510996

Types

Types for Proofs and Programs

Coordination Action
FP6-2002-IST-C

Periodic activity report no 1, revised version

Period covered: Sept 1, 2004 – Aug 31, 2005

Date of preparation: March 17, 2006

Duration of project: Sept 1, 2004 – Aug 31, 2007

Coordinator: Bengt Nordström, Chalmers University of Technology

Contents

1 Project objectives and major achievements 6

1.1 Relationship to other type-related research. 6

2 Work-package progress 6

2.1 WP 1: Coordination and evaluation 6

2.1.1 D1: periodic project reports 6

2.2 WP 2: TYPES 2004 conference 7

2.2.1 D4: The Paris meeting 7

2.2.2 D7: Informal Types proceeding 7

2.2.3 D10: Refereed Types Proceedings 7

2.3 WP 3: Thematic workshops 7

2.3.1 D12: Small Workshop: Types for Mathematics / Libraries of Formal Mathematics 7

2.3.2 D18: Thematic workshop proceedings, available at the workshop and through our www-site 8

2.3.3 D13: Small Workshop: High Level Languages for Proofs . 8

2.3.4 D19: Thematic workshop proceedings, available at the workshop and through our www-site 8

2.4 WP 4: Education 8

2.4.1 D24: Summer school 8

2.4.2 D25: Lecture notes of the summer school 9

2.5 WP 5: Visits between sites 9

2.6 WP 6: The Types web page 12

2.6.1 D30 The www-site 12

3 Consortium management 13

4 Involvement in other EU projects 14

5 Industrial cooperation 15

6 Coauthored papers and presentations 16

7 Major scientific results 19

7.1 Chalmers 20

7.2 CNRS – Paris 7 25

7.3 INRIA-Futurs 27

7.4 INRIA-Sophia 31

7.5 Paris – Sud 33

7.6 Munich – LMU 36

7.7 Munich – TU 39

7.8 Nijmegen 42

7.9 Bialystok 44

7.10 Royal Holloway 46

7.11 Edinburgh 47

7.12 Manchester 48

7.13 Torino 50

7.14 Udine 51

7.15 Warsaw 52

7.16 Tallinn 53
7.17 Bergen 55
7.18 Helsinki 56
7.19 Minho 57
7.20 Padova 58
7.21 Savoie 60
7.22 Swansea 61
7.23 Toulouse 63
7.24 Birmingham 64
7.25 Nottingham 66
7.26 Sheffield 67

A Appendix 1 – Plan for using and disseminating the knowledge 68
A.1 Exploitable knowledge and its Use 68
A.2 Dissemination of knowledge 68
A.3 Publishable results 68

Summary of the Types project, 1.9.2004 – 31.8.2005

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, six smaller thematic workshops on designated research themes, one summer school, short courses and short visits between sites.

The consortium consists of 35 research groups from universities and industries in Europe. It is coordinated by Bengt Nordström (Chalmers University, Göteborg, Sweden). 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 hierachy 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, Munich – LMU, Munich – 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 first annual report. During this year we organized the Types 2004 Conference, one summer school, two small workshops and had many short visits between the sites.

Types 2004 Conference. The meeting took place on Campus Thales in Jouy-en-Josas in France in December 15 – 18, 2004. It attracted 103 participants and there were 51 regular presentations.

Types Summer School. The school took place during two weeks in the end of August in 2005 on Hisingen in Sweden. The school attracted 89 students from Europe, Asia, Latin America and North America.

Small Workshop: Types for Mathematics / Libraries of Formal Mathematics. This workshop took place in Nijmegen, Netherlands on November 1 – 2, 2004 and attracted 28 participants.

Small Workshop: High Level Languages for Proofs. The workshop took place at the LAMA near Chambery in France on April 13 – 14, 2005 and had 15 participants.

A more detailed description of the Types project can be found on the Types home-page:

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

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.

The consortium is mainly working 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.

A more detailed description of our work in these areas is found in section 6.

1.1 Relationship to other type-related research.

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 have 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).

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 school, the annual Types meeting, small workshops and individual visits. For instance, in 2006, the Types meeting will be colocated with TFP 2006 (Trends in Functional Programming). We have joint sessions, keynote speakers and social events.

2 Work-package progress

All deliverables proposed for the first year are completed. The current status of all deliverables for each work-package is described below.

2.1 WP 1: Coordination and evaluation

2.1.1 D1: periodic project reports

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

2.2 WP 2: TYPES 2004 conference

2.2.1 D4: The Paris meeting

The Types conference took place in December 15-18, 2004 on Campus Thales in Jouy-en-Josas in France.

The workshop was organized by INRIA-Futurs (H. Herbelin, B. Werner) and Université Paris-Sud (J.-C. Filliâtre, C. Paulin).

The topic of this conference is formal reasoning and computer programming based on Type Theory : languages and computerized tools for reasoning, and applications in several domains such as analysis of programming languages, certified software, formalization of mathematics and mathematics education.

There were 103 participants attending the conference. We had 51 regular presentations, 5 tools demonstrations and 2 shorter poster presentations. There were three invited speakers : Zhong Shao (Yale University) presented his work on "The Essence of Proof-Carrying Code"; Tom Hales (Pittsburgh University) gave a talk entitled "Toward a formal proof of the Kepler Conjecture" and Per Martin-Löf (Stockholm University) was speaking on "100 years of Zermelo's axiom of choice: what was the problem with it?"

2.2.2 D7: Informal Types proceeding

The notes of the talks can be found at the home page `http://types2004.lri.fr/`

2.2.3 D10: Refereed Types Proceedings

As for previous Types conferences, there was a post-conference call for papers. We received 33 submissions which have been fully refeered. Finally 17 papers were accepted, and they will soon be published by Springer-Verlag in a volume (LNCS 3839) of the LNCS series. This deliverable is not due during this reporting period.

2.3 WP 3: Thematic workshops

2.3.1 D12: Small Workshop: Types for Mathematics / Libraries of Formal Mathematics

The workshop took place in Nijmegen on November 1 – 2, 2004.

The workshop was held at the campus of the Radboud University Nijmegen. The topics of the workshop were (inclusive, but not limited to):

- Formalizing mathematics using type theory
- Type theory as a foundational basis for mathematics
- Repositories of formalized mathematics
- Interaction with / presentation of (esp. large) bodies of formalized maths

There were two invited speakers, the first funded from the Types budget and the second funded from local sources: Robert L. Constable (from Cornell) speaking on "Foundations for the Management of Formal Mathematical Knowledge" and Bruno Buchberger (Linz) speaking on "Proving from first and intermediate principles". Apart from this, there were 13 contributed talks. There were 28 participants, providing for lively discussions at and around the talks.

2.3.2 D18: Thematic workshop proceedings, available at the workshop and through our www-site

The notes of the talks can be found at the home page `http://www.cs.ru.nl/fnds/typesworkshop/`.

2.3.3 D13: Small Workshop: High Level Languages for Proofs

This workshop took place on April 13 – 14 at the LAMA near Chambery.

The topic of the workshop is the development of language for proofs that would allow proofs to be

- robust (that can be easily adapted to small changes in the theorem),
- readable (by a human),
- portable (from one theorem prover to another)

The workshop started with an introduction to the Mizar system, which was valuable, since this system is very powerful but not very well-known among the type community.

2.3.4 D19: Thematic workshop proceedings, available at the workshop and through our www-site

There were 15 participants and the full program of the workshop is available at `www.lama.univ-savoie.fr/ raffalli/types-workshop.html`.

2.4 WP 4: Education

2.4.1 D24: Summer school

The Types summer school took place on Hisingen, Göteborg, Sweden on August 15 – 26, 2005. 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). There were introductory and advanced lectures on lambda calculus, type theory, logical frameworks, program extraction, and other topics with relevant theoretical background. Several talks were devoted to applications.

Three state-of-the-art proof assistants were presented during the school: Coq, Isabelle and Agda. Participants were given extensive opportunities to use the systems for developing their own proofs.

The school had 89 students (this is more than we anticipated, it is clear that the interest in this topic is increasing). There were 20 lecturers, the top specialists in the world. There were 22 students who could get partial support for their expenses. This was paid by money from the Types project (which also paid some of the expenses for the lecturers).

The students could borrow personal laptops with pre-installed proof systems. This was a very positive experience, there were students working all the time and everywhere! When the building was closed at 10 p.m., there were always some students who stayed longer.

2.4.2 D25: 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 (`www.cs.chalmers.se/Cs/Research/Logic/TypesSS05`).

2.5 WP 5: Visits between sites

There is plenty of interaction between the sites, most of them is shown in the table on page 10. The following is a short list of talks given during some of the short visits:

- Marino Miculan visited Edinburgh in 3-12 April 2005 and gave a a talk about "Models of Variables and Names" (joint work with K.Yemane). [1]

- Furio Honsell visited Edinburgh in 1-3 April 2005 and gave a talk about "Set theoretic functors" (joint work with D. Cancila, M. Lenisa). [1]

- Assia Mahboubi (Inria Sophia-Antipolis) gave a talk in Nijmegen on March 8 with the title “Induction over real numbers”. [1]

  We have a constructive look at a quite elementary lemma of real classical real analysis which can be considered as an "open induction principle". Following an idea of Th. Coquand, who has proved the result for the dyadic Cantor set, we provide a new constructive proof also using monotone bar induction. This latter proof works directly with the real numbers and an appropriate kind of real open sets. The computational content of such an induction principle over real numbers is quite easy to extract but it would be rather interesting to understand its status in the hierarchy of non-classical axioms.

- Monday 31 Jan Pierre Letouzey (Munich) gave a talk in Nijmegen “Extraction in Coq and modular proofs and programs” [1]

  Almost since its origin, the Coq proof assistant includes a mechanism named extraction. This tool allows us to automatically generate certified programs from constructive proofs formalized in Coq. These extracted programs are written in functional languages, more precisely Ocaml or Haskell. During my PhD, I've completely redesigned this Coq extraction, in order to extend its range of use. In fact, the previous extraction was indeed suffering several important limitations: it was refusing some Coq proofs and was even able to generate incorrect programs in some situations. In a first part, I will describe the current state of this new extraction Coq at the end of my PhD and present both the implementation and the theoretical correctness results. Then I will focus on one particular new feature which is the possibility of certifying and then extracting modular programs. This feature is particularly appealing for proving realistic programs. Indeed, Coq now includes a system of modules, signatures and

[1] This was paid by Types money

Table 1: List of visits between sites:

From	To	Who
Bergen	Chalmers	Bezem
Durham	Chalmers	Callahan
Inria-Sophia	Chalmers	Thery
LMU - Munich	Chalmers	Abel
LMU - Munich	Helsinki	Schwichtenberg
Helsinki	LMU - Munich	Negri
Helsinki	LMU - Munich	von Plato
Swansea	LMU - Munich	Setzer
Tolouse	LMU - Munich	Soloviev
Holloway	Nottingham	Luo
Manchester	Holloway	Aczel
Tolouse	Holloway	Soloviev
Manchester	Holloway	Adams
Nottingham	Holloway	McBride
Edinburgh	Holloway	Pollack
Warsaw	Inria-Futurs	Walukiewicz-Chrzaszcz
Warsaw	Inria-Futurs	Chrzaszcz
Paris	Inria-Futurs	Miquel
Edinburgh	Inria-Futurs	Dixon
Bologna	Inria-Futurs	Sacerdotti
Inria-Sophia	Inria-Futurs	Despeyroux
Inria-Sophia	Nijmegen	Mahboubi
Inria-Sophia	Paris 6	Liquori
Tallinn	Minho	Uustalu
LMU - Munich	Nijmegen	Letouzey
Inria-Sophia	Nijmegen	Mahboubi
Birmingham	Nijmegen	Jung
Paris 7	Padova	Baillot
Birmingham	Padova	Ritter
Warsaw	Paris Sud	Walukiewiecz
Warsaw	Paris Sud	Chrząszcz
Warsaw	Paris Sud	Czarnik
Torino	Swansea	Berardi
Edinburgh	Swansea	Aspinall
Torino	Swansea	Dezani
Torino	Swansea	Berardi
LMU - Munich	Swansea	Pattinson
Edinburgh	Swansea	Hancock
LMU - Munich	Tallinn	Shkaravska
Bergen	Tallinn	Bezem
Inria-Sophia	Torino	He
Tolouse	Torino	Soloviev
Torino	Novi Sad	Dezani-Ciancaglini
Padova	Paris	Faggian
Padova	Birmingham	Maietti
Swansea	Nottingham	Setzer
Tallinn	Nottingham	Uustalu
Swansea	Nottingham	Michelbrink
Udine	Edinburgh	Miculan
Udine	Edinburgh	Honsell
Torino	Warsaw	Bono

functors quite similar to the one of Ocaml. The new extraction allows then to link these two systems. I will describe in particular the certification with J.-C. Filliâtre of a finite set library coming from Ocaml standard library.

- Tarmo Uustalo gave a talk titled "A compositional natural semantics and Hoare logic for low-level languages" (joint work with Ando Saabas) in Nottingham 10 June 2005. [1]
- Achim Jung visited Nijmegen on Sep 28, 2004 and gave a talk " Domain environments for real numbers". [1]

  A domain environment for a topological space X is a (usually continuous) dcpo D together with a homomorphism from X to the space of maximal elements of D endowed with the relative Scott-topology. Through the work of Lawson, Edalat, Martin and others, quite a bit is now known about the kind of spaces which can be presented in this way. Another motivation for studying domain environments, however, is to provide a setting in which the elements of the space in question can be used in actual computation. The prime examples are Edalat's approach to computable measure theory and exact real number computation.
- Sara Negri and Jan von Plato from Helsinki visited Munich. Sara Negri gave a lecture course on proof analysis. Jan von Plato gave two seminars on proof-theoretical methods in geometry and arithmetic.
- Pierre Letouzey visited LMU and talked about Coq and Program extraction from proofs with Exercises (Winter 2004/2005, Summer 2005)
- Christian Urban visited LMU and talked about Nominal Logic (summer 05)
- Stefano Berardi (Turin) has visited Swansea and given on Wednesday September 15, 2004, 14:00, a talk on "Programming With Non-Recursive Maps"
- David Aspinall (Edinburgh) has visited Swansea and given on Thursday November 11, 2004, 14:00, a talk on "Logics for Certifying Resource Bounds"
- Mariangiola Dezani (Turin) has visited Swansea and given on Thursday November 18, 2004, 14:00, a talk on "Boxed Ambients with Communication Interfaces"
- Dirk Pattinson (LMU Muenchen) has visited Swansea and given on Tuesday February 01, 2005, 14:00, a talk on "Data Types for Differentiable Functions"
- Peter Hancock (Edinburgh) has visited Swansea and given on Thursday April 14, 2005, 14:00, a talk on "Computational meaning of topological notions."
- A. Setzer from Swansea has visited Torino, Italy. He has given a talk at the logic colloquium on "Universes in Type Theory: Mahlo and Π_3-Reflection".

