510996

TYPES
Types for Proofs and Programs

Coordination Action
FP6-2002-IST-C

Periodic activity report no 2
revised version

Period covered: Sept 1, 2005 – July 31, 2006

Date of preparation: November 30, 2006

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

Coordinator: Bengt Nordström, Chalmers University of Technology

Contents

Summary of the Types project, 1.9.2005 – 31.7.2006

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

The funding for the Types project goes to coordination of and communications between research groups. The research itself is funded by other sources. The Types consortium receives funding for three annual meetings to communicate recent work throughout, at least six smaller thematic workshops on designated research themes, one summer school, short courses and short visits between sites.

The consortium is coordinated by by Bengt Nordström (Chalmers University, Göteborg, Sweden) and consists of 35 research groups from universities and industries in Europe. It would have been unfeasible to let all groups be full participants in the action. In order to manage this, we have created a two-level hierarchy with 15 main sites (the contractors of the project) and 21 subsites (subcontractors). The following are the main sites: Chalmers, CNRS – Paris 7, INRIA-Futurs, INRIA-Sophia, Paris – Sud, 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 second annual report. During this year we organized the Types 2006 Conference, four small workshops and had many short visits between the sites.

Types 2006 Conference. The meeting took place in Nottingham, UK in April 18 – 21. It attracted more than 100 participants and there were more than 60 regular presentations.

Small Workshop: MERLIN 2005 , MEchanized Reasoning about Languages with varIable biNding This workshop took place in Tallinn, Estonia on 30 September 2005. There were 30 participants and 7 accepted papers.

Small Workshop: Constructive analysis, types and exact real numbers The workshop was organized by the Nijmegen group and had 34 participants and 14 talks.

Small Workshop: Isomorphism of Types This workshop took place in Toulouse 28 – 29 Oct 2005.

Small Workshop: Mathematically Structured Functional Programming, July 2006 This small workshop on a TYPES-related theme was held on July 2, 2006 in Kuressaare, Estonia.

Cooperation, visits and coauthored papers The full report describes briefly around 40 different cooperation activities inside the Types project. There were 26 refereed scientific papers with coauthors from different sites produced during the reporting period. In addition to this, there were 28 refereed coauthored conference contributions. There were more than 80 visits between the sites and more than 50 talks were given during these visits.

Industrial cooperation There are at least 13 projects where the different research groups cooperates in industrial projects.

The Types web page The home page of the Types project was completely rebuilt during this period. It can be found at:

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

We think it is important that we have an open atmosphere, this should hold for all scientific enterprises. All our meetings are widely announced and open to everybody, this includes our summer school, the annual Types meeting, small workshops and individual visits. For instance, in 2006, the Types meeting was colocated with TFP 2006 (Trends in Functional Programming). We had joint sessions, keynote speakers and social events.

2 Work-package progress

All deliverables proposed for the second 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 D2: periodic project reports

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

2.2 WP 2: Types 2005 conference

2.2.1 D5: The Nottingham meeting

The Annual Conference of the Types project (`www.cs.nott.ac.uk/types06/`) was held in Nottingham in 2006, organised by Thorsten Altenkirch, James Chapman, Conor McBride, Peter Morris and Wouter Swierstra. With over 100 participants and over 60 talks, including invited talks from Bart Jacobs, Simon Peyton Jones and Hongwei Xi, the meeting was the busiest ever, and an acknowledged success. Also, for the first time, Types was co-located not only with the Symposium on Trends in Functional Programming, but also with the Spring School on Datatype-Generic Programming. This combination of the three meetings was of clear benefit to all. Nottingham was a busy place in April!

2.2.2 D8: Informal Types proceeding

The electronic proceedings are available from the homepage of the meeting and also directly from `www.cs.nott.ac.uk/types06/programme.html`

2.2.3 D11: Refereed Types Proceedings

The Post-Proceedings of the Types 2004 Workshop were edited by Jean-Christophe Filliatre, Christine Paulin, and Benjamin Werner. It is now published as the volume 3839 of the Lecture Notes in Computer Science (LNCS) series. Previous Types post-workshop proceedings include LNCS volumes 3085, 2646, 2277, 1657, 1512, 1158, 996 and 806.

More information about this volume can be found online at the web page `http://www.springeronline.com/3-540-31428-8`.

2.3 WP 3: Thematic workshops

During the reporting period we organized four small workshops.

2.3.1 D14: Small Workshop: MERLIN 2005, MEchanized Reasoning about Languages with varIable biNding

This workshop was hosted by the Tallinn site on 30 September 2005. The program committee included members from the Edinburgh, Udine, INRIA and LMU–Munich sites, and the organising committee included members from the Edinburgh and Udine sites. Two of the eight program committee members were

external to Types, and papers and participation (from Types and external) was solicited by email advertising of the workshop.

There were 30 official registrations. The workshop was composed of one external invited talk, 7 accepted papers (refereed to the standard of an international workshop), and a panel discussion with audience participation. Printed proceedings were distributed at the workshop.

The workshop was attended by 26 people (excluding the local organizers).

Closer information is available at the workshop homepage, `http://merlin.dimi.uniud.it/`.

The subject areas of MERLIN 2005 were:

- Automation of the meta-theory of programming languages and related calculi, particularly work which involves variable binding and fresh name generation.
- Theoretical and practical issues concerning the encoding of variable binding and fresh name generation, especially the representation of, and reasoning about, datatypes defined from binding signatures.

2.3.2 D20: Proceedings for MERLIN 2005

The workshop proceedings were published by ACM Press. The electronic version is included in the ACM Digital Library.

The papers in the proceedings are pre-refereed full papers. They are available from `http://homepages.inf.ed.ac.uk/rap/Types/MERLIN_05/proceedings.html`.

2.3.3 D15: Small Workshop: Constructive analysis, types and exact real numbers

The topics of the workshop were (but not limited to):

- the development of constructive analysis in type theory
- program extraction from such developments
- exact real number computation
- co-inductive methods for continuous structures
- semantics for real computations (e.g. domain theory, formal topology)

The workshop was organized by Herman Geuvers, Bas Spitters, Milad Niqui and Freek Wiedijk. See `http://www.cs.ru.nl/fnds/typesreal/`. There were 34 participants and 14 talks, of which two were by the invited speakers Martin Escardo and Erik Palmgren. The workshop was funded by the Types project and by a grant from NWO (the Dutch association for scientific research).

In connection with the workshop, there was a friendly competition for investigating the state of the art in the various implementations of exact real arithmetic. This competion was organised by Milad Niqui and Freek Wiedijk. Nine teams competed and the competition was won by the mpfr team from LORIA. See `http://www.cs.ru.nl/ milad/manydigits/`.

