's design in the light of research from Nottingham and elsewhere. In particular, our foundational research on Dependent Pattern Matching, Indexed Containers and on Observational Type Theory is now being integrated directly into the Epigram system. Moreover, some technology arising from the implementation of Epigram is novel in itself. The system continues to be used in teaching, and has now acquired a wealth of examples and tutorial material. See <http://www.e-pig.org/>.

## Publications

### Refereed journal papers

1. Graham Hutton and Joel Wright. What is the Meaning of These Constant Interruptions? *Journal of Functional Programming*, 2007. to appear
2. N Ghani and P Johann. Monadic augment and generalised short cut fusion. *Journal of Functional Programming*, 2007. Accepted for Publication
3. Conor McBride and Ross Paterson. Applicative programming with effects. *Journal of Functional Programming*, 2007. forthcoming article available online

### Refereed conference papers

1. Peter Morris, Thorsten Altenkirch, and Neil Ghani. Constructing strictly positive families. In *The Australasian Theory Symposium (CATS2007)*, January 2007
2. Wouter Swierstra and Thorsten Altenkirch. Beauty in the beast. In *The Haskell Workshop*, 2007
3. Thorsten Altenkirch, Conor McBride, and Wouter Swierstra. Observational equality, now! In *Programming languages meet program verification (PLPV)*, 2007
4. Thorsten Altenkirch, Conor McBride, and Peter Morris. *Generic Programming*, chapter Generic Programming with dependent types. Springer, 2007
5. N Ghani and P Johann. Initial algebra semantics is enough! In *Proceedings of TLCA 2007*, number 4583 in Lecture Notes in Computer Science, pages 207–222. Springer-Verlag, 2007
6. N Ghani and A Kurz. Higher order trees, algebraically. In *Proceedings of CALCO 2007*, Lecture Notes in Computer Science. Springer-Verlag, 2007. To appear

## Books

1. Graham Hutton. *Programming in Haskell*. Cambridge University Press, January 2007

## Dissertations

1. Peter Morris. *Constructing Universes for Generic Programming*. PhD thesis, University of Nottingham, 2007

## 8.22 Kraków

**Foundational Research** We investigated the size of the fraction of tautologies (inhabited types) against the number of all formulas (types) for implicational logic, in particular the asymptotic behavior of this fraction.

We proved that asymptotically intuitionistic and classical logics are identical. Research on asymptotic probabilities in logic has already resulted in PhD work prepared in Jagiellonian University and defended in 2006.

We continue investigated the computational models of Banach spaces and characterized continuous posets which are partially metrizable in their Scott topology.

## Publications

### Refereed journal papers

1. Lidia Badura, Marek Zaionc, "Parametrizability by regular expressions for equations on words", *Bulletin of the Section of Logic*, Vol. 36:1/2 (2007) pp 79 - 93.
2. Zofia Kostrzycka, Marek Zaionc *Asymptotic densities in logic and type theory*, accepted at *Studia Logica* .
3. Paweł Waszkiewicz, *Partial metrisability of continuous posets*, *Math. Structures in Comp.Sci.*16(2) (2006), pp.359-37.

### Refereed conference papers

1. Herve Fournier, Daniele Gardy, Antoine Genitrini, Marek Zaionc "Classical and intuitionistic logic are asymptotically identical", *Computer Science Logic 2007*, *Lecture Notes in Computer Science* 4646, pp 177-193.

## Talks

1. Z. Kostrzycka, M. Zaionc "Asymptotic densities in logic and type theory" *Trends in Logic IV*, Toruń, Poland, September, 2006.
2. Classical and intuitionistic logic are asymptotically identical, *TYPES 2007*, Conference of the Types Project, 2-5 May 2007 Cividale del Friuli (Udine), Italy.
3. "Asymptotic Densities in Logic", seminar, Computer Science Department, University of Savoy, Savoie, France, lipiec 2007.

## Dissertations

1. Jakub Kozik, "Decidability of relative density in Chomsky hierarchy of languages" PhD thesis Jagiellonian University, November 2006.