- U. Berger, M. Michelbrink and A. Setzer have visited the Types group at LMU Munich in November 2004 and gave talks at the workshop Constructive Logic and Mathematics. U. Berger's talk was titled A strong normalization theorem based on continuous semantics, and M. Michelbrink's talk was titled Interfaces as games, programs as strategies, A. Setzer's talk was titled The Π_3-Reflecting Universe.

- Daria Walukiewicz-Chrzaszcz and Jacek Chrzaszcz (Warsaw) visited Ecole Polytechnique from June 11 to July 11, 2005. Title of seminar: Consistency and completeness of rewriting in the Calculus of Constructions

- Viviana Bono (Torino) visited Warsaw from Feb 13 to Feb 20, for collaboration with Pawel Urzyczyn on type inference for object-oriented languages. Title of seminar: Mobile mixins and O'KLaim.

- Patryk Czarnik (Warsaw) visited Universite Paris Sud from 18 to 21 April 2005, for collaboration with Christine Paulin group on Krakatoa and Why verification tools. Title of seminar: Static verification of Java programs using Krakatoa tool

2.6 WP 6: The Types web page

2.6.1 D30 The www-site

The web page of the project can be found at `www.cs.chalmers.se/Cs/Research/Logic/Types/`.

It 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.

It has been rightly pointed out that the web page is not so user-friendly and well-designed. This will be improved.

3 Consortium management

Project management and coordination has been conducted without any friction. The steering group and the coordinator has regular exchange of emails and has also met during the Types conference and the summer school. During the Types conference we also had an open business meeting discussing various organizational matters (such as suggestions for small workshops, place and time for the summer school and the next Types meeting).

The research group in Durham has moved to Royal Holloway, with obvious consequences for the list of main sites. The university of Manchester has changed its structure, the consequences for the Types project is currently investigated.

There have been no conflicts within the consortium.

4 Involvement in other EU projects

The sites are also cooperating in other European projects:

- *APPSEM* (Chalmers, Edinburgh, Birmingham, Nottingham, LMU – Munich, Minho, Tallinn) (`http://www.appsem.org`) - a thematic network funded by the IST program of the EU to promote research in application-oriented semantics of programming languages. This work is most related to our efforts in Foundational Research and Correctness of Computer System.

- *Mowgli* (Bologna (coordinator), Nijmegen, Inria – Futurs, Inria – Sophia,): The Mowgli project aims at developing www based tools for presenting (rendering), browsing and querying formalized mathematics. In Mowgli there has been a strong emphasis on mathematics formalized in type theory, esp. Coq. This is strongly related to our research area Formal Mathematics and Mathematics Education.

- *MRG* (Edinburgh): Independently verifiable certificates describing resource behavior (space, time, etc.) of computer programs; uses ISABELLE/HOL, one of the TYPES proof tools. This is related to our research areas Proof Technology and Correctness of Computer Systems.

- *Mobius* (Inria – Sophia (coordinator), Edinburgh, Inria – Futurs, Tallinn): Continues the work of MRG to other areas of trust management via static enforcement mechanisms, for instance proof carrying code. This is related to our research area Correctness of Computer Systems.

- *MATHLOGAPS* (LMU – Munich) - a multi-participant Early Stage Research Training program between universities in Leeds, Manchester, Lyon and Munich to fund young researchers in the area of the mathematical logic and its applications. This is related to our area Foundational Research.

- *CiE* (LMU – Munich) - 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 Industrial cooperation

The group at Inria-Futurs is part of the French Averroes project, involving France-Telecom and Cril Technology. They will very likely be involved in the INRIA-Microsoft laboratory to be launched January 2006.

The Munich–LMU site is participating in the EU FVI OpenFET project, which started in March 2005. The aims of the EmBounded project are to identify, to quantify and to certify resource-bounded code in a domain-specific high-level programming language for real-time embedded systems. The AbsInt GmBH, Saarbruecken is a project partner which has produced tools for worst case execution time analysis applied in modern cars and airplanes like the new Airbus A380.

The Munich–TU site has a collaboration with Siemens in the Verisoft project.

The Paris – Sud site is collaborating with Dassault Aviation in the area of proofs of C programs. They also have a collaboration with the Axalto company (a smart-cards manufacturer) on proofs of Java and C programs, Java-card applets and operating systems. Th. Hubert (Dassault), J. Andronick and N. Rousset (Axalto) are studying for their PhD part-time in the industry and part-time in our laboratory.

There is a collaboration between Orsay, Grenoble and the industrial subsite France Télécom R& D in the AVERROES national project (analysis and verification for the reliability of embedded systems) (`http://www-verimag.imag.fr/AVERROES`).

There is also have a collaboration with César Muñoz at NIA, Hampton, USA on proof of Java programs for avionics.

The Paris – Sud site also participates in the new competitiveness cluster System@tic (`http://www.systematic-paris-region.org`). In this cluster, the main industrial and academic research centers in the Ile-de-France Region are collaborating in the area of complex systems.

The Swansea site, and in particular M Roggenbach and A Gimblett (together with Prof H Schlingloff, Fraunhofer FIRST, Berlin) have applied CSP-CASL in an industrial case study, where main parts of ep2, a new international standard for electronic payment systems, were to be formalized. Parts of this specification were verified using CSP-Prover. Furthermore, M. Roggenbach (together with Dr Y Isobe, AIST, Japan) is in the planning stage for a cooperation with the company Qinetiq (http://www.qinetiq.com/) on another case study for CSP-Prover.

The Nottingham site has a collaboration with Microsoft around dependent typing of Haskell.

The Warsaw group has a cooperation with ComArch, a polish software company.

6 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.

Refereed journal papers

- P. Hancock, A. Setzer: Guarded induction and weakly final coalgebras in dependent type theory (Extended version). 30 pages. T. Altenkirch, M. Hofmann, J. Hughes (Eds.): *Dependently typed programming.* Dagstuhl Seminar Proceedings 04381, Dagstuhl, Germany, 2005. http://drops.dagstuhl.de/opus/volltexte/2005/176.

- M. Dezani-Ciancaglini, S. Ghilezan, S. Likavec: "Behavioral inverse limit lambda models" Theoretical Computer Science 316 (2004) 49-74

- Andreas Abel, Ralph Matthes, and Tarmo Uustalu. Iteration schemes for higher-order and nested datatypes. *Theoretical Computer Science*, 333(1–2):3–66, 2005

- A. Bove and V. Capretta. Modelling general recursion in type theory. *Mathematical Structures in Computer Science*, 15:671–708, February 2005. Cambridge University Press

- Thierry Coquand, Henri Lombardi and Claude Quitté, *Generating non noetherian modules constructively.* Manuscripta mathematica 115, (2004), 513-520.

- Thierry Coquand and Bas Spitters, *A constructive proof of the Peter-Weyl theorem.* Math. Log. Q. 51, No.4, 351-359 (2005).

- Thierry Coquand, Henri Lombardi and Peter Schuster, *A nilregular element property.* Arch. Math. 85, No.1, 49-54 (2005).

- Peter Dybjer and Anton Setzer. Indexed induction-recursion. *Journal of Logic and Algebraic Programming*, 2005. In press

- Ralph Matthes and Tarmo Uustalu. Substitution in non-wellfounded syntax with variable binding. *Theoretical Computer Science*, 327(1–2):155–174, 2004

- Andreas Abel, Ralph Matthes, and Tarmo Uustalu. Iteration and coiteration schemes for higher-order and nested datatypes. *Theoretical Computer Science*, 333(1–2):3–66, 2005

- D. Aspinall, L. Beringer, M. Hofmann, H-W. Loidl, and A. Momigliano. A Program Logic for Resources. *Theoretical Computer Science*, 2005. Special Issue on Global Computing. Submitted July 2005

Refereed conference papers

- D. Dougerty, S. Ghilezan, P. Lescanne, S. Likavec: "Strong normalization of the dual classical sequent calculus" LPAR 2005, LNCS 3835 (2005) 169-183
- A Language for Verification and Manipulation of Web Documents, WWW-04, ENTCS, by Luigi Liquori (Sophia), Furio Honsell and Rekka Redamalla (Udine).
- L. Liquori and S. Ronchi della Rocca (Turin). Towards and Intersection Typed System a' la Church. In Proc. of ITRS, Workshop on Intersection Types and Related Systems, number To appear in Electronic Notes in Theoretical Computer Science, Elsevier Science, 2004.
- Andreas Abel and Ralph Matthes. Fixed points of type constructors and primitive recursion. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic, CSL'04*, volume 3210 of *Springer Lecture Notes in Computer Science*, pages 190–204. Springer Lecture Notes in Computer Science, 2004
- Andreas Abel and Ralph Matthes. Fixed points of type constructors and primitive recursion. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic: 18th International Workshop, CSL 2004, 13th Annual Conference of the EACSL, Karpacz, Poland, September 20-24, 2004. Proceedings*, volume 3210 of *Lecture Notes in Computer Science*, pages 190–204. Springer, 2004
- David Aspinall, Lennart Beringer, Martin Hofmann, Hans-Wolfgang Loidl, and Alberto Momigliano. A resource-aware program logic for grail. In *TPHOL 2004: 17th International Conference on Theorem Proving in Higher Order Logics, Park City, Utah, USA, September 14-17*, 2004

As mentioned above, cooperation between researchers are also done in other ways. As one example, Yves Bertot published 4 papers in 2005, two of these papers had a single author, but they were greatly improved after interaction with other members of the TYPES Community:

The paper "Filters on CoInductive Streams, an Application to Eratosthenes' Sieve", Proceedings of TLCA'05, Springer LNCS 3461, 2005, benefited from interaction with Ana Bove from Chalmers, Milad Niqui from Nijmegen, Thorsten Altenkirch from Nottingham, and Pietro di Gianantonio from Udine at the TYPES small workshop on termination (funded by the previous European TYPES project).

The paper "Calcul de formules affines et de séries entières en arithmétique exacte avec types co-inductifs" publié à JFLA2006 (an extended version in english has been submitted for publication in an international journal) has benefited from interactions with Milad Niqui (Nijmegen) and Per Martin Löf (Stockhom) at the TYPES summer school in Göteborg in 2005.

The third paper has three authors (Benjamin Grégoire, Yves Bertot, Xavier Leroy, "A structured approach to proving compiler optimizations based on dataflow analysis"), all of them from INRIA, it was published in the proceedings of the first TYPES workshop and naturally benefited from the refereeing process by anonymous colleagues, probably within the TYPES funded community.

The fourth paper "Vérification formelle d'extraction de racines entières" did not take any particular benefit from interaction within the TYPES community, except that, of course, it relies on the tools designed in the community, namely the Coq system.

7 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

We first describe the main sites of the project: Chalmers, CNRS – Paris 7, INRIA-Futurs, INRIA-Sophia, Paris – Sud, Munich – LMU, Munich – TU, Nijmegen, Bialystok, Royal Holloway, Edinburgh, Manchester, Torino, Udine, Warsaw, Tallinn.

This is followed by a description of the minor sites: Bergen, Helsinki, Minho, Padova, Savoie, Swansea, Toulouse, Birmingham, Nottingham, Sheffield.

7.1 Chalmers

Correctness of Computer Systems Andreas Abel, Marcin Benke, Ana Bove, John Hughes and Ulf Norell explored the use of Type Theory for verifying Haskell program. The result was presented at the conference Haskell'05, Tallin, September 2005

Foundational Research David Wahlstedt defended his licentiate thesis in October 2004. He presented a normalization proof for Martin-Löf's logical framework extended with size-changed termination.

Andreas Abel and Thierry Coquand developed a correctness proof for deciding conversion in Martin-Löf's logical framework with surjective pairs. The results were presented at the conference TLCA'05, Nara, September 2005.

Arnaud Spivack, a visiting master student from the ENS Cachan, and Thierry Coquand simplified a normalization proof of Ulrich Berger using the notion of intersection types. The results were presented at the TYPES summer school, August 2005

Peter Dybjer, Erik Palmgren and Thierry Coquand have started the writing of a book on type theory for constructive mathematics. A preliminary version of this book was given to the students of the TYPES summer school.

Formal Mathematics and Mathematics Education Ana Bove developed in Agda the correctness proof of the bitonic sort algorithm, based on the 0/1 law. She and Thierry Coquand formalized another new abstract correctness proof of the same algorithm. This will be published in the proceeding of TYPES 2004.

Proof technology Andreas Abel, Ulf Norell and Thierry Coquand explored a new way to connect a logical framework and a FOL prover. The work was summarized in a paper presented at the conference FroCoS'05, Vienna, September 2005.

Marc Bezem and Thierry Coquand explored automatic deduction in coherent logic, producing explicit proof objects for the proof system Coq.

Type theory and Language Technology There were two PhD theses in the borderline between language technology and type theory. The first one was written by Peter Ljunglöf, the title was Expressivity and Complexity of the Grammatical Framework and it was presented in December 2004. The second thesis was by Kristofer Johannisson (Formal and Informal Software Specifications) and it was defended in June 2005.

There was a new version of GF (Grammatical framework, version 2.3) and the GF resource grammar library, version 0.9 was released. See the home-page of GF (`http://www.cs.chalmers.se/ aarne/GF`).

Publications

Refereed journal papers

- Andreas Abel, Ralph Matthes, and Tarmo Uustalu. Iteration schemes for higher-order and nested datatypes. *Theoretical Computer Science*, 333(1–2):3–66, 2005

- A. Bove and V. Capretta. Modelling general recursion in type theory. *Mathematical Structures in Computer Science*, 15:671–708, February 2005. Cambridge University Press

- Thierry Coquand, Henri Lombardi and Claude Quitté, *Generating non noetherian modules constructively.* Manuscripta mathematica 115, (2004), 513-520.