2.3.4 D21: Proceedings for the workshop on Constructive analysis

The proceedings can be found at `http://www.cs.ru.nl/fnds/typesreal/`. A formal refereed proceedings will appear as a special issue of MSCS (Mathematical Structures in Computer Science), edited by Spitters, Geuvers, Niqui and Wiedijk.

2.3.5 D16: Small Workshop: Second International Workshop on Isomorphisms of Types.

The Toulouse site organized the second international Workshop on Isomorphism of Types (WIT-2005), 28-29 oct. 2005. There were seven presentations during the two days and plenty of informal interaction between the 17 participants.

2.3.6 D22: Proceedings for the workshop on Isomorphisms of Types.

The electronic proceedings are available from `www.irit.fr/zeno/WIT2005/`.

2.3.7 D17: Small workshop: Mathematically Structured Functional Programming, July 2006

This workshop was organized as a satellite event of the 8th International Conference on Mathematics of Program Construction, MPC 2006, held at Kuressaare, Estonia, 3-5 July 2006, hosted by IoC. The workshop took place 2 July 2006. The organizers (PC cochairs) were Conor McBride (Nottingham) and Tarmo Uustalu (IoC).

The motivation for this new workshop was to promote the use of structures originating from mathematics or mathematical semantics in functional programming practice, via language/tool support or by direct expression in programs themselves.

The PC of MSFP 2006 received 16 submissions of which it selected 9 for presentation at the workshop and inclusion in the proceedings. In addition, the programme feature two invited talks, by Andrzej Filinski (University of Copenhagen) and John Power (University of Edinburgh).

The workshop was attended by 30 people.

Closer information is available from the workshop webpage, `http://cs.ioc.ee/mpc-amast06/msfp/`.

2.3.8 D23: Proceedings for the workshop on Mathematically Structured Functional Programming

The proceedings were printed and handed out to the participants. They have been published as a volume of the Electronic Workshops in Computing series of the British Computer Society, `http://ewic.bcs.org/`.

The papers in the proceedings are pre-refereed full papers.

There will also be a special issue of J. of Functional Programming dedicated to the workshop. The papers in the special issue will be significally expanded and revised versions of the proceedings papers.

2.4 WP 5: Visits between sites

We have had at least 81 visits between the sites, these are summarized in the tables on page 10 and 11. The tables do not include visits to workshops organized by Types. The visits marked (*) have been paid by Types.

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

From	To	Who
Sheffield	Bamberg	Mike Stannett
Sheffield	Bamberg	Simon Foster
Nijmegen	Bergen	Barendsen
Swansea	Bergen	Michelbrink
Birmingham	Chalmers	Adedayo Adetoye
Munich LMU	Chalmers	Schwichtenberg
Nijmegen	Chalmers	Spitters
Munich LMU	Chalmers	Abel
Tallinn	Helsinki	T. Uustalu
Toulouse	Helsinki	Soloviev
Nijmegen	Inria-Sophia	Niqui
Inria-Sophia	Inria-Futurs	Bertot
Munich - LMU	Manchester	Schuster
Padua	Manchester	Sambin
Birmingham	Manchester	Vickers
Tallinn	Minho	Uustalu
Toulouse	Munich LMU	Matthes
Edinburgh	Munich	Lucas Dixon *
Inria-Sophia	Nijmegen	Mahboubi
Inria-Sophia	Nijmegen	Bertot
Manchester	Nijmegen	Peter Aczel
Manchester	Nijmegen	Joao Belo *
Munich	Nijmegen	Joao Belo *
Paris VII	Nijmegen	Chantal Berline
Uppsala	Nijmegen	Palmgren
Birmingham	Nijmegen	Martin Escardo
Sheffield	Nottingham	Stannett, Foster, Hughes
Tartu	Nottingham	Varmo Vene
St Andrews	Nottingham	Edwin Brady
Edinburgh	Nottingham	Lucas Dixon
Swansea	Nottingham	Anton Setzer
Swansea	Nottingham	Markus Michelbrink
St Andrews	Nottingham	James McKinna
INRIA Futurs	Novi Sad - Belgrade	H.Herbelin
Torino	Novi Sad	M.Dezani-Ciancaglini
Nijmegen	Orsay	Corbineau
Munich LMU	Oslo	Schwichtenberg
Munich LMU	Oslo	Urban
Birmigham	Padova	E. Ritter

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

1. Milad Niqui visited Inria-Sophia on May 3rd and 4th and gave a talk on "Certified computing with Infinite Objects",
2. Yves Bertot and Assia Mahboubi visited Nijmegen on October 3rd and 4th and Bertot gave a talk on "Real arithmetic in Coq",

Table 3: List of visits between sites, part II:

From	To	Who
Toulouse	Paris 7	Matthes
Nijmegen	Paris 7	Loeb
Torino	Paris 7	Luca Fossati (3 visits)
Bergen	Paris-Sud	Marc Bezem
INRIA Sophia	Paris-Sud	Philippe Audebaud
Nijmegen	Paris-Sud	Pierre Corbineau
Nottingham	Royal Holloway	McBride
Manchester	Royal Holloway	Aczel
Sheffield	Royal Holloway	Stannett, Foster, Hughes
Nottingham	Sheffield	Graham Hutton
Nottingham	Sheffield	Conor McBride
Munich LMU	Stockholm	Schwichtenberg
Helsinki	Stockholm	Negri
Bergen	Swansea	Magne Haveraaen
Bergen	Swansea	Uwe Wolter
Krakow	Swansea	Marek Zaionc
LMU München	Swansea	Jan Johannsen
Manchester	Swansea	Paul Taylor
Nottingham	Swansea	Neil Ghani
Paris Sud	Swansea	Marie Claude Gaudel
Paris 7	Swansea	Thomas Ehrhard
Cracow(site: Warsaw)	Swansea	Marek Zaionc
Udine	Tallinn	M. Miculan *
Nottingham	Tallinn	T. Altenkirch *
Minho	Tallinn	Frade
Royal Holoway	Toulouse	Luo
Inria-Sophia	Toulouse	Bertot
Edinburgh	Udine	A. Momigliano
LMU Munich	Uppsala	Schwichtenberg
LMU Munich	Uppsala	Schuster
Birmingham	Uppsala	Vickers
Chalmers	Uppsala	Coquand
Chalmers	Uppsala	Dybjer
Chalmers	Uppsala	Wahlstedt
TU Munich	Uppsala	Pattinson
Torino	Warsaw	Viviana Bono
Bialystok	Warsaw	Naumowicz *

3. Yves Bertot visited Inria-Futurs on June 12th 2006 and gave a talk on "real numbers as co-inductive streams",

4. Yves Bertot visited Toulouse on June 13th 2006, and give introductory courses.

5. Marc Bezem from Bergen visited Paris-Sud 30 Sept 2005. He gave a talk about " Mechanizing projective geometry using Coherent Logic".