## 8.23 Bamberg

**Correctness of Computer Systems** Synchronous programming languages (such as Statecharts, Esterel, Signal, Lustre, Lucid Synchrone) are becoming increasingly successful in the avionics and automotive industries for the high-level design of embedded real-time systems. The key advantage is their rigorous mathematical semantics which facilitates model-driven design and verification. However, the synchrony hypothesis, which involves the solution of non-monotonic fixed-point equations, poses a notorious compositionality problem: the synchronous response of a composite system is not the classical conjunction of the synchronous responses of the system's components. Moreover, causality paradoxes can arise in cyclic compositions such that the execution of a component depends on its own inhibition. The Bamberg group has shown how to solve these problems by using constructive semantics based on game-theory and intuitionistic type theory. We have shown how the type theory PST (*Propositional Stabilisation Theory*, developed earlier by Mendler) can be used as an interface language specifying the causal and timing responses of synchronous components in a compositional fashion. Our aim is to propagate PST as a type system for compilers of synchronous programming languages.

**Proof technology** Our work on Lax Types is described above (scientific collaboration) and in the Sheffield site report.

## Talks

1. Michael Mendler, *A constructive type theory for the timing analysis of synchronous distributed systems*, Department of Computer Science, University of Kiel, 21. Oct 2005.
2. Michael Mendler, *Interface Types for Causality and Timing Analyses*, SYNCHRON Workshop on Synchronous Languages, Malta, 21. Nov 2005.
3. Michael Mendler, *Typsysteme für visuelle komponentenbasierte Programmierungsumgebungen, Modellierung und Verifikation von Sicherheitsprotokollen*, IT-Cluster Oberfranken, Innovations und Gründerzentrum (IGZ) Bamberg, 30. Nov 2005.

## 8.24 Stockholm – Uppsala

**Constructive type theory** Per Martin-Löf has been working on sheaf models of type theory. PhD-student Johan Granström is working on meta-variables and eager evaluation strategies for type theory.

**Constructive/Effective Topology** The group in Uppsala (E.Palmgren, V. Stoltenberg-Hansen, and PhD-students G.Hamrin, F.Dahlgren) has been working extensively on constructive or computable aspects of topology: representation of spaces via Scott-domains, and point-free topology and its formalisation in type theory.

**Category theory and dependent types** Richard Garner from Cambridge is working on categorical models of intensional type theory. PhD-student Olov Wilander is currently working on proof-theoretic aspects of quasi-equational theories (partial Horn logic). These are related to Cartmell's generalised algebraic theories (under which Martin-Lof type theory fall). Palmgren has been working on a choice free formulation of locally cartesian closed categories, naturally arising from setoids.

## Publications

### Refereed journal papers

1. Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren, Peter Schuster) Binary refinement implies discrete exponentiation. *Studia Logica*, *Studia Logica*, 84 (2006), 361 - 368.
2. R. Garner. Double clubs. *Cahiers de Topologie et Geometrie Differentielle Categoriqes*, 47(2006), 261-317.
3. Erik Palmgren and Steve J. Vickers. Partial Horn logic and cartesian logic. *Annals of Pure and Applied Logic*, 145(2007), 314-355.
4. Erik Palmgren. A constructive and functorial embedding of locally compact metric spaces into locales. *Topology and its Applications*, 154 (2007), 1854 - 1880.
5. Jesper Carlström. A constructive version of Birkhoff's theorem. *Mathematical Logic Quarterly*, accepted for publication.
6. F. Dahlgren. Partial Continuous Functions and Admissible Domain Representations. *Journal of Logic and Computation*, accepted for publication.
7. Erik Palmgren. Resolution of the uniform lower bound problem in constructive analysis. *Mathematical Logic Quarterly*, accepted for publication.
8. Erik Palmgren. Locally cartesian closed categories without chosen constructions. *Theory and Applications of Category Theory*, accepted for publication.

## Talks

1. R. Garner. The theory of glueing things on. Category Theory '07, Carvoeiro
2. P. Martin-Löf. Topology, probability, quantum theory. Third workshop on formal topology, Padova, May 9-12, 2007.

3. E. Palmgren. Locally compact metric spaces and formal topology. Third workshop on formal topology, Padova, May 9-12, 2007.
4. E. Palmgren. Fest-kolloquium for Helmut Schwichtenberg, München, June 22-23, 2007.

## 8.25 Novi Sad - Belgrade

**Foundational Research** We develop an intersection type system for the  $\lambda\mu\tilde{\mu}$  calculus of Curien and Herbelin. This calculus provides a symmetric computational interpretation of classical sequent style logic and gives a simple account of call-by-name and call-by-value. The present system improves on earlier type disciplines for  $\lambda\mu\tilde{\mu}$ : in addition to characterizing the  $\lambda\mu\tilde{\mu}$  expressions that are strongly normalizing under free (unrestricted) reduction, the system enjoys the Subject Reduction and the Subject Expansion properties. Another line of research is to revisit in classical logic the known connection of natural deduction, sequent calculus and cut elimination in classical logic.