- Thierry Coquand and Bas Spitters, *A constructive proof of the Peter-Weyl theorem.* Math. Log. Q. 51, No.4, 351-359 (2005).

- Thierry Coquand, Henri Lombardi and Peter Schuster, *A nilregular element property.* Arch. Math. 85, No.1, 49-54 (2005).

- Peter Dybjer, Qiao Haiyan, and Makoto Takeyama. Random generators for dependent types. In *Proceedings of the First International Colloquium on Theoretical Aspects of Computing, Guiyang, China*, LNCS 3407, pages 342 – 356, September 2004

- Peter Dybjer, Qiao Haiyan, and Makoto Takeyama. Verifying haskell programs by combining testing, model checking and interactive theorem proving. *Information and Software Technology*, 46(15):1011 – 1025, 2004

- Peter Dybjer and Anton Setzer. Indexed induction-recursion. *Journal of Logic and Algebraic Programming*, 2005. In press

- A. Ranta and R. Cooper. Dialogue Systems as Proof Editors. *Journal of Logic, Language and Information*, 13:225–240, 2004

- A. Ranta. Computational semantics in type theory. *Mathematics and Social Sciences*, 165:31–57, 2004

- A. Ranta. Grammatical Framework: A Type-Theoretical Grammar Formalism. *The Journal of Functional Programming*, 14(2):145–189, 2004

Refereed conference papers

- A. Abel, M. Benke, A. Bove, J. Hughes, and U. Norell. Verifying Haskell programs using constructive type theory. In *Haskell Workshop*, September 2005

- Andreas Abel, Marcin Benke, Ana Bove, John Hughes, and Ulf Norell. Verifying Haskell programs using constructive type theory. In *Haskell'05, Tallinn, Estonia, 30 September, 2005*

- Andreas Abel, Thierry Coquand, and Ulf Norell. Connecting a logical framework to a first-order logic prover. In Bernhard Gramlich, editor, *5th International Workshop on Frontiers of Combining Systems, FroCoS'05, Vienna, Austria, September 19-21, 2005*, Springer Lecture Notes in Computer Science

- Andreas Abel and Ralph Matthes. Fixed points of type constructors and primitive recursion. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic, CSL'04*, volume 3210 of *Springer Lecture Notes in Computer Science*, pages 190–204. Springer Lecture Notes in Computer Science, 2004

- Andreas Abel and Thierry Coquand. Untyped algorithmic equality for martin-löf's logical framework with surjective pairs. In *TLCA'05*, volume 3461 of *Springer Lecture Notes in Computer Science*, pages 23–38. Springer Lecture Notes in Computer Science, 2005

- A. Bove and V. Capretta. Recursive functions with higher order domains. In *Typed Lambda Calculi and Applications TLCA'05*, number 3461 in Lecture Notes in Computer Science, pages 115–130. Springer-Verlag, April 2005

- A. Bove and T. Coquand. Formalising bitonic sort in type theory, August 2005. To appear in the post workshop proceedings of TYPES 2004

- Björn Bringert, Robin Cooper, Peter Ljunglöf, and Aarne Ranta. Multimodal dialogue system grammars. In *Proceedings of DIALOR'05, Ninth Workshop on the Semantics and Pragmatics of Dialogue*, pages 53–60, June 2005

- David A. Burke and Kristofer Johannisson. Translating formal software specifications to natural language—a grammar-based approach. In Philippe Blache and Edward Stabler, editors, *LACL 2005*, number 3492 in LNAI. Springer, 2005

- Thierry Coquand. Completeness theorems and lambda-calculus. In *TLCA*, pages 1–9, 2005

- M. Forsberg and A. Ranta. Functional Morphology. *Proceedings of the Ninth ACM SIGPLAN International Conference of Functional Programming, Snowbird, Utah*, pages 213–223, 2004

- H. Hammarström and A. Ranta. Cardinal Numerals Revisited in GF. In *Workshop on Numerals in the World's Languages. Dept. of Linguistics Max Planck Institute for Evolutionary Anthropology, Leipzig, Germany*, 2004

- Kristofer Johannisson. Disambiguating implicit constructions in OCL, 2004. Online proceedings of OCL and Model Driven Engineering Workshop at UML 2004, `www.cs.kent.ac.uk/projects/ocl/oclmdewsuml04/description.htm`

- J. Khegai and A. Ranta. Building and Using a Russian Resource Grammar in GF. In A. Gelbukh, editor, *Intelligent Text Processing and Computational Linguistics (CICLing-2004), Seoul, Korea, February 2003*, volume 2945 of *LNCS*, pages 38–41. Springer-Verlag, 2004

- Peter Ljunglöf. Grammatical Framework and multiple context-free grammars. In *9th Conference on Formal Grammar*, Nancy, France, August 2004

- A. Ranta. Grammatical Framework Tutorial. In A. Beckmann and N. Preining, editors, *ESSLLI 2003 Course Material I*, volume V of *Collegium Logicum*, pages 1–86. Kurt Gödel Society, 2004

Talks

- Björn Bringert, Robin Cooper, Peter Ljunglöf and Aarne Ranta, *Building Multimodal Dialogue Systems in GF.* Presented at TYPES 2004 conference, December 15-18, 2004, Jouy-en-Josas, FRANCE.

- Peter Dybjer, *Normalization by Evaluation for Untyped Combinatory Logic* `http://www.cs.chalmers.se/~peterd/slides/Uppsala2005.ps` Talk given at the Stockholm - Uppsala Logic seminar, February 2005.

- Peter Dybjer, *Combining Verification Methods in Software Development: an Overview of a Research Project at Chalmers* `http://www.cs.chalmers.se/~peterd/slides/Senri05.pdf`, Workshop on Automatic and Interactive Verification, Senri, Osaka, Japan, April 2005

- Peter Dybjer, *Constructive Type Theory and Interactive Theorem Proving.* Talk given at the 22nd Annual Meeting of the Japanese Society for Software Science and Technology, Sendai, Japan, September 2005.

- Peter Dybjer, *Typed and Untyped Normalization by Evaluation.* Talk given at Tohoku University, Sendai, Japan, and at the Workshop on New Approaches to Software Construction, Tokyo, Japan, September 2005.

- Peter Dybjer, *Constructive Type Theory and the Proof Assistant Agda.* Talk given at the AIST-JAIST Workshop, Kanazawa, Japan, September 2005.

- Fredrik Lindblad, *An Experiment in Automated Theorem Proving in Type Theory.* Presented at TPHOLs conference, Salt Lake City, Utah, USA, September 2005.

- Bengt Nordström, *Proof Documents: Presentation and Representation*, National Institute of Advanced Industrial Science and Technology, Senri, Japan, April 2005.

- Aarne Ranta, Démonat meeting, Paris, November 2004.

- Aarne Ranta, Stockholm-Uppsala Logic Seminar, February 2005.

- Aarne Ranta, TALK mini conference, Nancy, 2005.

- Aarne Ranta, WebALT meeting, Helsinki, June 2005.

- David Wahlstedt, *Type Theory with First-Order Data Types and Size-Change Termination* Presented at TYPES 2004 conference, December 15-18, 2004, Jouy-en-Josas, FRANCE.

Dissertations

- Kristofer Johannisson. *Formal and Informal Software Specifications.* PhD thesis, Chalmers University of Technology, Göteborg University, SE-412 96 Göteborg, Sweden, 2005

- Peter Ljunglöf. *Expressivity and Complexity of the Grammatical Framework.* PhD thesis, Göteborg University and Chalmers University of Technology, Gothenburg, Sweden, November 2004

- David Wahlstedt. Type theory with first-order data types and size-change termination. Technical report, 2004. Licentiate thesis 2004, No. 36L

- Björn Bringert. Embedded grammars. Master's thesis, Chalmers University of Technology, Gothenburg, Sweden, February 2005

7.2 CNRS – Paris 7

Foundational Research Alexandre Miquel investigated connections between set theory and pure type systems through the sets-as-pointed-graphs representation. He showed that a particular PTS is a conservative extension of (a variant of) Zermelo's set theory.

Michel Parigot gave a simple and generic proof of the characterization of constructive existence in classical logic due to Matthias Baaz. This proof allows in particular to generalize the result to other logics enjoying cut-elimination.

On the topic of linear logic and its application to verification of complexity in lambda-calculus by typing, Patrick Baillot has proposed in a joint work with K. Terui a new algorithm for type inference in Elementary linear logic .

In joint work with Claudia Faggian, Pierre-Louis Curien has established a connection between game semantics and proof nets based on a new notion of graph strategies over a universal arena.

Roberto Di Cosmo pursued his work on type isomorphisms, in contact with Sergei Soloviev (Toulouse) and Mariangiola Dezani-Ciancaglini (Torino). With his PhD student Thomas Dufour, he published an article in LPAR'05 on an equational theory of natural numbers which is strongly related to type isomorphisms for modern functional languages. Joachim de la Taillade pursued Olivier Laurent's work on type isomorphisms for Parigot's mu calculus, giving a finite and complete axiomatisation for type isomorphisms with second order types via a second order game semantics model.

Delia Kesner and Stephane Lengrand constructed a simple term language with explicit operators for erasure, duplication and substitution enjoying a sound and complete correspondence with the intuitionistic fragment of Linear Logic's Proof Nets. This formalism is the first term calculus with explicit substitutions having full composition and preserving strong normalization.

Chantal Berline obtained qualitative and quantitative results on the lattice of lambda-theories (the equational theories of pure lambda-calculus)

Publications

Refereed journal papers

- E. Bonelli, D. Kesner and A. RŠos. De Bruijn Indices for Metaterms. Journal of Logic and Computation (to appear)
- C. Berline and A. Salibra. Easiness in graph models, Theoretical Computer Science (to appear).

Refereed conference papers

- P. Baillot and K. Terui. A feasible algorithm for typing in Elementary Affine Logic, Proc. TLCA'05, Springer LNCS, pp 55-70.
- R. Di Cosmo and T. Dufour. The equational theory of $< N, 0, 1, +, \cdot, \uparrow>$ is decidable, but not finitely axiomatisable. Proc. LPAR'05, Springer LNCS, pp 240-256.
- P.-L. Curien and C. Faggian. L-nets, strategies and proof-nets, Proc. CSL 05, Springer LNCS, 2005.

- C. Faggian and F. Maurel, Ludics Nets, a game model of concurrent interaction, LICS 05, IEEE Computer Society, 2005
- D. Kesner and S. Lengrand. Extending the Explicit Substitution Paradigm. Proc. RTA 05, Springer LNCS 3467, pages 407-422, 2005.
- A. Miquel. Lambda-Z: Zermelo's Set Theory as a PTS with 4 Sorts. Proc. TYPES'04 (to appear).
- M. Parigot. On constructive existence. Proc. TYPES'04 (to appear).

7.3 INRIA-Futurs

Formal Mathematics and Mathematics Education The Coq proof system allowed the first formal proof of the four color theorem. This proof was completed by Georges Gonthier at Microsoft Research. He had started this work with Benjamin Werner at INRIA.

Benjamin Grégoire and Benjamin Werner presented a new kind of formal primality proofs, using the new compilation technology of Coq. This allows proving primality of numbers of the 18th Mersenne prime (almost 1000 digits).

Dale Miller and Alwen Tiu have pursued their study of the LINC logic (equipped with a ∇-quantifier) designed to describe proof search in a language with bindings . They have used this framework to specify the π-Calculus .

Dale Miller and Elaine Pimentel have continued their work on a linear framework for specifying sequent calculus .

Dale Miller and Alexis Saurin have studied a game semantics for proof search.

Proof Technology The evolution V8.0.pl2 of the Coq proof assistant was released. It includes an on-the-fly compiler developed by Benjamin Grégoire during his PhD and allows fast execution of computational proofs. This feature is currently unique to Coq and essential in the two formalizations mentionned above.

Julien Narboux has developed a decision procedure for geometry in Coq.

Foundational Research A lot of new results on various aspects of the computational nature of proofs have been obtained this year, by Hugo Herbelin, Dan Hernest Mircea and François-Régis Sinot.

Gilles Dowek showed that PTS's can be viewed as simple dependent types with rewrite rules; with Benjamin Werner he has given a presentation of arithmetic by rewrite rules only.

Media presentations

Benjamin Werner participated to the formal proof of the four-color theorem finished by Georges Gonthier by the end of 2004. Therefore, he and Gilles Dowek have been cited in various scientific magazines for wider audience. Coq was cited in even more cases in this respect (citations include Science, Süddeutsche Zeitung, La Recherche, Science et Vie, AFP and others).