   Coherent logic (CL) is a fragment of FOL extending resolution logic in that it allows certain existential quantifications. CL has a natural proof theory, reasoning in CL is constructive and proof objects can easily be obtained. A substantial number of reasoning problems (e.g., in confluence theory, lattice theory and projective geometry)can be formulated directly in CL without any clausification or Skolemization. This gives some additional benefits in terms of guiding an automated theorem prover, efficiency of the proof search and reusing the proof objects in other logical frameworks. After a short introduction to CL, he discussed a number of examples in projective geometry which have been formalized in Coq.

6. Philippe Audebaud from INRIA Sophia-Antipolis visited Paris-Sud and gave talk about the semantics of the probabilistic language Λ_O.

7. Pierre Corbineau from Radboud university at Nijmegen visited Paris-Sud on 30 June 2006 and gave a talk on a declarative proof language for Coq.

8. Because of geographical proximity, there are strong interactions between the sites Paris-Sud, INRIA Futurs and Université Paris 7. There is a common seminar between Paris-Sud and INRIA Futurs. J-C Filliâtre, J. Signoles and N. Oury gave seminars in Paris 7.

9. Peter Aczel (University of Manchester) gave a talk entitled 'A constructive version of the Lusin Separation Theorem' on Tuesday 14 March in the Brouwer seminar in Nijmegen.

10. Chantal Berline (Université Paris 7) gave a talk entitled 'The Universe of Lambda-theories explored via Lambda-models' on Tuesday 21 March in the Brouwer seminar in Nijmegen.

11. Joao Belo (University of Manchester) gave a talk entitled 'Dependently Sorted Logic' on Tuesday 28 March in the Brouwer seminar in Nijmegen.

12. Peter Aczel (University of Manchester) gave a talk entitled 'Another case study on the FTA' on Tuesday 11 April in the Brouwer seminar in Nijmegen.

13. I. Loeb, Natural Deduction via Graphs Talk given at the Séminaire de l'équipe PREUVES, PROGRAMMES ET SYSTEMES (CNRS-PARIS 7), Paris January 2006.

14. H. Barendregt, Progress in Computer Mathematics, June 12th 2006, The Joint Lab Seminar, Laboratoire de Recherche Commun INRIA-Microsoft.

15. Adam Naumowicz visited Warsaw on March 24, 2006 and presented a talk and a short demo "The Mizar System - Application to Teaching Logic and Set Theory".

16. Conor McBride visited Royal Holloway in July 2006, giving a talk titled "Dependently-typed programming".

17. Conor McBride visited Mike Stannett (Sheffield) in June 2006. He gave a talk on 'Dependent Pattern Matching'.

18. Hugo Herbelin visited Novi Sad and Belgrade in October 2005 and he gave a talk in Belgrade on October 2, 2005, at the Mathematical Institute SANU with the title The duality of computation (`http://www.mi.sanu.ac.yu/seminars/programs/seminar1.oct2005.htm`)

    The lambda-bar-calculus is a variant of lambda-calculus that is derived from Gentzen sequent calculus. Its strong symmetries show that sequent calculus can be computationally interpreted as the superimposition of a call-by-name lambda-calculus and of a call-by-value lambda-calculus. Starting from a comparison with usual lambda-calculus, the talk will cover various computational aspects of the lambda-bar-calculus, plus a tree representation of sequent calculus a la natural deduction.

19. Mariangiola Dezani-Ciancaglini visited Novi Sad in February 2006 and she gave a talk in Novi Sad on February 28, 2006, with the title A Distributed Object-Oriented language with Session Types. Session types are presented in order to specify the sequence and the direction of data exchange for users at different locations interacting by means of object-oriented code.

20. Alberto Momigliano visited Udine in November 2005, and gave a talk titled *A program logic for resources and its application to optimisation validation*, describing a research carried out in Edinburgh by Momigliano and other participants of the project.

21. Eike Ritter visited the site of Padova from the end of August to the beginning of September to work on the models for a double context intuitionistic linear calculus by means of fibrations.

22. Tarmo Uustalu visited Minho in 18–26 January 2006 and gave two talks: “Recursive coalgebras from comonads” and “The essence of dataflow programming”.

23. G. Curi gave a seminar entitled "Effective topology via formal spaces". at the Department of Mathematics of the University of Manchester, June, 7, 2005 (invited by P. Aczel).

24. Marek Zaionc gave an invited lecture “Examples and techniques for asymptotic densities in logic” in the Department of Computer Science, University of Wales in Swansea, UK in July 2006

25. Viviana Bono visited Warsaw in February/March 2006 and gave a talk “Mobile Java”

26. Marino Miculan visited IoC 31 Jan-7 Feb 2006 and gave a talk "Systems biology and brane logics" 2 Feb 2006 and "Behind the name: the many faces of atomic terms" 4 Feb 2006

27. Thorsten Altenkirch visited IoC 12-19 Feb 2006 and gave a talk "Is constructive logic relevant in computer science" 16 Feb 2006 and "Functional quantum programming" 17 Feb 2006

28. Tarmo Uustalu visited Univ. of Helsinki 24 March 2006 and gave a talk "Proof search and countermodel construction for bi-intuitionistic logic" (coauthor Luis Pinto) 24 March 2006.

29. Barendsen was opponent at the PhD graduation of Hoang Anh Truong, 15 May 2006, which includes a short talk. The rest of his visit to Bergen (14–16 May) has been used for scientific collaboration on type systems for resource-bounded component software.

30. Soloviev, Some extensions of reduction systems in lambda-calculus and invertibility of terms, talk given in Helsinki in June 13, 2006.

31. Uwe Wolter (Bergen) visited Swansea 18 - 28 May 2006 and gave a talk "From Universal Algebra to Lawvere Theories" in the "Proof Theory, Complexity and Verification Seminar" and a talk "A Journey from Total to Partial Algebras" in the Departmental Colloquium.

32. Magne Haveraan (Bergen) visited Swansea during the academic year 2004/05 until October 2006. He gave a talk on 4 October 2005 on "Guarded Algebras - handling errors the right way?" in the Departmental Colloquium;

33. Marie Claude Gaudel (Paris-Sud and CNRS, Orsay, France) visited Swansea on Friday 10 March 2006 and gave a talk "Formal Methods and Testing: Hypotheses, and Correctness Approximations" in the Departmental Colloquium.

34. Jan Johannsen (LMU München) visited Swansea 4 -7 April 2006 and gave a talk on "An infinite hierarchy in the linear time mu-calculus".