**Formal Mathematics and Mathematics Education** Within the bilateral project "Distance learning in the area of computer supported mathematical education" with Mathematics Department, University of Maribor, Slovenia, Novi Sad has started the discussion of strategies for constructing a common database of mathematical tools for learning logic, linear algebra and to involve formal methods developed in the TYPES project.

### Refereed journal papers

1. K. Došen, Z. Petrić: "Medial commutativity", *Annals of Pure and Applied Logic* 146(2007), pp. 237-255 (<http://arXiv.org/math/0610934>)
2. D. Dougherty, S. Ghilezan, P. Lescanne: "Characterizing strong normalization in the Curien-Herbelin symmetric lambda calculus: extending the Coppo-Dezani heritage", *Theoretical Computer Science* (special issue "Festschrift Coppo, Dezani, Ronchi", eds S. Berardi, U de' Liguoro) (to appear 2007)
3. K. Došen: "Models of deduction", *Synthese* 148 (2006) pp 639-657 (*Mathematical Reviews* 2007a:03078)
4. K. Došen, Z. Petrić: "Proof-Net Categories", *Polimetrica*, Monza, 2007, viii+147 pp. (electronic version at the Polimetrica site and at: <http://www.mi.sanu.ac.yu/kosta/pn.pdf>)

### Refereed conference papers

1. D. Dougherty, S. Ghilezan, P. Lescanne: "A general technique for analysing termination in symmetric proof calculi", *Proceedings of the 9th International Workshop on termination, WST'07* (D.Hofbauer, A.Serebrenik eds) pp 86–90.



2. K. Došen, Z. Petrić: "Symmetric self-adjunctions: A justification of Brauer's representation of Brauer's algebras", in: N. Bokan et al. eds, Proceedings of the Conference "Contemporary Geometry and Related Topics", Faculty of Mathematics, Belgrade, (2006) pp 177-187 ([http:// arXiv. org/ math. RT/ 0512102](http://arXiv.org/math.RT/0512102))
3. K. Došen, Z. Petrić: "Coherence and confluence", in: J.-Y. Béziau and A. Costa-Leite, eds, Perspectives on Universal Logic, Polimetrica, Monza, 2007, pp. 205-215 ([http:// arXiv. org/ math. CT/ 0506310](http://arXiv.org/math.CT/0506310))

### Dissertations

1. J. Ivetić: "Term calculi for intuitionistic sequent calculi " Master of Science Thesis, Faculty of Engineering, University of Novi Sad, 2007

## A Appendix 1 – Plan for using and disseminating the knowledge

### A.1 Exploitable knowledge and its Use

Our research is basic in its nature and it is difficult at this moment to point to some product or service which could come as a result of our work.

### A.2 Dissemination of knowledge

Most of the sites are universities. One of the main purpose of a university is exactly dissemination of knowledge. The most important method is to teach graduate and undergraduate students. After graduation most of them will continue to work outside the university.

As scientists, we disseminate our work also in the traditional ways earlier described in this report (published journal papers, conference papers, workshop presentations, lectures in the summer school and visits).

Our proof systems (including Coq, Agda, Isabelle and Mizar) are a significant means of dissemination. They are all freely available on the internet, including documentation, examples, and large and growing libraries of formalised mathematics and computer science. They are widely used by researchers and students, also outside our consortium. Several impressive proof developments have been carried out. A large number of advanced students have used these systems, and then go on to disseminate this work further in industry and academia.

We also have dissemination activities for industrial needs. Many participating teams have strong collaborations with industrial partners, in the area of critical systems development (smartcard technology for instance) or proof presentation, some of them (France Telecom, Dassault Aviation) being part of the consortium. We have and will invite our industrial contacts to participate in annual and thematic workshops, giving them the opportunity to present challenging problems or interesting case studies. In the past, sites have organised training in their tools and methodology in a format suitable for industry (a few days of hands-on tutorial, accessible with no previous theoretical knowledge).

The students we are training are natural candidates for employment in industry specialized in formal methods. More than that, bright students who feel comfortable with a new technology don't just fill the skill needs of industry, they accelerate technology transfer by encouraging their employers to use the technology they are familiar with. Their success in addressing some industrial problems can encourage industrial employers to experiment further with new technology.

Here are some concrete examples of how members have been present in media:

- H. Geuvers. Computer-ondersteund redeneren: de boekhouder steunt de denker (Dutch). *Automatisering Gids*, 10:page 15, March 9 2007

### **A.3 Publishable results**

There are not yet any economically exploitable results of the project.