Publications

Refereed journal papers

- Dale Miller and Alwen Tiu. A proof theory for generic judgments. *ACM Transactions on Computational Logic*, 6(4), October 2005

- G. Dowek. La théorie des types et les systèmes, informatiques de traitement des démonstrations mathématiques. *Mathématiques et Sciences Humaines*, 165:13–29, 2004

- Mircea-Dan Hernest and Ulrich Kohlenbach. A complexity analysis of functional interpretations. *Theoretical Computer Science*, 338, Issues 1-3:200–246, 2005

- Maribel Fernández, Ian Mackie, and François-Régis Sinot. Closed reduction: explicit substitutions without alpha-conversion. *Mathematical Structures in Computer Science*, 15(2):343–381, 2005

- Maribel Fernández, Ian Mackie, and François-Régis Sinot. Lambda-calculus with director strings. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 15(6):393–437, April 2005

- François-Régis Sinot. Director strings revisited: A generic approach to the efficient representation of free variables in higher-order rewriting. *Journal of Logic and Computation*, 15(2):201–218, 2005

- François-Régis Sinot and Ian Mackie. Macros for interaction nets: A conservative extension of interaction nets. *Electronic Notes in Theoretical Computer Science*, 127(5), 2005

- François-Régis Sinot. Token-passing nets: Call-by-need for free. *Electronic Notes in Theoretical Computer Science*, 2005. to appear

Refereed conference papers

- Dale Miller and Elaine Pimentel. Linear logic as a framework for specifying sequent calculus. In Jan van Eijck, Vincent van Oostrom, and Albert Visser, editors, *Logic Colloquium '99: Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic*, Lecture Notes in Logic, pages 111–135. A K Peters Ltd, 2004

- Bruno Barras and Benjamin Grégoire. On the role of type decorations in the calculus of inductive constructions. In *CSL'05*. LNCS, Springer-Verlag, August 22-25,2005, Oxford, UK

- G. Dowek. What do we know when we know that a theory is consistent. In R. Nieuwenhuis, editor, *Automated Deduction*, pages 1–6. Lecture Notes in Artificial Intelligence, 3632, Springer-Verlag, 2005

- G. Dowek and B. Werner. Arithmetic as a theory modulo. In J. Giesel, editor, *Term rewriting and applications*, pages 423–437. Lecture Notes in Computer Science 3467, Springer-Verlag, 2005

- P. Arrighi and G. Dowek. A computational definition of the notion of vectorial space. In N. Martıŋ-Oliet, editor, *Proceedings of the Fifth International Workshop on Rewriting Logic and Its Applications (WRLA 2004)*, pages 249–261. Electronic Notes in Theoretical Computer Science 117, 2005

- C. Muñoz, G. Dowek, and V. Carre no. Modeling and verification of an air traffic concept of operations. In *International Symposium on software testing and analysis*, 2004

- P. Arrighi and G. Dowek. Linear-algebraic lambda-calculus. In P. Selinger, editor, *International workshop on quantum programming languages.* Turku Centre for Computer Science General Publication, 33

- Hugo Herbelin. On the degeneracy of sigma-types in presence of computational classical logic. In Pawel Urzyczyn, editor, *Seventh International Conference, TLCA '05, Nara, Japan. April 2005, Proceedings*, volume 3461 of *Lecture Notes in Computer Science*, pages 209–220. Springer, 2005

- Zena M. Ariola, Hugo Herbelin, and Amr Sabry. A type-theoretic foundation of continuations and prompts. In *Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming (ICFP '04), Snowbird, Utah, September 19-21, 2004*, pages 40–53. ACM, 2004

- Jean Goubault-Larrecq and Jean-Pierre Jouannaud. Finite semantic trees suffice for ordered resolution and paramodulation. In *Workshop on Programming Logics in memory of Harld Ganzinger.* LNCS, Spiringer-Verlag, june 2005

- Dale Miller. Bindings, mobility of bindings, and the ∇-quantifier. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *18th International Workshop CSL 2004*, volume 3210 of *LNCS*, page 24, 2004

- Alwen Tiu and Dale Miller. A proof search specification of the π-calculus. In *3rd Workshop on the Foundations of Global Ubiquitous Computing*, September 2004

- Dale Miller and Alexis Saurin. A game semantics for proof search: Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS)*, 2005

- Elaine Pimentel and Dale Miller. On the specification of sequent systems. In *LPAR 2005: 12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, 2005

- Axelle Ziegler, Dale Miller, and Catuscia Palamidessi. A congruence format for name-passing calculi. In *Proceedings of SOS 2005: Structural Operational Semantics*, July 2005

- Julien Narboux. A decision procedure for geometry in coq. In Slind Konrad, Bunker Annett, and Gopalakrishnan Ganesh, editors, *Proceedings of TPHOLs'2004*, volume 3223 of *Lecture Notes in Computer Science.* Springer-Verlag, 2004

- Julien Narboux. Toward the use of a proof assistant to teach mathematics. In *Proceedings of ICTMT7*, 2005

- François-Régis Sinot. Call-by-name and call-by-value as token-passing interaction nets. In *Proceedings of Typed Lambda Calculi and Applications (TLCA'05)*, volume 3461 of *Lecture Notes in Computer Science*, pages 386–400, 2005

- Maribel Fernández, Ian Mackie, and François-Régis Sinot. Interaction nets vs. the rho-calculus: Introducing bigraphical nets. *Electronic Notes in Theoretical Computer Science*, 2005. to appear

Talks

- Dale Miller. Bindings, mobility of bindings, and the ∇-quantifier. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *18th International Workshop CSL 2004*, volume 3210 of *LNCS*, page 24, 2004
- J.-P. Jouannaud. Twenty years later. In *RTA 2004*. LNCS, Springer-Verlag, 2004
- J.-P. Jouannaud. Formal mathematics: Application to software safety and internet security. In *Invited presentation, 9th Articifial Intelligence Conference, Taipei*, 2004
- J.-P. Jouannaud. Theorem proving languages for verification. In *Invited presentation,2nd International Symposium on Automated Technology for Verification and Analysis, Taipei*, 2004

7.4 INRIA-Sophia

Correctness of Computer Systems. Benjamin Grégoire, Bernard Serpette, and Laurence Rideau have contributed to the proof of correctness of the back-end of a lightly optimized compiler from Cminor to the PowerPC code, which has been mainly done by Xavier Leroy from Inria-Rocquencourt. Two papers describing the methods used in this work have been published .

Formal Mathematics and Mathematics Education. Sabrina Tarento and Gilles Barthe have extended their formal analysis (using Coq) of crypto-systems to the case of an interactive adversary (that adheres to the Generic Model and to the Random Oracle Model), and to the case of parallel attacks.

Laurent Théry has developed a set of tactics to perform manipulation modulo associativity and commutativity of inequalities inside Coq (available by ftp from: //ftp-sop.inria.fr/lemme/Laurent.Thery/PolTac/index.html).

Proof Technology. Julien Charles and Benjamin Grégoire have developed a translation plug-in from Jack to Coq, integrated in Eclipse. Jack is a tool to perform statically proofs of properties of Java programs annotated with JML. This plug-in allows a Jack user to solve proof obligations both automatically and interactively. A set of tactics has been developed to simplify the interactive proofs.

Foundational Research. Gilles Barthe, Benjamin Grégoire and Fernando Pastawski have designed a inference algorithm for typed-based termination in a polymorphic setting (system F) . This type-based system and inference algorithm can be extended to the family of types theories.

In collaboration with Benjamin Wack, Luigi Liquori has designed an inference algorithm for a polymorphic version of the Rewriting Calculus inspired by the classical Damas-Milner style algorithm for ML.

Publications

Book

- Yves Bertot, Pierre Castéran. Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions, Springer Verlag, EATCS Texts in Theoretical Computer Science, ISBN 3-540-20854-2 (http://www.labri.fr/perso/casteran/CoqArt/)

Refereed conference papers

- G. Barthe. Type isomorphisms and back-and-forth coercions in type theory. *Mathematical Structures in Computer Science*, 2005. To appear

- G. Barthe and L. Prensa-Nieto. Formally verifying information flow type systems for concurrent and thread systems. pages 13–22

- Yves Bertot, Benjamin Grégoire, and Xavier Leroy. A structured approach to proving compiler optimizations based on data-flow analysis. TYPES'04.

- Benjamin Gregoire and Assia Mahboubi. Proving equalities in a commutative ring done right in coq. In *Proceedings of TPHOLs'05*, Oxford, UK, August 2005

- Bruno Barras and Benjamin Gregoire. On the role of type decorations in the calculus of inductive constructions. In *Proceedings of CSL'05*, Oxford, UK, August 2005

- G. Barthe, B. Grégoire, and F. Pastawski. To practical inference for typed-based termination in a polymorphic setting. In P. Urzyczyn, editor, Proceedings of TLCA'05, volume 3641 of Lecture Notes in Computer Science, pages 71-85, Nara, Japan, April 2005. Springer-Verlag.

- Benjamin Gregoire, Yves Bertot, and Xavier Leroy. A structured approach to proving compiler optimizations based on dataflow analysis. 2004. to appear in the post-proceeedings of TYPES'04

- Yves Bertot Filters on CoInductive Streams, an Application to Eratosthenes' Sieve , Proceedings of TLCA'05, Springer LNCS 3461, 2005. A preliminary version is available as INRIA research report RR-5343. The corresponding source code is also available.

- L. Liquori and B.P. Serpette. iRho: an Imperative Rewriting Calculus. In Proc. of PPDP, ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming, pages 167-178. The ACM Press, 2004. www-sop.inria.fr/mirho/Luigi.Liquori/PAPERS/ppdp-04.ps.gz.

- Luigi Liquori. iRho: the Software (system description). Proc. of DCM-05. To appear in Electronic Notes in Theoretical Computer Science. Elsevier Science, 2005.

- S. Tarento. Machine-checked security proofs of cryptographic signature schemes. In D. Gollmann S. De Capitani di Vimercati, P.F. Syverson, editor, *Proceedings of ESORICS'05*, volume 3679 of *Springer Lecture Notes in Computer Science*, pages 140–158. Springer Lecture Notes in Computer Science, 2005

- G. Barthe S. Tarento. A machine-checked formalization of the random oracle model. In *Proceedings of TYPES'04*, volume 3xxx of *Springer Lecture Notes in Computer Science*. Springer Lecture Notes in Computer Science, 2005

Talks

- Julien Charles gave a talk at Geccoo (2005-03-14), where he presented the new Coq plug-in for Jack.

7.5 Paris – Sud

Correctness of Computer Systems

Proving C or Java programs Our main activity is related to program verification. We mainly focus on the verification of behavioral specifications for programming languages such as C, Java and ML. We develop a tool ”Why” which is a verification conditions generator: from an annotated program written in a small imperative language with Hoare logic-like specification, it generates conditions expressing the correctness and termination of the program. These 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).

On top of this tool, we built a system called Krakatoa which verifies Java source code annotated with the Java Modeling Language (JML). The main challenge was the design of a suitable model for the Java memory heap in order to tackle programs with possible aliases .

J.-C. Filliâtre and C. Marché designed a similar tool called Caduceus for dealing with C programs. This tool was used by Th. Hubert and C. Marché for proving a subtle algorithm due to Schorr & Waite for graphs traversal. J. Andronick experimented on using this tool for formal verification of security properties of smart card embedded source code.

Timed automata Orsay and France Telecom R& D collaborated on the definition of a model of timed automata in Coq. It is integrated in the CALIFE platform, a general tool for specification and automatic or interactive verification of protocols. We are currently studying the quantitative analysis of behavior of protocols built on random choices.

Dependent types For his master work supervised by C. Paulin, M. Sozeau designed a language with a subset type (in the spirit of the PVS language) which is convenient for programming with (a restricted class of) dependent types. He proposed a translation of a term in this language to a Coq term containing existential variables corresponding to type-checking conditions.

Case studies We developed several case studies in Coq related to correctness of computer systems.
J.-F. Monin from Grenoble subsite proved that the functional sprintf function of Danvy and the usual version of sprintf (with a dependent typing) are intensionally equal. Th. Hubert developed libraries for certifying termination proofs using dependent pairs criteria in Coq.

Formal Mathematics and Mathematics Education J. Duprat together with L. Vuillon from the Chambery subsite is working on formalizing discrete geometry by inductive objects.

Proof Technology For his master work supervised by J-C. Filliâtre, N. Ayache designed an interactive tactic for calling first-order automatic provers from the Coq proof assistant. The main difficulty was to derive an apropriate first-order theory from an higher-order environment.

Foundational Research

Automatic deduction Integrating automatic deduction into type theory is a long term research. P. Corbineau made a significant contribution extending results in first-order intuitionistic logic with equality to the case of predicate defined by constructors. S. Conchon is studying decision procedures adapted to automatic resolution of proof obligations generated by checking correctness of programs.

Extensionality Mathematical proofs make an implicit use of extensionality which identify two objects which are provably equal. N. Oury studied this rule and proposed a translation of a derivation in an extensional system into an intensional proof in a system like Coq.

Publications

Refereed journal papers

- Sylvain Conchon and Sava Krstić. Strategies for combining decision procedures. *Theoretical Computer Science*, 2004. Special Issue of TCS dedicated to a refereed selection of papers presented at TACAS'03.
- Evelyne Contejean, Claude Marché, Ana Paula Tomás, and Xavier Urbain. Mechanically proving termination using polynomial interpretations. *Journal of Automated Reasoning*, 2005.
- Claude Marché, Christine Paulin-Mohring, and Xavier Urbain. The KRAKATOA tool for certification of JAVA/JAVACARD programs annotated in JML. *Journal of Logic and Algebraic Programming*, 58(1–2):89–106, 2004. http://krakatoa.lri.fr.
- Claude Marché and Xavier Urbain. Modular and incremental proofs of AC-termination. *Journal of Symbolic Computation*, 38:873–897, 2004.
- Sava Krstić and Sylvain Conchon. Canonization for disjoint unions of theories. *Information and Computation*, 2004. Special Issue of Information and Computation dedicated to a refereed selection of papers presented at CADE-19.

Refereed conference papers

- June Andronick, Boutheina Chetali, and Christine Paulin-Mohring. Formal verification of security properties of smart card embedded source code. In John Fitzgerald, Ian J. Hayes, and Andrzej Tarlecki, editors, *International Symposium of Formal Methods Europe (FM'05)*, volume 3582 of *Lecture Notes in Computer Science*, Newcastle,UK, July 2005. Springer-Verlag.

- Evelyne Contejean and Pierre Corbineau. Reflecting proofs in first-order logic with equality. In *20th International Conference on Automated Deduction (CADE-20)*, Lecture Notes in Computer Science, Tallinn, Estonia, July 2005. Springer-Verlag.

- Jean-Christophe Filliâtre and Claude Marché. Multi-prover verification of C programs. In Jim Davies, Wolfram Schulte, and Mike Barnett, editors, *Sixth International Conference on Formal Engineering Methods*, volume 3308 of *Lecture Notes in Computer Science*, pages 15–29, Seattle, WA, USA, November 2004. Springer-Verlag.

- Thierry Hubert and Claude Marché. A case study of C source code verification: the Schorr-Waite algorithm. In *3rd IEEE International Conference on Software Engineering and Formal Methods (SEFM'05)*, Koblenz, Germany, September 2005.

- Bart Jacobs, Claude Marché, and Nicole Rauch. Formal verification of a commercial smart card applet with multiple tools. In *Algebraic Methodology and Software Technology*, volume 3116 of *Lecture Notes in Computer Science*, Stirling, UK, July 2004. Springer-Verlag.

- Claude Marché and Christine Paulin-Mohring. Reasoning about Java programs with aliasing and frame conditions. In Hurd and Melham .