35. Paul Taylor (Manchester) visited Swansea 26 - 28 March 2006 and gave a talk on "Abstract Stone Duality and Real Analysis"

36. Neil Ghani (Nottingham) visited Swansea 31 October - 2 November 2005 and gave a talk about "Containers 2".

37. Graham Hutton (Nottingham) visited Swansea 18 - 19 October 2005 and gave a talk about "Calculating an Exceptional Machine".

38. Markus Michelbrink: *An Introduction into Dependent Type Theory.* Lecture series (5 sessions) given at the University of Bergen, Winter 2005/2006.

39. Markus Michelbrink: *Types for Object Oriented Programming.* Series of tutorials (4 sessions) given at the University of Bergen, Winter 2005/2006.

40. Adedayo Adetoye visited Chalmers on 10–13 June 2006 and gave a talk entitled "Information Flow Policies for Programs with Implicit Declassification" (joint work with E. Ritter and M.D. Ryan).

41. Conor McBride visited Sheffield in May 2006 and gave two tutorial-style talk on the topic of *Dependent Pattern Matching Evolves* to a combined meeting of the Computer Science department's 'Theory' and 'Verification and Testing' research groups.

42. Mike Stannett, Andrew Hughes and Simon Foster visited Royal Holloway College on 19 July 2006 to attend a Types tutorial workshop.

43. Mike Stannett visited Bamberg from 24–28 July 2006 and gave a talk entitled *Lax Types* (joint work with M. Mendler).

44. Simon Foster visited Bamberg from 24–28 July 2006 and gave a talk entitled *Behavioural Types for Service Composition.*

45. Steve Vickers (Birmingham), Classifying categories, 21 September 2005, Stockholm-Uppsala logic seminar.

46. Helmut Schwichtenberg (LMU Munich), Program Extraction from Normalization Proofs, 1 November 2005, Stockholm-Uppsala logic seminar.

47. Thierry Coquand (Chalmers), Syntax and Semantics of the Logical Framework, 7 December 2005, Stockholm-Uppsala logic seminar.

48. Peter Dybjer (Chalmers), Inductive and Recursive Definitions in Intuitionistic Type Theory. (joint work with Anton Setzer, Swansea). 7 December 2005, Stockholm-Uppsala logic seminar.

49. Helmut Schwichtenberg (LMU Munich), A direct proof of the equivalence between Brouwer's fan theorem and König's lemma with a uniqueness hypothesis, 7 December 2005, Stockholm-Uppsala logic seminar.

50. Helmut Schwichtenberg (LMU Munich), Logic for computable functionals and their approximations, 15 Februari 2006, Stockholm-Uppsala logic seminar.

51. Minisymposium on Concrete Analysis, 2 March 2006, Uppsala, talks by Peter Schuster (LMU Munich) , Dirk Pattinson (TU Munich), Erik Palmgren, Helmut Schwichtenberg (LMU Munich).

52. Peter Schuster (LMU Munich), Power Set, real numbers, partitions, and the axiom of choice. Mathematics Colloquium, 24 March 2006.

53. Sara Negri (Helsinki), Equality in the presence of apartness: a problem of Van Dalen and Statman revisited, 5 april 2006, Stockholm-Uppsala logic seminar.

54. David Wahlstedt (Chalmers), Dependent Type Theory with Parametric First-Order Data Types and Pattern-Matching, 10 May 2006, Stockholm-Uppsala logic seminar.

55. Ralph Matthes visited LMU Munich and gave a talk on 30.03.06 on "Towards verifying terminating programs involving nested datatypes".

56. Ralph Matthes visited Paris 7 and gave a talk on 01.06.06 on "Program verification for nested datatypes in intensional type theory".

2.5 WP 6: The Types web page

2.5.1 D30 The www-site

The web page of the project has been redesigned. The adress is:
`www.cs.chalmers.se/Cs/Research/Logic/Types/`.

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

The new layout has been designed by a professional web-designer. The page was earlier very efficient for people inside the project but is now more easy to overview by outsiders thanks to the new structure. The new design is mainly a change in form; the content is the same.

The page is regularly updated to reflect the activities in the project. New activities are announced before they happen and reported after they happened. We also use the mailing list for these announcements. The mailing list now has more than 250 participants.

3 Consortium management

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

Due to some local adminstrative reason at Inria it has become necessary to let Inria-Futurs be the main Inria site, while Inria-Sophia becomes a subsite. The managerial consequences of this is currently being investigated in Brussels.

There have been no conflicts within the consortium.

4 Scientific collaboration inside the Types project

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

The first example is the collaboration between the Tallinn site and the sites in Udine and Nottingham. In the case of Udine, this was supported by a visit by Miculan to Tallinn in this reporting period (and Uustalo's coming visit to Udine). In the case of Nottingham, this was supported by Uustalo's visit to Nottingham in the previous period 2004/2005, by Altenkirch's visit to Tallinn in this period and by the attendance of the Tallinn group at Nottingham in this period.

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

Paris-Sud promote exchange of students betweeen different sites. P. Corbineau got his PhD in Paris-Sud in September 2005 and started a post-doc position at Rabdoub university in Nijmegen. Nicolas Oury from Paris Sud will defend his PhD in September 2006 and got a Marie-Curie fellowship for a post-doc at university of Nottingham.

Mark Bezem from the Bergen University site and Stefan Berghofer from the TU München site have worked on an interface between Isabelle and an automatic prover for Coherent Logic developed by Mark Bezem and Thierry Coquand. The interface allows proof terms produced by the Coherent Logic prover to be checked inside Isabelle/HOL.

The integration of the proof planning tool *IsaPlanner* into Isabelle by Lucas Dixon from the Edinburgh site is done in close collaboration with Markus Wenzel from the TU München site.

Iris Loeb from Nijmegen payed a 3 month visit to Paris VII, funded by NWO (Dutch association for scientific research).

Soloviev (Toulouse) is collaborating with PPS (Paris 7, Roberto di Cosmo) on Isomorphism of Types. He is also working with Munich on extensions of reduction systems.

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

Zhaohui Luo from the Royal Holloway site and Sergei Soloviev from the Toulouse site have collaborated on coercive subtyping and they have given a joint presentation at the Types small workshop WIT'05 in 2005.

Zhaohui Luo and Robin Adams from the Royal Holloway site and Conor McBride from the Nottingham site have together organised a one-day workshop on Dependent Type Theory in July 2006 at Royal Holloway, Univ of London.

Stefano Berardi and U. Berger started a joint paper about a recursive model of maps recursive in the halting problem, using the notion of learning from S. Hayashi. Starting this model they hope to design better compilers for lambda calculus with continuations.

There was a joint research of H. Herbelin (INRIA, Futurs), S. Ghilezan and S. Likavec (Novi Sad). Böhm's separability property is investigated in different settings of classical lambda calculi. Parigot's $\lambda\mu$-calculus does not satisfy Böhm's separability property, as shown by R. David and W. Py. A. Saurin showed that Ph. de Groote's variant of $\lambda\mu$-calculus enjoys separability.

There was also a joint work of M. Dezani-Ciancaglin (Torino), S. Ghilezan and J. Pantović (Novi Sad). The actual focus of this long-standing ongoing research is the role and importance of type introduction in handling the security levels of dynamic web data.

During the Annual Types 2006 meeting J. Espirito-Santo (Minho), S. Ghilezan and J. Ivetić (Novi Sad) have started foundational research on the introduction of intersection types in sequent systems of lambda calculus.

M.Kolundžija (Novi Sad) took a PhD student position at Torino and Inria Sophia-Antipolis (cotutelle) from Januray 2006

People in Udine and Padova have started several collaborations with other sites:

- collaboration with Eike Ritter (University of Birmingham) about categorical models of linear type systems.
- collaboration with P. Martin-Löf (University of Stockholm)
- collaboration with Steve Vickers (University of Birmingham), about formal topology and the basic picture. Vickers visited Padova in February 2006.
- collaboration with Tarmo Uustalu (Institute of Cibernetics, Tallinn). Miculan visited Tallinn in February 2006; Uustalu is expected to visit Udine in August 2006.
- collaboration with Luigi Liquori (INRIA Sophia-Antipolis).

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

James McKinna [St Andrews] and Joel Wright [Nottingham] have submitted a publication on *A type-correct, stack-safe, provably correct expression compiler in Epigram.*

IoC Tallinn started a collaboration with Udine on a categorical account of variable binding (T. Uustalu, M. Miculan). This is expected to lead to a joint paper soon.

With Nottingham, IoC Tallinn is collaborating on a monadic treatment of partiality from non-termination and on resumption semantics of interactive input-output (T. Uustalu, V. Vene, T. Altenkirch). Also here there are joint papers in progress.

Marc Bezem from Bergen has finished his contribution to Barendregt's book *Typed Lambda Calculus.* The contribution consists of 3 sections in Chapter 5 (*Extensions*) of Part 1 (*Simple Types*), entitled *5.3. Gödel's system T: higher-order primitive recursion*, *5.4. Spector's system B: bar recursion*, *5.5. Platek's system Y: fixed point recursion.*

Marc Bezem and Thierry Coquand (Chalmers) have an ongoing cooperation on Coherent Logic with type-theoretic proof objects. This has resulted a joint publication: *Automating Coherent Logic*, Proceedings LPAR-12, LNCS 3835, pages 246–260, Springer-Verlag, Berlin, 2005.

Marc Bezem and Dimitri Hendriks (Nijmegen, moved recently to Amsterdam) collaborate on the automation of proofs in geometry, based on type theoretic and coherent logic.

Anton Setzer (Swansea) is collaborating with Thierry Coquand, Peter Dybjer (Chalmers) and Erik Palmgren (Uppsala) on writing a book with tentative title "Constructive Logic and Type Theory".

Anton Setzer (Swansea) is collaborating with Peter Dybjer (Chalmers) on further developing the theory of inductive recursive definitions. This includes new extensions of inductive-recursive definitions in order to include definitions which could be as regarded in the spirit of type theory but don't fall under the concept of inductive-recursive definitions. Furthermore they are working on Mahlo inductive recursive definitions with the goal of incorporating Mahlo universes and similar constructions into the concept of inductive-recursive definitions.

Anton Setzer and Markus Michelbrink (Swansea) are collaborating with Neil Ghani, Peter Hancock and Thorsten Altenkirch (Nottingham) on category theoretic characterisations of inductive recursive definitions. One goal is not just to define set indexed families of sets by induction recursion but to place extra mathematical structure on both the inductively defined object U and the codomain of the recursively defined function T.

Anton Setzer and Markus Michelbrink (Swansea) are collaborating with Neil Ghani, Peter Hancock, Thorsten Altenkirch and Connor McBride (Nottingham) on interfaces and containers.

Markus Michelbrink (Swansea) is collaborating with Magne Haveraaen (Bergen) on Types for Object Oriented Programming. One goal of their work is the interference of static and dynamic typing.

Ulrich Berger (Swansea) is collaborating with Thierry Coquand (Chalmers) on domain-theoretic normalisation proofs for lambda-calculi and higher type

term rewriting systems.

Ritter (Birmingham) and Maietti (Padova) are working on a Curry-Howard correspondence for a variant of linear type theory with double contexts, which is used in functional programming to model resource control.

Mike Stannett (Sheffield) and Michael Mendler (Bamberg) have begun collaborating on a new project, to develop a novel theory of "Lax Types", based on the existing theory of Lax Logic.

Helmut Schwichtenberg (LMU Munich) spent a sabbatical term in Uppsala, 20 September 2005 – 20 March 2006.

The Inria–Sophia site have a lot of cooperations with other sites:

- With the Udine site with A. Ciaffaglione and M. Miculan, Luigi Liquori illustrated a methodology for formalizing and reasoning about Abadi and Cardelli's object-based calculi, in (co)inductive type theory, such as the *Calculus of (Co)Inductive Constructions*, by taking advantage of *Natural Deduction Semantics* and *coinduction* in combination with *weak Higher-Order Abstract Syntax* and the *Theory of Contexts*. With F. Honsell and M. Lenisa we introduce a *General Logical Framework*, called GLF, for defining Logical Frameworks, based on dependent types, in the style of the well known Edinburgh Logical Framework LF. The framework GLF features a generalized form of lambda abstraction where β-reductions fire provided the argument satisfies a logical predicate and may produce an n-ary substitution. The type system *keeps* track of when reductions have yet to fire. The framework GLF subsumes, by simple instantiation, LF as well as a large class of generalized constrained-based lambda calculi, ranging from well known restricted lambda calculi, such as Plotkin's call-by-value lambda calculus, to lambda calculi with patterns.

- With the Torino site with S. Ronchi della Rocca, Luigi Liquori presented a fully typed λ-calculus based on the intersection-type system discipline, which is a counterpart à la Church of the type assignment system as invented by Coppo and Dezani. The relationship between this calculus and the intersection type assignment system is the standard isomorphism between typed and type assignment system, and so the typed language inherits from the untyped system all the good properties, like subject reduction and strong normalization. Moreover both type checking and type reconstruction are decidable.