- Jean-François Monin. Proof pearl: From concrete to functional unparsing. In K. Slind, A. Bunker, and G. Gopalakrishnan, editors, *International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2004)*, volume 3223 of *Lecture Notes in Computer Science*, pages 217–224. Springer-Verlag, Park City, Utah, USA, September 2004.

- Nicolas Oury. Extensionality in the Calculus of Constructions. In Hurd and Melham .

Dissertations

- Nicolas Ayache. Coopération d'outils de preuve interactifs et automatiques. Master's thesis, Université Paris 7, 2005.

- Pierre Corbineau. *Démonstration Automatique en Théorie des Types*. Thèse de doctorat, Université Paris-Sud, September 2005.

- Thierry Hubert. Certification des preuves de terminaison en Coq. Rapport de DEA, Université Paris 7, September 2004. In French.

- Matthieu Sozeau. Coercion par prédicats en Coq. Master's thesis, Université Paris 7, 2005.

7.6 Munich – LMU

Correctness of Computer Systems M. Hofmann, H.-W. Loidl and others continued their research on Mobile Resource Guarantees using resource aware type systems for functional languages like Grail, to be able to create formal proofs certifying bounds for resource usage.

Formal Mathematics and Mathematics Education C. Urban worked on using nominal logic in the theorem prover Isabelle to allow natural reasoning over languages with binders like lambda calculus . He formalised major parts of Barendrecht's text book proves in a nearly one to one way.

Proof Technology H. Schwichtenberg, S. Berghofer, P. Letouzey and U. Berger investigated the computational content of Tait's strong normalization proof for typed lambda calculus and extracted the normalization by evaluation algorithm using the theorem provers Minlog and Coq .

Foundational Research R. Matthes continued the research on nested data-types and started case studies in the theorem prover Coq which display a trade-off between truly nested data-types and dependent heterogeneous data-types that are directly supported by the Coq system.

Publications

Refereed journal papers

- Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, To appear, 2005

- Ralph Matthes and Tarmo Uustalu. Substitution in non-wellfounded syntax with variable binding. *Theoretical Computer Science*, 327(1–2):155–174, 2004

- Andreas Abel, Ralph Matthes, and Tarmo Uustalu. Iteration and coiteration schemes for higher-order and nested datatypes. *Theoretical Computer Science*, 333(1–2):3–66, 2005

- Ralph Matthes. Non-strictly positive fixed-points for classical natural deduction. *Annals of Pure and Applied Logic*, 133:205–230, 2005

- Helmut Schwichtenberg. Minlog. To appear in: The Seventeen Provers of the World, Complied by Freek Wiedijk, Springer LNAI, 2005

- Helmut Schwichtenberg. An arithmetic for polynomial-time computation. To appear: TCS, 2005

- D. Aspinall, L. Beringer, M. Hofmann, H-W. Loidl, and A. Momigliano. A Program Logic for Resources. *Theoretical Computer Science*, 2005. Special Issue on Global Computing. Submitted July 2005

- Klaus Aehlig and Felix Joachimski. Continuous normalization for the lambda-calculus and Gödel's *T*. *Annals of Pure and Applied Logic*, 133(1–3):39–71, May 2005

- Klaus Aehlig and Jan Johannsen. An elementary fragment of second-order lambda calculus. *ACM Transactions on Computational Logic*, 6(2):468–480, April 2005

- Klaus Aehlig. Induction and inductive definitions in fragments of second order arithmetic. *The journal of Symbolic Logic*, 2005? to appear

Refereed conference papers

- Andreas Abel and Ralph Matthes. Fixed points of type constructors and primitive recursion. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic: 18th International Workshop, CSL 2004, 13th Annual Conference of the EACSL, Karpacz, Poland, September 20-24, 2004. Proceedings*, volume 3210 of *Lecture Notes in Computer Science*, pages 190–204. Springer, 2004

- David Aspinall, Lennart Beringer, Martin Hofmann, Hans-Wolfgang Loidl, and Alberto Momigliano. A resource-aware program logic for grail. In *TPHOL 2004: 17th International Conference on Theorem Proving in Higher Order Logics, Park City, Utah, USA, September 14-17*, 2004

- J. Cheney and C. Urban. Alpha-Prolog: A Logic Programming Language with Names, Binding, and α-Equivalence. In *Proc. of the 20th International Conference on Logic Programming (ICLP)*, volume 3132 of *LNCS*, pages 269–283, 2004

- C. Urban and J. Cheney. Avoiding Equivariance in Alpha-Prolog. In *Proc. of the 7th International Conference on Typed Lambda Calculi and Applications*, volume 3461 of *LNCS*, pages 401–416, 2005

- C. Urban and C. Tasson. Nominal Techniques in Isabelle/HOL. In *Proc. of the 20th International Conference on Automated Deduction (CADE)*, volume 3632 of *LNCS*, pages 38–53, 2005

- C. Urban and M. Norrish. A Formal Treatment of the Barendregt Variable Convention in Rule Inductions. In *Proc. of the 3rd International ACM Workshop on Mechanized Reasoning about Languages with Variable Binding and Names*, 2005. (Accepted for publication)

- Klaus Aehlig, Jolie G de Miranda, and C H Luke Ong. The monadic second order theory of trees given by arbitrary level-two recursion schemes is decidable. In *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications (TLCA '05)*, pages 39–54, 2005

- Pawel̃ Urzyczyn, editor. *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications (TLCA '05)*, volume 3461 of *Lecture Notes in Computer Science*. Springer-Verlag, April 2005

- Klaus Aehlig, Jolie G de Miranda, and C H Luke Ong. Safety is not a restriction at level two for string languages. In *Foundations of Software Science and Computation Structures (FOSSACS '05)*, pages 490–504, 2005

- Vladimiro Sassone, editor. *Foundations of Software Science and Computation Structures (FOSSACS '05)*, volume 3441 of *Lecture Notes in Computer Science*. Springer Verlag, April 2005

Talks

- Helmut Schwichtenberg. Minimal logic for computable functionals. To appear: Proc. ASL Summer meeting in Athens, 2005

- Helmut Schwichtenberg. Program extraction from constructive proofs. Mathematics Colloquium, Uppsala University, 9 2005

- Helmut Schwichtenberg. Proof search in minimal logic. In B. Buchberger and J.A. Campbell, editors, *Artificial Intelligence and Symbolic Computation, 7th International Conference, AISC 2004, Linz, Austria, September 2004, Proceedings*, volume 3249 of *LNAI*, pages 15–25. Springer Verlag, 2004

- Helmut Schwichtenberg. Constructive analysis with witnesses. To appear: Proceedings NATO Advanced Study Institute, Marktoberdorf, 2003, 2005

- Ralph Matthes. Higher-order inductive types - 4 years later. Munich (Colloquium of the GKLI), 2 2005

- Ralph Matthes. Monadic stabilization for operationalized second-order classical. 3 2005

- Ralph Matthes. Types inductifs au-delя̆ de la stricte positivite (english translation: inductive types beyond strict positivity). Toulouse at IRIT (Institut de Recherche en Informatique de Toulouse), 5 2005

- Ralph Matthes. Towards iteration for truly nested datatypes. Dagstuhl (Seminar on Dependently Typed Programming, `www.dagstuhl.de/04381/`), 9 2004

7.7 Munich – TU

Correctness of Computer Systems

- Norbert Schirmer has built a verification environment for C0 programs. Veronika Ortner has applied this environment to prove the correctness of a BDD normalization algorithm, which she presented at the Types 2004 workshop in Paris.
- Farhad Mehta and Tobias Nipkow published a paper which shows how pointer programs can be modeled and verified in HOL.
- Tobias Nipkow, together with Gregor Snelting, Frank Tip and Daniel Wasserrab wrote a report where they present a formal semantics and type soundness proof for a C++-like programming language featuring multiple inheritance.

Formal Mathematics and Mathematics Education

- Gertrud Bauer has submitted her PhD thesis where she formalizes part of Thomas Hales' proof of the Kepler conjecture.
- Steven Obua has developed a method for proving bounds for the linear programs arising in the proof of the Kepler conjecture using Isabelle/HOL. This work was presented at the Types 2004 workshop, as well as at TPHOLs 2005.

Proof Technology

- Clemens Ballarin has extended Isabelle's *Locale* package for structured specifications to support *interpretations*, a mechanism to instantiate abstract specifications to concrete ones.
- Tobias Nipkow and Larry Paulson studied function definitions over finite sets.

Foundational Research

- Together with Christian Urban from the LMU München site, Stefan Berghofer is working on a definitional package for so-called *nominal data-types*, which can be used in formalizations of languages involving binders. Jesper Bengtson from Joachim Parrow's group in Uppsala, who is currently visiting TU München, is already applying a preliminary version of the package to a formalization of the Pi-calculus.
- Stefan Berghofer has also formalized parts of the PoplMark challenge in Isabelle/HOL using de Bruijn indices. Once the implementation of the nominal package is finished, this case study will be used to compare the nominal and the de Bruijn encoding techniques.
- Stefan Berghofer has formalized a constructive proof of weak normalization for the simply-typed λ-calculus due to Ralph Matthes and Felix Joachimski in Isabelle/HOL, and extracted a normalization algorithm

from it. He presented this work at the Types 2004 workshop in Paris. He has also contributed to an invited journal article by Pierre Letouzey and Helmut Schwichtenberg from the LMU München site, as well as Ulrich Berger from the Swansea site, which is about program extraction from Tait-style normalization proofs using the proof assistants Minlog, Coq, and Isabelle. The proofs presented in this article yield the so-called *normalization by evaluation algorithm* invented by Berger and Schwichtenberg.

Publications

Refereed journal papers

- Farhad Mehta and Tobias Nipkow. Proving pointer programs in higher-order logic. *Information and Computation*, 199:200–227, 2005
- Stefan Berghofer and Tobias Nipkow. Random testing in Isabelle/HOL. In Jorge R. Cuellar and Zhiming Liu, editors, *Software Engineering and Formal Methods (SEFM 2004)*, pages 230–239. IEEE Computer Society, 2004

Refereed conference papers

- Tobias Nipkow and Lawrence C. Paulson. Proof pearl: Defining functions over finite sets. In Joe Hurd, editor, *Theorem Proving in Higher Order Logics (TPHOLs 2005)*, volume 3603 of *Springer Lecture Notes in Computer Science*, pages 385–396. Springer Lecture Notes in Computer Science, 2005
- Veronika Ortner and Norbert Schirmer. Verification of BDD normalization. In Joe Hurd and Tom Melham, editors, *18th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2005*, volume 3603 of *Springer Lecture Notes in Computer Science*, pages 261–277. Springer Lecture Notes in Computer Science, 2005
- Stefan Berghofer. Extracting a normalization algorithm in Isabelle/HOL. In Jean-Christophe Filliâtre, Christine Paulin, and Benjamin Werner, editors, *Types for Proofs and Programs (TYPES 2004)*, LNCS. Springer, 2005
- Steven Obua. Proving Bounds for Real Linear Programs in Isabelle/HOL. In Joe Hurd and Tom Melham, editors, *18th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2005*, volume 3603 of *Springer Lecture Notes in Computer Science*, pages 227–244. Springer Lecture Notes in Computer Science, 2005

Talks

- Stefan Berghofer: *Extracting a normalization algorithm from a proof of weak normalization for the simply-typed Lambda-calculus.* Types workshop, December 2004, Paris.

- Steven Obua: *Proving Bounds for Real Linear Programs in Isabelle/HOL*. Types workshop, December 2004, Paris.
- Veronika Ortner: *Verification of BDD-Algorithms in Isabelle/HOL* Types workshop, December 2004, Paris.

Dissertations

- Gertrud Bauer. *Formalizing Plane Graph Theory — Towards a Formalized Proof of the Kepler Conjecture*. PhD thesis, Technische Universität München, 2005. Submitted

7.8 Nijmegen

Formal Mathematics and Mathematics Education Two theses have been completed that contain large formalisations of mathematics in Coq. Both deal with constructive analysis. The first, by Luis Cruz-Filipe formalizes – in Coq – a considerable part of Bishop's Constructive Analysis (including Rolle's theorem, Taylor's theorem and the Fundamental Theorem of Calculus). The second, by Milad Niqui constructs – in Coq – a model of the real numbers, proves properties about it and shows the model is essentially unique. The thesis of Niqui also studies computationally "good" representations of the reals as infinite objects (e.g. lazy streams), defines algorithms over these representations and proves properties of them. See

The formalization work at Nijmegen has been unified in the "C-CoRN" framework: the Constructive Coq Repository at Nijmegen" which is an extension of the FTA library that already existed. C-CoRN aims at establishing a coherent library of formalised constructive algebra and analysis in Coq.

Barendregt has contributed to the Discussion Meeting "The nature of mathematical proof", organized by the Royal Society in London (Monday 18 to Tuesday 19 October 2004), by a talk "the Challenge of Computer Mathematics" (paper to appear in the Phil. Transactions of the Royal Society).

Proof Technology Wiedijk and Cruz-Filipe have further developed the automation of equational reasoning in Coq by developing the idea of "hierarchical reflection", where equational (rewriting) techniques that operate on various structures in the algebraic hierarchy (monoids, groups, rings, fields) are unified into one.

Foundational Research Loeb and Geuvers have worked on a finer analysis of natural deduction proofs, leading to the notion of "Graph Deduction". Geuvers has also worked with Jojgov on the formalization of the notion of "open proof" in a type theoretic context and the notions of "proof state" and "proof transformation" derived from that.

Publications

Refereed papers

- Michael Beeson and Freek Wiedijk. The meaning of infinity in calculus and computer algebra systems. *Journal of Symbolic Computation*, 39:523–538, 2005.

- Thierry Coquand and Bas Spitters. A constructive proof of the Peter-Weyl theorem. *Mathematical Logic Quarterly*, 4:351–359, 2005.

- Luis Cruz-Filipe. *Constructive Real Analysis: a Type-Theoretical Formalization and Applications.* PhD thesis, Radboud Universiteit Nijmegen, 2004.

- Luis Cruz-Filipe, Herman Geuvers, and Freek Wiedijk. C-corn, the constructive coq repository at nijmegen. In Andrzej Trybulec Andrea Asperti, Grzegorz Bancerek, editor, *Mathematical Knowledge Management, MKM 2004*, LNCS, pages 88–103. Springer, 2004.