- With the Lyon subsite with D. Dougherty (WPI, USA) and P. Lescanne, Luigi Liquori present a formalism called *Addressed Term Rewriting Systems,* which can be used to model implementations of theorem proving, symbolic computation, and programming languages, especially aspects of sharing, recursive computations and cyclic data structures. Addressed Term Rewriting Systems are therefore well suited for describing object-based languages, and as an example we present a language, incorporating both functional and object-based features.

- With the Loria, Nancy (subsite) with C. Kirchner, H. Cirstea, B. Wack, Luigi Liquori continued the exploration on the new rewriting calculus. A web page describing our complete development can be foiund at `rho.loria.fr`. A number of paper dealing with various type systems has been delivered in

2005-2006, mostly dealing with polymorphic type features, or imperative features of the framework. A running (coq certified) interpreted has been released.

5 Involvement in other EU projects

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

- *MOBIUS, Mobility Ubiquity and Security* (Chalmers, Edinburgh, LMU – Munich, Tallinn, INRIA, Nijmegen, Warsaw) - an integrated project to develop the technology for establishing trust and security for the next generation of global computers, using the Proof Carrying Code paradigm. The Coq type theory proof assistant (from Types partner INRIA) is the main proof system for this project, although Isabelle (from Types partner TUM – Munich) is also being used. This is related to our research area Correctness of Computer Systems.

- *APPSEM* (Chalmers, Edinburgh, Birmingham, Nottingham, LMU – Munich, Minho, Paris 7, 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.

- *ALFA/LerNet* (Chalmers) The group is involved in the ALFA (Latin America Academic Training) network LerNet (Language Engineering and Rigorous Software Development). ALFA is a programme of cooperation between higher education institutions of the European Union and Latin America.

- *EmBounded* (Munich LMU) The aims of the EmBounded Project are to identify, to quantify and to certify resource-bounded code in Hume, a domain-specific high-level programming language for real-time embedded systems. Using formal models of resource consumption as a basis, the project will develop static analyses for time and space consumption and assess these against realistic applications for embedded systems. The work is novel in combining analyses of both source and machine code into a single framework.

- *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.

- *AdHocSys* Wireless Ad-Hoc Broadband Monitoring System, Sixth Framework Programme Priority FP6-2004-IST-4,(`http://www.adhocsys.org`) Software reliability and security software must be able to deal with unexpected situations. The software should continuously analyze node performances, compare them with baselines and send alerts to prevent node

failures or battery outage. The node might be target of attacks from inside and from outside. Software must be robust and should provide a quick and easy way to fix vulnerabilities. The foundational research of this project is related to our research in the domain of type application in security control.

6 Industrial cooperation

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

The 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 TU München site is involved in the project *Verisoft* funded by the German Ministry of Education and Research (BMBF). The main goal of the project is the pervasive formal verification of computer systems (such as those used e.g. in automotive engineering). They are closely cooperating with *OneSpin Solutions* (the former hardware verification division of Infineon), which is one of the industry partners involved in the project. As a part of this cooperation, the Isabelle/Isar proof language has been extended with additional specification methods that allow to formalize large proofs about properties of microprocessors in a modular way.

Chalmers cooperates with Japan's National Institute of Advanced Industrial Science and Technology (AIST) on the development and application of the proof environment Agda. AIST, in turn, is strongly focused on industrial cooperation. The Agda system is the latest of the proof assistants developed in Chalmers inside the Types project.

Several members of INRIA-Futurs and INRIA-Sophia are involved in the INRIA and Microsoft joint lab. There was a Workshop Proofs & Numbers 12-13/06/06 organised in Orsay by INRIA Futurs. It was organised conjointly with the new Microsoft joint-lab in Orsay, so it is an example of a global interaction of Types with industry. The URL with the programme is at `www-sop.inria.fr/marelle/Laurent.Thery/microsoft/Workshop`.

The site in Paris-Sud is collaborating with Dassault Aviation and France Telecom R&D in the area of proofs of C programs. They also have a collaboration with the Axalto company (a smart-cards manufacturer) on proofs of Java and C programs, Java card applets and operating systems. J. Andronick defended her PhD-thesis at Paris Sud in march 2006, the work was done part-time in Axalto. Th. Hubert (Dassault), N. Rousset (Axalto), Y. Moy (France telecom R&D) are studying for their PhD part-time in the industry and part-time in the university.

There was a collaboration between Orsay, Grenoble and the industrial subsite France Telecom R&D in the AVERROES national project (analysis and verification for the reliability of embedded systems) which finished in march 2006 (`http://www-verimag.imag.fr/AVERROES`).

Paris-Sud is participating in the french competitiveness cluster System@tic (see `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.

Thorsten Altenkirch (Nottingham) and Robert Reitmeier (PhD student) collaborate with Simon Peyton Jones (Microsoft Research) on the design of an intermediate language for functional programming with dependent types. The PhD student is supported by Microsoft Research Cambridge.

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

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

Markus Roggenbach and Mr Lim Beng Chuang from Swansea have cooporated with the company C.A.R.U.S (Hamburg, Germany) on systematic testing of the electronic payment standard EP2. Under supervision of Dr Roggenbach, Mr Lim Beng Chuan has developed a prototype for a hardware-in-the-loop testing environment for an EP-2 terminal.

7 Coauthored papers and presentations

Collaborations between researchers in the consortium are taking place in many forms. People are visiting each other, meeting in workshops and exchanging emails. Some of this activity leads to joint publications. Here is a list of some cooperations between people from different groups in the Types project. These papers are also included in section 8, which contains all Types-related publications for each site.

Refereed journal papers

1. Luigi Liquori, Furio Honsell, and Rekha Redamalla. A language for verification and manipulation of web documents. *WWV: Automated Specification and Verification of Web Systems. Electr. Notes Theor. Comput. Sci.*, 157(2):67–78, 2006

2. Michel Cosnard and Luigi Liquori. Virtual organisation in arigatoni: the formal model. *DCM: Development in Computational Models. Electr. Notes Theor. Comput. Sci.*, 2006. To appear

3. Horatiu Cirstea, Kirchner Claude, Luigi Liquori, and Benjamin Wack. Polymorphic type inference for the rewriting calculus. In *JFLA: Journées Francophones des Langages Applicatifs*. INRIA, 2006

4. Luigi Liquori and Simona Ronchi Della Rocca. Intersection typed system *agrave; la* church. *To appear in the Journal of Information and Computation*, 2006

5. Daniel J. Dougherty, Pierre Lescanne, and Luigi Liquori. Addressed term rewriting systems: Application to a typed object calculus. *To appear in the Journal of Mathematical Structures in Computer Science*, 2006

6. Daniel J. Dougherty, Pierre Lescanne, Luigi Liquori, and Frédéric Lang. Addressed term rewriting systems: Syntax, semantics, and pragmatics: Extended abstract. *TERMGRAPH: Term Graph Rewriting. Electr. Notes Theor. Comput. Sci.*, 127(5):57–82, 2005

7. Alberto Ciaffaglione, Luigi Liquori, and Marino Miculan. Reasoning about object-based calculi in (co)inductive type theory and the theory of contexts. *To appear in the Journal of Automated Reasoning*, 2006

8. Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, 82:27–51, 2006. This is the result of a close coperation between Helmut Schwichtenberg at the LMU Munich group and Ulrich Berger (Swansea University), Stefan Berghofer (TU Munich) and Pierre Letouzey (Paris VII). Pierre Letouzey has spent a year as a postdoc in Munich, which led to a rather close cooperation.

9. T. Coquand and B. Spitters, Formal Topology and Constructive Mathematics: the Gelfand and Stone-Yosida Representation Theorems, Journal of Universal computation volume 11, issue 12 2005.

10. T. Coquand and B. Spitters A constructive proof of the Peter-Weyl theorem, Mathematical Logic Quarterly. Vol. 4, 2005, page 351-359.

11. J Pang, P. Calllaghan and Z. Luo. *LFTOP: an LF-based approach to domain-specific reasoning.* Journal of Computer Science and Technology, 20(4), pp 526-535. 2005.

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

13. Alberto Ciaffaglione, Pietro Di Gianantonio "A Certified, Corecursive Implementation of Exact Real Numbers" Theoretical Computer Science 351(1), Special issue on Real Numbers and Computers, 2005

14. G. Battilotti, G. Sambin, Pretopologies and a uniform presentation of suplattices, quantales and frames, in Annals of Pure and Applied Logic, 137, 1-3, pp. 30-61

15. G. Boniolo, S. Valentini, Vagueness, Kant and Topology. to appear in the Journal of Philosophical Logic, 2006.

16. G. Curi, "On the collection of points of a formal space". Ann. Pure Appl. Logic 137, 1-3, 2006, pp. 126-146.

17. M.E. Maietti, Modular correspondence between dependent type theories and categorical universes, including pretopoi and topoi, Mathematical Structures in Computer Science, 15(6):1089–1149, 2005

18. G.Sambin and G.Trentinaglia. On the meaning of positivity relations for formal spaces. to appear in Constructivity, computability and logic. A collection of papers in honour of the 60th birthday of Douglas Bridges, C.S.Claude, H.Ishihara eds., 2006

19. S. Valentini, The problem of the formalization of constructive topology. Archive for Mathematical Logic, vol. 44 (1),(2005), pp. 115-129

20. S. Valentini, Every countably presented formal topology is spatial, classically. To appear in the Journal of Symbolic Logic, 2006.

21. [BHHMS06] Anna Bucalo, Martin Hofmann, Furio Honsell, Marino Miculan, Ivan Scagnetto. Consistency of the Theory of Contexts. Journal of Functional Programming, Volume 16, Issue 03, May 2006, pp 327-395

22. Peter Dybjer and Anton Setzer. Indexed induction-recursion. *Journal of Logic and Algebraic Programming*, 66:1 – 49, 2006

23. Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program extraction from normalization proofs. *Studia Logica*, 82:25–49, 2006

24. E. Palmgren and P. Schuster. Apartness and formal topology. *New Zealand Journal of Mathematics,* 34(2005), 1-8.

25. Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren, Peter Schuster) Binary refinement implies discrete exponentiation. *Studia Logica*

26. F. Barral, D. Chemouil, S. Soloviev. Non-standard reductions and categorical models in typed lambda-calculus. (Anglais.) - Logitcheskie Issledovaniya (Studies in Logics), 13, Moscow, "Nauka", december 2005, pp.300-315.

Refereed conference papers

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

2. Th. Coquand A. Abel and U. Norell. Connecting a logical framework to a first-order logic prover. In B. Gramlich, editor, *Proceedings of 5th International Workshop on Frontiers of Combining Systems, Lecture Notes in Artificial Intelligence*, volume 3717, pages 285–301. Springer-Verlag, September 2005

3. C. Coquand, D. Synek, and M. Takeyama. An Emacs-Interface for Type-Directed Support for Constructing Proofs and Programs. In *Proceedings of User Interfaces for Theorem Provers, UITP 2005, Edinburgh, Scotland*. To be published in ENTCS, Elsevier, 2006

4. T. Coquand and A. Spiwack. Proof of strong normalisation using domain theory. In *Proceedings of LICS 2006*, 2006

5. Fredrik Lindblad and Marcin Benke. A tool for automated theorem proving in agda. In *TYPES 2004*, volume 3839 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2006

6. Benjamin Grégoire, Laurent Théry, and Benjamin Werner. A computational approach to pocklington certificates in type theory. In Masimi Hagiya and Philip Wadler, editors, *Proceedings of Functional and Logic Programming Symposium (FLOPS'06)*, volume 3945 of *Lecture Notes in Computer Science*, pages 97 – 113. Springer-Verlag, 2006

7. Benjamin Grégoire and Laurent Théry. A purely functional library for modular arithmetic and its application to certifying large prime numbers. In Furbach and Shankar [48], pages 423–437

8. Raphael Chand, Michel Cosnard, and Luigi Liquori. Resource discovery in the arigatoni model. In *I2CS: International Workshop on Innovative Internet Community Systems*, volume LNCS. Springer, 2006. To appear. Also available as RR INRIA

9. Didier Benza, Michel Cosnard, Luigi Liquori, and Marc Vesin. Arigatoni: Overlaying internet via low level network protocol. In *JVA: John Vincent Atanasoff International Symposium Modern Computing*. IEEE Press, 2006. To appear. Also available as RR INRIA

10. Philippe Audebaud and Christine Paulin-Mohring. Proofs of randomized algorithms in coq. In Tarmo Uustalu, editor, *Mathematics of Program Construction, MPC 2006*, volume 4014 of *Lecture Notes in Computer Science*, Kuressaare, Estonia, July 2006. Springer-Verlag

11. Andreas Abel, Marcin Benke, Ana Bove, John Hughes, and Ulf Norell. Verifying Haskell programs using constructive type theory. In *ACM SIGPLAN 2005 Haskell Workshop, Haskell'05, Tallinn, Estonia, September 30, 2005*, pages 62–73. ACM Press, 2005.

12. 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*, volume 3717 of *Lecture Notes in Artificial Intelligence*, pages 285–301. Springer-Verlag, September 2005.

13. S. Berghofer and C. Urban. A Head-to-Head Comparison of de Bruijn Indices and Names. In *Proc. of the International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP*, ENTCS, pages 53–67, 2006.