- Luis Cruz-Filipe and Freek Wiedijk. Hierarchical reflection. In Ganesh Gopalakrishnan Konrad Slind, Annette Bunker, editor, *Theorem Proving in Higher Order Logics, TPHOLs 2004*, LNCS, pages 66–81. Springer, 2004.

- H. Geuvers and F. Wiedijk. A logical framework with explicit conversions. In Carsten Schürmann, editor, *LFM'04, Proceedings of the Fourth International Workshop on Logical Frameworks and Meta-Languages, Cork*, ENTCS, pages 32–45, 2004.

- Georgi Jojgov and Herman Geuvers. A calculus of tactics and its operational semantics. In Fairouz Kamareddine, editor, *MKM symposium 2003, Edinburgh*, volume 93 of *ENTCS*, pages 3118–137, 2004.

- Milad Niqui. *Formalising Exact Arithmetic: Representations, Algorithms and Proofs*. PhD thesis, Radboud Universiteit Nijmegen, September 2004.

- Milad Niqui and Yves Bertot. QArith: Coq formalisation of lazy rational arithmetic. In Stefano Berardi, Mario Coppo, and Ferruccio Damiani, editors, *Types for Proofs and Programs: International Workshop, TYPES 2003, Torino, Italy, April 30 – May 4, 2003, Revised Selected Papers*, volume 3085 of *LNCS*, pages 309–323. Springer, 2004.

- Russell O'Connor. Essential incompleteness of arithmetic verified by Coq. In Joe Hurd and Thomas F. Melham, editors, *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005, Oxford, UK, August 22-25, 2005, Proceedings*, volume 3603 of *Lecture Notes in Computer Science*, pages 245–260. Springer, 2005.

- Bas Spitters. Almost periodic functions, constructively. *submitted*, 2005.

- Bas Spitters. Approximating integrable sets by compacts constructively. In Laura Crosilla and Peter Schuster, editor, *From Sets and Types to Topology and Analysis – Towards Practicable Foundations for Constructive Mathematics*, page ?? Oxford University Press, 2005.

- Freek Wiedijk. Formal proof skteches. In Stefano Berardi, Mario Coppo, and Ferruccio Damiani, editors, *Types for Proofs and Programs: Third International Workshop, TYPES 2003, Torino*, LNCS, pages 378–393. Springer, 2004.

Talks

- Henk Barendregt, Interactive Computer Mathematics, 3/9/2005, Eindhoven University

- Henk Barendregt, The Challenge of Computer Mathematics, 18/10/2004, Royal Society London

- Henk Barendregt, The Quest for Correctness, 29/11/2004, OzsL Schoolweek (Research School Logic), Nunspeet NL

- Herman Geuvers, Formalization of mathematics in type theory, 30/11/2004 OzsL Schoolweek (Research School Logic), Nunspeet NL

- Freek Wiedijk, The 16 provers of the world, 2/12/2004 OzsL Schoolweek (Research School Logic), Nunspeet NL

7.9 Bialystok

Formal Mathematics and Mathematics Education One of the primary objectives was to develop computer-managed repository of mathematical facts. It was done in three directions: encoding thoroughly chosen textbook, complete translation of papers published in renowned mathematical journals and formalization of well-known non trivial theorems in the field. The results of the work are: encoded three sections of "General Topology" by R. Engelking covering first 47 pages, the paper "New Concepts in the Theory of Topological Space – Supercondensed Set, Subcondensed Set, and Condensed Set" by Y. Isomichi published in Pacific Journal of Mathematics and machine checked proofs of the Brouwer Fixed Point Theorem and the Jordan Curve Theorem.

The use of software created by our consortium (Mizar) in undergraduate eduction was extended into teaching of more advanced courses in mathematics (lattice theory) on graduate level. Some results obtained with the help of proof-assistants were also used in two PhD theses defended last year.

Proof Technology The main objective was to develop both technology for presentation of knowledge and strengthening the computational power of the Mizar checker. The cooperation with other proof-assistants is provided by recently introduced (since Mizar version 7.3.01 issued Feb. 2005) representation of the Mizar Mathematical Library in XML format. This technology improves readability of the proof code for human via an appropriate XSL style-sheet and enables information exchange between cooperating systems. Recent works on using more sophisticated computer algebra techniques connected with Buchberger's algorithm resulted in the strengthening the computational power of the Mizar checker.

Publications

Refereed journal papers

- Adam Grabowski, "On the Computer-Checked Solution of the Kuratowski Closure-Complement Problem" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 25-33
- Adam Grabowski, Magdalena Jastrzebska, "On the Mizar Encoding of the Fibonacci Numbers" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 75-82
- Adam Grabowski, "On the Computer-Assisted Reasoning about Rough Sets" Monitoring, Security, and Rescue Techniques in Multiagent Systems, Advances in Soft Computing Dunin-Keplicz, B.; Jankowski, A.; Skowron, A.; Szczuka, M. (Eds.), 2005, pp. 215-226
- Krzysztof Retel, Anna Zalewska, "Mizar as a Tool for Teaching Mathematics" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 35-42
- Robert Milewski, "Robustness of Systems for Formalizing Mathematics – Testing Monotonicity and Permutability of References in Mizar" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 51-58

- Roman Matuszewski, Piotr Rudnicki, "Mizar: the First 30 Years" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 3-24
- Artur Kornilowicz, Christoph Schwarzweller, "Computers and Algorithms in the Mizar System" Mechanized Mathematics And Its Applications, Vol. 4, No. 1, March 2005, pp. 43-50

Refereed conference papers

- Adam Grabowski, "Solving Two Problems in General Topology via Types" accepted to Types for Proofs and Programs (TYPES 2004) post-proceedings edited by Jean-Christophe Filliatre, Christine Paulin, and Benjamin Werner, LNCS Springer
- Adam Grabowski, Markus Moschner, "Managing Heterogeneous Theories within a Mathematical Knowledge Repository" Proceedings of Mathematical Knowledge Management 2004 edited by Andrea Asperti, Grzegorz Bancerek, and Andrzej Trybulec LNCS 3119, pp. 116-129
- Adam Grabowski, Christoph Schwarzweller, "Rough Concept Analysis - Theory Development in the Mizar System" Proceedings of Mathematical Knowledge Management 2004 edited by Andrea Asperti, Grzegorz Bancerek, and Andrzej Trybulec LNCS 3119, pp. 130-144
- Adam Naumowicz, "Improving Mizar Texts with Properties and Requirements" Proceedings of Mathematical Knowledge Management 2004 edited by Andrea Asperti, Grzegorz Bancerek, and Andrzej Trybulec LNCS 3119, pp. 290-301

Dissertations

- Adam Grabowski, "On the Structure Connected with Substitutions" PhD thesis in mathematics, Silesian University, Katowice, Poland, defended September 13th, 2005
- Adam Grabowski, "Computer-Assisted Theory Exploration: Formalizing Lattice Theory in Mizar" PhD thesis in computer science, Shinshu University, Nagano, Japan defended February 28th, 2005
- Adam Naumowicz, "Mizar Codification of the Theory of Partial Linear Spaces as an Example of Formalizing Recent Mathematical Results" PhD thesis in computer science, Shinshu University, Nagano, Japan defended February 28th, 2005

7.10 Royal Holloway

Formal mathematics and mathematics education R. Adams and Z. Luo have worked on development of logic-enriched type theory in the logical framework PAL+ and its use in formalization of different approaches to mathematics, including WeylŠs classical predicative mathematics.

Proof technology J. Pang, together with P. C. Callaghan and Z. Luo, has worked on the domain-specific reasoning, publishing a paper in Journal of Computer Science and Technology.

Y. Luo has implemented a prototype system of PAL+ and the system UTT (inductive types and universes). R. Pollack, since arriving at Royal Holloway in June, is implementing a proof checker for PAL+.

Foundational research Y. Luo and Z. Luo have worked on transitivity of coercive sub-typing, publishing a paper in Information and Computation.

R Adams and Z Luo has been studying logic-enriched type theories, its metatheories and its applications.

Publications

Refereed journal papers

- Z. Luo and Y. Luo. Transitivity in coercive subtyping. Information and Computation, 197(1-2), pp 122-144. 2005.
- J. Pang, P.C. Callaghan and Z. Luo. LFTOP: an LF-based approach to domain-specific reasoning. Journal of Computer Science and Technology. 2005. To appear.

Refereed conference papers

- R. Admas. Formalized Metatheory with Terms Represented by an Indexed Family of Types. Submitted for publication in Proceedings of TYPES 2004 Workshop.

Dissertations

- Y. Luo. Transitivity in Coercive Subtyping. PhD thesis, Univ of Durham. Dec 2004. (Supervisor: Z. Luo)

7.11 Edinburgh

Correctness of Computer Systems: Longley and Pollack developed a program logic for reasoning about pure functional ML programs. This logic is implemented in ISABELLE/HOL (one of the TYPES proof tools), and examples are developed.

Proof Technology: Aspinall and others: Proof General, a widely used generic interface for proof assistants. Existing version used by many of the TYPES research tools. A new version based on modern technology is in development.

Dixon, Fleuriot and others: Proof Planning, the use of very high-level tactics to bring formal machine-checked proof closer to informal mathematics, both for construction of proofs and their readability and maintainability. Tools for proof planning in Isabelle/HOL have been developed.

Momigliano, Pollack, Power: Reasoning about languages with binding. This is currently a hot topic in the programming language research community, thus extending the impact of TYPES to other researchers. Momigliano and Pollack have given talks and organized workshops, both in TYPES and outside TYPES, bringing researchers together. There is a hot email group on this topic that we have contributed significantly to.

Pollack co-organised a workshop "Binding Challenges 2005" (Kanazawa, Japan, April 24 - 25, 2005). This workshop continued some of the work from the Small TYPES workshop "Types for Mathematics" (Nijmegen Nov 1-2, 2004). Further progress directly following from this workshop was reported in the TYPES Workshop MERLIN (Tallinn, Sept 30, 2005).

Publications

Refereed journal papers

- L. Dixon and J. D. Fleuriot. "A Proof-Centric approach to Mathematical Assistants". To appear in Journal of Applied Logic: Special Issue on Mathematics Assistance Systems.

Refereed conference papers

- Longley, Pollack: "Reasoning about CBV functional programs in Isabelle / HOL". In "Theorem Proving in Higher Order Logics". TPHOLs, Sept. 2004." Springer-Verlag LNCS 3223.
- L. Dixon and J. D. Fleuriot. "Higher Order Rippling in IsaPlanner". Theorem Proving in Higher Order Logics 2004 (TPHOLs'2004), (Springer LNCS 3223).

7.12 Manchester

Formal Mathematics and Mathematics Education Robin Adams has been experimenting with the formalization of mathematics in logic-enriched type theories. This work has been done within the prototype implementation of the logical framework PAL+ developed for the Pythagoras project.

Peter Aczel has supervised several Manchester MSc dissertations including "Investigations into the software systems for learning mathematical theorem proving and problem solving techniques" and "Toward the automation of category theory - an implementation in Coq".

Foundations Robin Adams has been investigating the metatheory of logical frameworks.

Peter Aczel developed a theory of type setups for predicate logic that provides an abstract setting for a generalization of the notion of a logic-enriched type theory previously developed by Gambino and Aczel.

Joao Belo completed an MSc dissertation that gives a semantics and completeness proof for classical predicate logic over a type setup. Joao Belo has gone on to study for a PhD fibrational semantics for dependently sorted logics, a further generalization of logic-enriched type theories. He plans to investigate the general theory of dependently sorted logic and possible applications.

Peter Aczel has continued to work on Constructive Set Theory and the development of Constructive Mathematics, particularly point-set and point-free Topology. Chris Fox completed his PhD on this topic supervised by Aczel.

Publications

Refereed journal papers

- Adams, *"Pure Type Systems with Judgemental Equality"*, accepted for publication in the Journal of Functional Programming.
- Gambino and Aczel, *"The Generalised Type-theoretic Interpretation of Constructive Set Theory"*, submitted to the Journal of Symbolic Logic.
- Aczel, *"Aspects of General Topology in Constructive Set Theory"*, to appear in a special issue of the Annals of Pure and Applied Logic, 200?.

Refereed conference papers

- Adams, *"Formalized Metatheory with Terms Represented by an Indexed Family of Types"*, submitted for publication in Proceedings of TYPES 2004 Workshop.

Talks

- Adams, *"A Formalization of the Theory of Pure Type Systems in Coq"* (TYPES 2004 Workshop, December 2004)
- Aczel, *"Type Setups for predicate logic"* (TYPES 2004 Workshop, December 2004)

- Aczel, *"Weak Constructive Set Theory"* (CLM 2004, Benediktbeuern, November 2004)
- Aczel, *"Topology in Constructive Set Theory"* (Oberwolfach, March 2005)
- Aczel, *"Short course on Constructive Set Theory"* (ASL summer meeting, July-August 2005)

Dissertations

- Adams, *"A Modular Hierarchy of Logical Frameworks"*, University of Manchester, 2004.
- Fox, *"Point-set and Point-free Topology in Constructive Set Theory"*, University of Manchester, submitted September 2005.

7.13 Torino

Foundational Research: We investigate some syntactic properties of Wadler's dual classical sequent calculus, a term calculus which corresponds to classical sequent logic in the same way that Parigot's lambda-ţ calculus corresponds to classical natural deduction. Our main result is strong normalization theorem for reduction in the dual calculus; we also prove some confluence results for the typed and untyped versions of the system. We clarify the relation of the dual calculus to Gentzen's system LK. Also, research has been done in categorial proof theory at the border between logic and category theory.

Proof technology: More in general, we investigate how to develop algorithm, inspired by constructive interpretation of classical proofs, able to learn from their mistakes and improve their own results, applying mathematical tools developed in Game Theory. The algorithms we plan to study start with a question given by the user, then make some hypothesis about the correct answer, and check it through examples. If they find some counterexample, they use the very counterexample they found to make some better hypothesis, and re-check it. If also the new hypothesis is discarded, they use the new counterexample to find an even better hypothesis, and so forth. This class of algorithms is suitable in all cases in which the correctness of the answer we are looking for can be checked through a finite list of sample cases.

Publications

Refereed journal papers

- Kosta Dosen, Zoran Petric: "Proof-Theoretical Coherence" KCL Publications, London, (book: pages 1-377).
- Dan Dougerty, Silvia Ghilezan, Pierre Lescanne, Silvia Likavec: "Strong normalization of the dual classical sequent calculus" accepted for LPAR 2005 to appear in LNCS (refereed conference).
- S. Berardi. A generalization of conservativity theorem for classical versus intuitionistic arithmetic. MLQ, 50(1):41-46, 2004.
- S. Berardi and C. Berline. Building continuous webbed models for system f. TCS, 315:3-34, 2004.
- S. Valentini S. Berardi. Krivine's intuitionistic proof of Classical Completeness. APAL, 129:93-106, 2004.
- S. Berardi. Classical Logic as Limit Completion. MSCS, 15(01): 167-200, 2005.
- S. Berardi "Some Intuitionistic Equivalent of Classical Principles for degree 2 Formulas", Annals of Pure and Applied Logic, 2005, to appear.

7.14 Udine

Formal Mathematics and Mathematics Education A new representation for the real numbers that can be conveniently used to implement exact real number computation with a lazy programming languages, with a real number version of the Karatsuba algorithm for multiplication, has been developed by Lenisa, Power and Watanabe.

Foundational Research Gianantonio has presented an alternative formulation of the multiplicative fragment of cyclic linear logic of Yetter. The new presentation uses, as formalism, the calculus of structures, and has the interesting feature of avoiding the cycling rule.

Miculan has presented a category theoretic model where both ?variables? and ?names? are particular cases of the more general notion of "distinction". Initial algebra/final coalgebra constructions can be transferred from the former models to the new.

We have used the concept of a distributive law of a monad over a copointed endofunctor to define and develop a reformulation and mild generalization of Turi and Plotkin's notion of an abstract operational rule.

The model construction technique of Linear Realizability can be used to provide fully complete models for various typed lambda-calculi and lambda-theories.

Publications

Refereed journal papers

- M. Lenisa, J. Power, H. Watanabe, "Category theory for operational semantics", Theoretical Computer Science 327 (2004), 135–168.
- S. Abramsky, M. Lenisa, "Linear realizability and full completeness for typed lambda-calculi", Annals of Pure and Applied Logic 134 (2005), 122-168.
- F. Alessi, M. Dezani-Ciancaglini, S. Lusin. "Intersection types and domains operators." Theoretical Computer Science 316, 25-47, 2004.
- F. Alessi, M. Dezani-Ciancaglini, F. Honsell. "Inverse limit models as filter models", HOR '04, 2nd International Workshop on Higher-Order Rewriting (Delia Kesner, Femke van Raamsdonk, Joe Wells eds.) 2004.

Refereed conference papers

- P. Di Gianantonio: Structures for Multiplicative Cyclic Linear Logic: Deepness vs Cyclicity. Proceeding of CSL 2004. LNCS 3210, pp. 130-144.
- P. Di Gianantonio and P. L. Lanzi: "Lazy Algorithms for Exact Real Arithmetic", Workshop of the COMETA project on Computational Metamodels. ENTCS 104(C), pp. 113–12.
- M. Miculan, K. Yemane: "A unifying model of variables and names". In Proceedings of FOSSACS'05. LNCS 3441, pages 170-186, 2005.

7.15 Warsaw

Daria Walukiewicz-Chrzaszcz and Jacek Chrzaszcz worked on consistency and completeness of definitions by rewriting in the calculus of constructions. They showed that consistency follows from the assumption that all functions defined by rewrite rules are complete and presented a sound and terminating, but necessarily incomplete algorithm to verify this property. The algorithm accepts all definitions by pattern matching from functional programming languages. Moreover, for dependent types, the algorithm accepts also definitions without impossible cases, like an empty list in the definition of the "head" function on lists.

Jacek Chrzaszcz and Jean-Pierre Jouannaud from Ecole Polytechnique worked on comparison of module systems in OBJ, ML and Coq. They studied the example of abstract sorting algorithm based on a priority queue in order to show the similarities and differences in these approaches. All three systems provide the possibility to define parametric modules. However, in OBJ a particular form of parametricity can also be obtained by the so-called theory extension which is missing from ML and Coq module systems. On the other hand in the latter two it is possible to define a higher-order functor, not available in OBJ. A second order functor ideally represents the structure of the example of sorting by priority queues.

Aleksy Schubert worked on automata approach to the problem of non-structural subtype entailment problem. An instance of the problem is a pair set A of subtype inequalities and a subtype inequality e. The question is to asses if there is a substitution for which all the inequalities in A hold and the inequality e does not hold. The solution of this problem leads to stronger methods for ensuring program correctness based on type systems.

Publications

Refereed journal papers

- Marek Zaionc "Probability distribution for simple tautologies", accepted for Theoretical Computer Science, to appear in 2005
- Marek Zaionc "Probabilistic approach to the lambda definability for fourth order types", accepted at Electronic Notes in Theoretical Computer Science, to appear in 2005
- P. Waszkiewicz, R. Kopperman, H.-P. Kunzi Bounded complete models of topological spaces, Topology and Its Applications 139 (2004), 285-297
- P. Waszkiewicz, Completeness and Compactness of Quantitative Domains Lecture Notes in Computer Science 3623, Springer, 2004, pp 341-351
- P. Waszkiewicz, Approximations simply characterized, Electronic Notes in Theoretical Computer Science 2004, to appear in 2005

7.16 Tallinn

Correctness of Computer Systems A. Saabas and T. Uustalu developed a new compositional approach to semantic and logic description of low-level languages, where a piece of code is a flat set of labelled instructions with no explicit structure. A salient feature of the approach is direct support for compositional compilation of high-level program proofs.

Foundational Research Summing up their earlier work, A. Abel, R. Matthes and T. Uustalu published a thorough comparative study of the rewriting metatheory of structured recursion schemes for higher-order and nested data-types.

N. Ghani, T. Uustalu and V. Vene gave a new semantic footing to the 'fold'/'build' syntax of programming with inductive types and the corresponding short-cut deforestation transformation. This is based on the equivalence of the standard initial algebra semantics of inductive types to an alternative one which interprets inductive types as limits of algebra-structure forgetting functors. They also showed that a useful 'augment'-like combinator is definable for a far wider class of parameterized inductive types than free monads, namely for all monads arising from a parameterized monad via an initial algebra construction.

T. Uustalu and V. Vene developed a new method to describe the semantics of dataflow programming languages based on comonads and distributive laws as central structuring devices. This extends Moggi and Wadler's approach to effectful computation to context-dependent computation. Capitalizing on this work, they also formulated a comonadic approach to attribute grammar specification languages. This relies on the comonad structure present in zipper data-types.

Publications

Refereed journal papers

- T. Uustalu, V. Vene. Signals and comonads. J. of Univ. Comput. Sci., v. 11, n. 7, pp. 1310-1326, 2005.
- N. Ghani, T. Uustalu, V. Vene. Generalizing the augment combinator. In H.-W. Loidl, ed., Trends in Functional Programming 5, Intellect, to appear.
- A. Abel, R. Matthes, T. Uustalu. Iteration schemes for higher-order and nested datatypes. Theor. Comput. Sci., v. 333, n. 1-2, pp. 3-66, 2005.

Refereed conference papers

- T. Uustalu, V. Vene. The essence of functional programming (short version). In K. Yi, ed., Proc. of 3rd Asian Symp. on Programming Languages and Systems, APLAS 2005 (Tsukuba, Nov. 2005), v. 3780 of Lect. Notes in Comp. Sci., pp. 2-18. Springer-Verlag, 2005.
- A. Saabas, T. Uustalu. A compositional natural semantics and Hoare logic for low-level languages. In P. D. Mosses, I. Ulidowski, eds., Proc. of 2nd Wksh. on Structured Operational Semantics, SOS 2005 (Lisbon, July 2005), Electr. Notes in Theor. Comput. Sci., Elsevier, to appear.

- T. Uustalu, V. Vene. Signals and comonads. In M. A. Musicante, R. M. F. Lima, eds., Proc. of 9th Brazilian Symp. on Programming Languages, SBLP'05 (Recife, PE, May 2005), pp. 215-228. Univ. de Pernambuco, Recife, 2005.

- N. Ghani, T. Uustalu, V. Vene. Build, augment and destroy, universally. In W.-N. Chin, ed., Proc. of 2nd Asian Symp. on Programming Languages and Systems, APLAS'04 (Taipei, Nov. 2004), v. 3302 of Lect. Notes in Comp. Sci., pp. 327-347. Springer-Verlag, 2004.

7.17 Bergen

Correctness of Computer Systems We have developed 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. The language features are: instantiation and reuse of components, explicit deallocation as well as sequential composition, choice and and a scope operator.

Formal Mathematics and Mathematics Education We have carried out a formal verification of Hessenberg's Theorem stating that the Pappus' Axiom implies Desargues' Axiom in projective plane geometry. Large parts of the verification have been automated.

Proof Technology We have developed a program that can disprove false statements in Geometric Logic. This complements an already existing theorem prover.

Publications

Refereed conference papers

- M.A. Bezem. *Disproving Distributivity in Lattices Using Geometric Logic.* In W. Ahrendt, P. Baumgartner and H. de Nivelle, editors, *Proceedings of the CADE workshop DISPROVING*, Tallinn, Estonia, 22 July 2005, pages 24–31.

7.18 Helsinki

The site has been working mainly on proof systems for various logics and mathematical theories. Systematic results on the structural analysis of proofs have been achieved with what are known as intermediate logics (those between intuitionistic and classical). These have been also studied by algebraic methods that have given new and fast algorithms for proof search. Secondly, modal and related logics have been studied, with a proof of normalization for the standard modal logic S4. Proof-theoretical methods have been further applied to foundational problems in elementary arithmetic, with improved proofs of known results such as the existence property for Heyting arithmetic, and Gentzen's result on the consistency of arithmetic.

Publications

Refereed journal papers

- Sara Negri and Jan von Plato: Proof systems for lattice theory, Mathematical Structures in Computer Science, vol. 14 (2004), pp. 507-526.
- Sara Negri, Jan von Plato, and Thierry Coquand: Proof-theoretical analysis of order relations, Archive for Mathematical Logic, vol. 43 (2004), pp. 297-309.
- Jan von Plato: Normal derivability in modal logic, Mathematical logic Quarterly, vol. 51 (2005), pp. 632-638.

Refereed conference papers

- Sara Negri and Jan von Plato, The duality of classical and constructive notions and proofs, in L. Crosilla and P. Schuster, eds, From Sets and Types to Analysis and Topology: Practicable Foundations for Constructive Mathematics, Oxford University Press 2005.

7.19 Minho

J. Espírito Santo and L. Pinto continued work on the generalised multiary lambda-calculus LambdaJm. On the one hand, they studied the relationship of LambdaJm with natural deduction, found a new argument for strong normalisation of reduction and established preliminary results on the interaction between reduction and permutative conversions. On the other hand, jointly with M.J. Frade, they explored the overlap between generality and multiarity and produced a refined study of permutative conversions and a refined view of the internal structure of LambdaJm.

J. Espírito Santo [1] studied a refined version of the lamba-calculus with generalised applications, obtaining an isomorphism between normalisation in this system and cut-elimination in a sequent calculus.

In collaboration with T. Uustalu, L. Pinto worked on propositional dual intuitionistic logic, establishing a decision procedure and a method for counter-model construction. Work in progress under this topic aims at establishing a contraction-free formulation of the logic and at investigations into computational interpretations of the logic.

7.20 Padova

Faggian and Maurel (Paris) have proposed Ludics nets (L-nets) as a game model of concurrent interaction.

Maietti and Sambin have introduced minimal type theory, a variant of Martin-Löf's intensional type theory in which propositions are defined inductively but independently of sets, and have shown that extensional concepts (the "toolbox") can be developed over it. They have shown that these two different levels of abstraction are needed for a systematic formalization of mathematics: the "program" level, where to implement computations, and the "proof" level, where to perform proofs as in the common mathematical practice (while keeping compatibility with traditional foundations for mathematics, like classical set theory, the internal theory of a topos, Aczel's set theory and Martin-Löf's type theory). The methodology by which the two levels are connected (called the forget-restore principle) is a precise proposal to connect intensionality with extensionality (see the problem mentioned in Annex 1, sect. 2.4).

Maietti and Valentini performed a categorical analysis of formal topologies with particular focus on the exponentiation of inductively generated formal topologies

Based on a modular correspondence between type theoretic constructors and categorical properties, Maietti has produced an internal type theory for various categorical structures. She used the internal type theory of Joyal's arithmetic universes to get categorical results about sketches that can be used for a better conceptual modelling of databases.

Publications

Refereed journal papers

- G. Battilotti, G. Sambin, Pretopologies and a uniform presentation of sup-lattices, quantales and frames, Annals of Pure and Applied Logic, to appear
- Berardi S., Valentini S., Krivine's intuitionistic proof of classical completeness (for countable languages), Annals of Pure and Applied Logic 1-3 (2004), pp. 93-106
- Boniolo G., Valentini S. Vagueness, Kant and Topology, Journal of Philosophical Logic, to appear
- G. Curi, On the collection of points of a formal space, Annals of Pure and Applied Mathematics, to appear
- M.E. Maietti, P. Maneggia, V. de Paiva, and E. Ritter, Relating Categorical Semantics for Intuitionistic Linear Logic, Applied Categorical Structures 13 (2005), pp. 1-36
- M.E. Maietti. Modular correspondence between dependent type theories and categories including pretopoi e topoi, Mathematical Structures in Computer Science, to appear
- M.E. Maietti and S. Valentini, A structural investigation on formal topology: coreflection of formal covers and exponentiability. Journal of Symbolic Logic 69 (2004), pp. 967–1005

- Valentini S., The problem of the formalization of constructive topology, Archive for mathematical Logic 44 (2005), pp. 115-129
- Valentini S., Every countably presented formal topology is spatial, classically. Journal of Symbolic Logic, to appear
- Claudia Faggian, Ludics and interactive observability: the geometry of tests, Theoretical Computer Science, to appear

Refereed conference papers

- Faggian, Claudia and Maurel, FranĐois, Ludics Nets, a game model of concurrent interaction, Proceedings 20th annual Symposium on Logic in Computer Science(LICS'05), IEEE Computer Society Press 2005, pp. 376–385
- Curien, Pierre-Louis and Faggian, Claudia, L-nets, strategies and proof-nets, Proceedings of annual conference on Computer Science Logic(CSL'05), Springer LNCS 3634, 2005, pp. 167–183
- M.E. Maietti and G. Sambin, Toward a minimalist foundation for constructive mathematics, in: "From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics", Oxford University Press, edited by L. Crosilla and P. Schuster, October 2005.
- M.E. Maietti, Predicative exponentiation of locally compact formal topologies over inductively generated ones, in "From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics", Oxford University Press, edited by L. Crosilla and P. Schuster, October 2005.
- M.E. Maietti, Reflection into models of finite decidable FP-sketches in an arithmetic universe, "Category Theory and Computer Science, 2004", Electronic Notes in Theoretical Computer Science 122, Elsevier 2005, pp. 105–126.

Talks

- G. Curi, Exact approximations to Stone-Cech compactification, Summer Topology Conference, section: topology in computer science (Denison University, Ohio, 10-13 July 2005)
- G. Curi, Effective topology via formal space, seminar given at the Department of Mathematics, University of Manchester (invited by Peter Aczel, May 7, 2005).
- M.E. Maietti (joint work with V. de Paiva) Relating algebraic models of predicate logic, 1st World Congress on Universal Logic, Montreux, Switzerland, 31/3-3/4/2005.

7.21 Savoie

Correctness of Computer Systems F. Ruyer, in his thesis, studies more precisely Raffalli's system ST, giving a complete subject reduction proof, which is new, and studying its semantics, the expressiveness and the limits of the system. We build on this basis a functionnal language with first-order modules containing specifications in their signature, which is also new, and give a correctness proof.

Formal Mathematics and Mathematics Education The proof by contextual menu presented by C. Raffalli in the last TYPES meeting is a very powerful new tool to use proof assistants. We are starting to use it for teaching and it seems promising. The user explains what he wants to do by some clicks and selections (for instance by clicking on an hypothesis to use it) and is presented with a choice of sentences in natural language (French or English) which could be part of an informal proof. Then it suffices to make a choice to continue the proof. This approach considerably diminish the learning time of the prover.

Foundational Research R. David and K. Nour, have made good progress toward the comprehension of normalization in classical natural deduction. They managed many proof of strong normalization for various proof systems.

Publications

Refereed journal papers

- K. Nour and K. Saber A semantics of realizability for the classical propositional natural deduction Accepted in Electronic Notes in Theoretical Computer Science, 2005
- R. David and K. Nour Why the usual candidates of reducibility do not work for the symmetric lambda-mu-calculus Accepted in Electronic Notes in Theoretical Computer Science, 2005
- K. Nour and K. Saber A semantical proof of the strong normalization theorem of full propositional classical natural deduction Accepted in Archive for Mathematical Logic, 2005

Refereed conference papers

- R. David and K. Nour Arithmetical proofs of strong normalization results for the symmetric lambda-mu-calculus TLCA 2005, LNCS 3461, pp. 162-178, 2005

7.22 Swansea

Proof Technology A. Setzer has developed with P. Dybjer indexed inductive-recursive definitions. This provides a type theory in which all standard extensions of Martin-Löf type theory (MLTT) can be formulated. He has together with P. Hancock developed a generalisation of guarded induction in dependent type theory and developed a type theory with weakly final coalgebras.

M. Michelbrink and A. Setzer have investigated state dependent monads in type theory. M. Michelbrink has generalised P. Hancock and A. Setzer's notion of interfaces. This gives rise to the investigation of different categories of interactive games.

M. Roggenbach has developed in cooperation with Dr. Y. Isobe (AIST, Japan) CSP-Prover, a generic theorem prover for the process algebra CSP based on Isabelle-HOL. CSP-Prover has been extended by a package for deadlock analysis.

U. Berger has implemented, in collaboration with H. Schwichtenberg, P. Letouzey (LMU Munich) and S. Berghofer (TU Munich), strong normalisation proofs for the simply typed lambda calculus in the Proof systems Coq, Isabelle and Minlog. From each of the proofs an efficient normalisation program (normalisation by evaluation) has been extracted fully automatically.

Foundational Research. A. Setzer has developed a model for MLTT with one Mahlo universe and a lower bound for its proof theoretic strength.

M. Roggenbach has worked out the semantical foundations of CSP-CASL, a novel combination of algebraic specification and process algebra.

U. Berger has developed in collaboration with S. Berardi (Turin) a novel computational interpretation of classical logic and arithmetic via dynamic learning objects (work in progress). He has as well developed a new domain-theoretic technique for proving strong normalisation of higher type rewrite systems.

Publications

Refereed journal papers

- A. Setzer: *Proof theory of Martin-Löf type theory - An overview.* Mathematiques et Sciences Humaines, 42 année, n^o 165, 2004, p. 59–99.
- U. Berger: *Uniform Heyting Arithmetic*, Annals of Pure and Applied Logic 133, 2005, p. 125-148.
- U. Berger: *Strong normalization for applied lambda calculi* LMCS 1 (2), 2005, p. 1-14.

Refereed conference papers

- M. Michelbrink, A. Setzer: *State-dependent monads in type theory.* Electronic Notes in Theoretical Computer Science, 122 (2005) 127 – 146.
- U. Berger, P. Oliva: *Modified Bar Recursion and Classical Dependent Choice.* Proceedings of the ASL Locic Colloquium'01, Vienna, A.K. Peters, Lecture Notes in Logic, 2005, p. 89-107.

- Y. Isobe, M. Roggenbach: *A generic theorem prover of CSP refinement.* In N. Halbachs, L. D. Zuck (Eds): Tools and Algorithms for the Construction and Analysis of Systems. Proceedings of TACAS '05. LNCS 3440, pp. 108–123, Springer 2005.

Talks

- P. Hancock, A. Setzer: Interactive programs and weakly final coalgebras in dependent type theory. In: L. Crosilla, P. Schuster (Eds.): *From sets and types to topology and analysis: Towards practicable foundations for constructive mathematics.* Oxford Logic Guides, Oxford University Press, 2005, p. 115 – 136. (Invited plenary talk).

- A. Setzer: *Universes in type theory I – Inacccessibles and Mahlo.* 32 pp, 2005. After revision to appear in Proceedings of the Logic Colloquium 2004, Turin, Italy. (Invited special session talk).

- U. Berger: Continuous semantics for strong normalization. In: S. Barry Cooper, Benedikt LŽwe, Leen Torenvliet: *New Computational Paradigms. Proceedings of CiE, Amsterdam, 8-12 June 2005.* Springer Lecture Notes in Computer Science 3526, p. 23-34. (Invited special session talk).

- U. Berger: An abstract strong normalization theorem. In: Luke Ong: *Computer Science Logic. Proceedings of CSL, Oxford, 22-25 August 2005*, Springer Lecture Notes in Computer Science 3634, p. 27-35. (Invited plenary talk).

7.23 Toulouse

The group is working in two main areas:

- Results about strong normalization and confluence of simply-typed lambda-calculus with inductive types extended by non-standard reductions. Main cases studied: the notion of "copy" and "isomorphic copy" of a type and related reductions; finite types and related reductions.

- Results about proof-theory of multiplicative linear logic with categorical equivalence relations on derivations. Main new contribution: the study of equivalence relations corresponding to non-free categorical structures. Application to verification of commutativity of diagrams in computer algebra.

Publications

Refereed journal papers

- D. Chemouil. Isomorphisms of Simple Inductive Types through Extensional Rewriting. - to appear in Math. Str. in Comp. Sci., 15 (5), 2005.

- F. Barral, D. Chemouil, S. Soloviev. Non-standard reductions and categorical models in typed lambda-calculus. - Accepted for publication in "Logicheskie Issledovaniya" (Studies in Logic), series published by editions "Science", Moscow, Russia.

- L. Mehats, S. Soloviev. Permutability of Inferences and Categorical Equivalence of Derivations in IMLL. - Accepted for publication in Notes of Scientific Seminars of Tver University (Russia).

- S. Soloviev. Foreword of the special issue of Math. Str. in Computer Science on Isomorphism of Types (to be published as MSCS 15(5), 2005).

Dissertations

- David Chemouil. "Types inductifs, isomorphismes et recriture extensionnelle". Ph. d. thesis. Toulouse, september 2004. (Adviser S. Soloviev)

7.24 Birmingham

Correctness of Computer Systems Mark Ryan and Eike Ritter are also working on verification of security protocol using formal methods. The latest work concerns multi-party protocols, for example contract signing protocols, where a trusted third-party is necessary for the execution of the protocol. Both semantic approaches (eg via Strand-spaces) as well as model checking tools have been used in this work.

Formal Mathematics and Mathematics Education Manfred Kerber has been working on mathematical knowledge representation systems. His work shows how to represent matrices in a theorem prover in a way which is very close to the mathematical textbook style. He also shows how to represent different formalisations of the same problem in a theorem prover in such a way that the theorem prover can use concepts from both formalisations to solve a given problem, for example the mutilated checker board problem.

Foundational Research Ritter and Maietti (from Padova) classified categorical models for linear logic and extended it to capture variants of linear logic which have been used to model resource usage.

Proof technology David Pym and Eike Ritter have continued their work on semantics for proof search. The most recent work gives a semantics for the connection method, which is used in several automated theorem provers. More generally, this semantics also models search strategies used in theorem provers based on resolution.

Publications

Refereed journal papers

- M.E. Maietti, P. Maneggia and V. de Paiva and E. Ritter. Relating Categorical Semantics for Intuitionistic Linear Logic. Applied Categorical Structures, 13(1). 2005.

Refereed conference papers

- S. Kremer, A. Mukhamedov and E. Ritter. Analysis of a Multi-Party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space model. 2005 Conference on Financial Crytography and Data Security. 2005. To appear in LNCS.
- M. Kerber and M. Pollet. A Tough Nut for Mathematical Knowledge Management. 2005 Conference on Mathematical Knowledge Management. 2005. To appear.
- Martin Pollet, Volker Sorge and Manfred Kerber. Intuitive and Formal Representations: The Case of Matrices. MKM04. LNCS3119. 2004.
- N.Zhang and M.D. Ryan and D. Guelev. Evaluating Access Control Policies Through Model Checking. Eighth Information Security Conference (ISC'05). LNCS3650. 2005.

- S. Kremer and M.D. Ryan. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. ESOP05, LNCS3444. 2005.

7.25 Nottingham

Correctness of computer systems Based on discussion within the Nottingham group (Altenkirch,Chapman,Morris,Swierstra) and others in the TYPES project, among them McKinna and Brady (St Andrews) and Callaghan (Durham), McBride has continued to develop the Epigram system, a dependently typed programming language and program development system, which is available from http://www.e-pig.org/.

Jointly with Altenkirch and McBride, Morris has investigated the use of dependent types for datatype generic programming, while Chapman has implemented an independent type checker for Epigram's underlying programming language.

Foundational research Abott, Altenkirch,Ghani and McBride have investigated a generic representation of datatypes, container types, which use dependent types and used them to investigate the notion of a derivative of a datatype which has applications in generic symbolic programming. This work is currently expanded and will feed into the practical work on the Epigram system.

Altenkirch and McBride are working on Observational Type Theory, a variant of extensional Type Theory with decidable type checking.

Publications

Refereed journal papers

- Michael Abbott, Thorsten Altenkirch, and Neil Ghani. Containers - Constructing Strictly Positive Types. *Theoretical Computer Science, 342:3-27*, September 2005. Applied Semantics: Selected Topics.
- Michael Abbott, Thorsten Altenkirch, Neil Ghani, and Conor McBride. PARTIAL for data. Fundamentae Informatica 65(1,2):1–28. March 2005. Special Issue on Typed Lambda Calculi and Applications 2003.

Refereed conference papers

- James Chapman, Thorsten Altenkirch, and Conor McBride, Epigram Reloaded: A Standalone Typechecker for ETT. Preliminary proceedings of Trends in Functional Programming, September 2005.
- Healf Goguen, Conor McBride, and James McKinna. A few constructions on constructors. To appear in the proceedings of TYPES 04.
- Peter Morris, Thorsten Altenkirch and Conor McBride. Exploring the Regular Tree Types. To appear in the proceedings of TYPES 04.

Talks

- Conor McBride. Practical dependently typed programming in Epigram. In T. Uustalu and V. Vene, editors. Advanced Functional Programming, volume 3622 of LNCS, pages 130-171. Springer-Verlag, 2005.

7.26 Sheffield

E. Lewis-Kelham has just completed his PhD thesis on "Multi-Level Lax Logic". His work was greatly aided by detailed conversations he had with members of the TYPES project at their December-2004 meeting; he would not have been able to attend this meeting without financial support from TYPES.

B Norton has worked on timed process calculi, esp developing a new CaSE calculus and Haskell representations of relevant processes.

M Stannett has been Ed's and Barry's PhD supervisor and is currently working on an algebraic analysis of the abstract structure of Lax Logic.

Publications

Refereed conference papers

- Barry Norton. 'Behavioural Types for Synchronous Software Composition' Workshop on Foundation of Interface Technologies (FIT 2005)
- Barry Norton, Simon Foster, Andrew Hughes. 'A Compositional Operational Semantics for OWL-SŠ. 2nd International Workshop on Web Services and Formal Methods (WS-FM 2005) LNCS 3670
- Barry Norton. 'Quality of Service Profiles for Web Services' 4th International Conference on COTS-Based Software Systems (ICCBSS 2005) LNCS 3412
- Barry Norton, Matt Fairtlough. 'Reactive Types for Dataflow-Oriented Software Architectures' 4th Working IEEE/IFIP Conference on Software Architecture (WICSA04) IEEE Computer Society Press P2172

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

Our work is disseminated in the traditional ways earlier described in this report (published journal papers, conference papers, workshop presentations, lectures in the summer school, visits), but also in the regular activity of a researcher (classes, seminars, graduate and undergraduate students etc). One of the main activity of a university researcher is exactly dissemination of knowledge.

Our proof systems (including Coq, 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.

Benjamin Werner from Inria participated in the formal proof of the four-color theorem finished by Georges Gonthier by the end of 2004. Therefore, he and Gilles Dowek have been mentioned in various scientific magazines for wider audience. Coq was cited in even more cases in this respect (citations include Science, Süddeutsche Zeitung, La Recherche, Science et Vie, AFP and others).

A.3 Publishable results

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