14. Donald Sannella, Martin Hofmann, David Aspinall, Stephen Gilmore, Ian Stark, Lennart Beringer, Hans-Wolfgang Loidl, Kenneth MacKenzie, Alberto Momigliano, and Olha Shkaravska. Mobile Resource Guarantees. In *Trends in Functional Programing*, volume 6, Tallinn, Estonia, Sep 23–24, 2005. Intellect.

15. C. Urban and S. Berghofer. A Recursion Combinator for Nominal Datatypes Implemented in Isabelle/HOL. In *Proc. of the 3rd International Joint Conference on Automated Reasoning (IJCAR)*, volume 4130 of *LNAI*, pages 498–512, 2006.

16. A. Asperti, H. Geuvers, I. Loeb, L. Mamane and C. Sacerdoti Coen An Interactive Algebra Course with Formalised Proofs and Definitions to appear in the Proceedings of the Fourth Conference Mathematical Knowledge Management, MKM 2005 (Bremen, July 2005), Springer LNCS.

17. Conor McBride, Healfdene Goguen, and James McKinna. A few constructions on constructors. In *Post Conference Proceedings, 2004 TYPES Workshop*, volume 3839 of *LNCS*, pages 252–267. Springer Verlag, 2006

18. [Mai05] M.E. Maietti. Predicative exponentiation of locally compact formal topologies over inductively generated ones. In L. Crosilla and P. Schuster, editor, From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics, number 48 in Oxford Logic Guides, pages 202–222, Oxford University Press, 2005.

19. [MS05] M.E. Maietti, G. Sambin, Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editor, From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics, number 48 in Oxford Logic Guides, pages 91–114. Oxford University Press, 2005.

20. [CHR05] Alberto Ciaffaglione, Matthew Hennessy, Julian Rathke "Proof Methodologies for Behavioural Equivalence in Distributed pi-calculus" Best Paper Award. In Proceedings of FORTE, Taipei (Taiwan) Lecture Notes in Computer Science 3731, 2005

21. [HLR06] F. Honsell, M. Lenisa, R. Redamalla: "Coalgebraic Description of Generalized Binary Methods", *Developments in Computational Models (DCM'05)* Workshop Proceedings, M. Fernandez et al eds., ENTCS **135**(3), 2006 , 73–84.

22. [CHL06] D. Cancila, F. Honsell, M. Lenisa: "Functors Determined by Values on Objects", *MFPS XXII* Conference Proceedings, S. Brookes and M. Mislove ed., ENTCS **158**, 2006, 151–169.

23. [CHL06a] D. Cancila, F. Honsell, M. Lenisa: "Some Properties and Some Problems on Set Functors", *Coalgebraic Methods in Computer Science (CMCS'06)* Workshop Proceedings, ENTCS (to appear).

24. [MSH06] M. Miculan, I. Scagnetto, F. Honsell: "Translating Specifications from Nominal Logic to CIC with the Theory of Contexts". In R. Pollack, editor, Proceedings of MERLIN'05. ACM DL, 2005.

25. J. Chrząszcz and J.-P. Jouannaud. From OBJ to ML to Coq. In *Goguen Festschrift*, volume 4060 of *LNCS*. Springer, 2006

26. J. Chrząszcz, A. Gąsienica Samek, A. Schubert, and T. Stachowicz. Minik: A Tool for Maintaining Proper Java Code Structure. In *Software Engineering Techniques 2006*, LNCS, Warsaw, 2006. Springer

27. M. Cielecki, J. Fulara, K. Jakubczyk, Ł. Jancewicz, J. Chrząszcz, A. Schubert, and Ł. Kamiński. Propagation of JML non-null annotations in Java programs. In *International Conference on Principles and Practices of Programming in Java*, Mannheim, 2006. ACM Press

28. A. Gąsienica-Samek, T. Stachowicz, J. Chrząszcz, and A. Schubert. KOTEK: Clustering of The Enterprise Code. In *Software Engineering: Evolution and Emerging Technologies*, volume 130. IOS Press, 2005

Talks

- Z. Luo and S. Soloviev. Coercive subtyping: PAL$^+$ and beyond. WIT'05, Toulouse, Oct. 2005.
- Healfdene Goguen, Conor McBride, and James McKinna. Eliminating dependent pattern matching. In *Algebra, Meaning and Computation, a Festschrift for Joseph Goguen*, volume 4060 of *LNCS*. Springer Verlag, 2006
- Miki Tanaka and John Power. A unified category-theoretic formulation of typed binding signatures. In *Proceedings of the 3rd workshop on MEchanized Reasoning about Languages with variable bINding, MERLIN'05*, September 2005
- Ornaghi, Fiorentini, and Momigliano. Snapshots generation via constructive logic. In *MoVeLog'05*, October 2005
- Neil Ghani, Makoto Hamana, Tarmo Uustalu, Varmo Vene, *Representing Cyclic Structures as Nested Types* in Proceedings of TFP 2006.

- Healfdene Goguen, Conor McBride and James McKinna, *Eliminating Dependent Pattern Matching*, in "Goguen Festschrift", K. Futasugi et al. (Eds.), LNCS 4060, Springer-Verlag. 2006.
- F. Barral, S. Soloviev. Inductive Type Schemas as Functors.- Proceedings of the International Computer Science Symposium in Russia CSR 2006, June 8-12, St.Petersburg, Russia. LNCS, 3967, pp.35-45.

8 Major scientific results

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

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

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

8.1 Chalmers

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 Haskell Workshop'05, Tallin, September 2005

Nils Anders Danielsson, Jeremy Gibbons, John Hughes and Patrik Jansson proved that "Fast and Loose Reasoning is Morally Correct", relating the semantics of total and partial functional languages. The resulting paper was presented at POPL 2006.

Foundational Research Carlos Gonzalía defended his PhD thesis in March 2006. The thesis investigates how to express and reason about relational concepts and methods inside the constructive logical framework of Martin-Löf's monomorphic type theory.

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.

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.

The cooperation with Japan's National Institute of Advanced Industrial Science and Technology (AIST) on the development and application of the proof environment Agda continues. An Agda Implementor's Meeting was held in May, 2006, in Osaka, Japan.

Publications

Refereed conference papers

- A. Abel, M. Benke, A. Bove, J. Hughes, and U. Norell. Verifying Haskell programs using constructive type theory. In *Haskell Workshop*. ACM, September 2005
- Th. Coquand A. Abel and U. Norell. Connecting a logical framework to a first-order logic prover. In B. Gramlich, editor, *Proceedings of 5th International Workshop on Frontiers of Combining Systems, Lecture Notes in Artificial Intelligence*, volume 3717, pages 285–301. Springer-Verlag, September 2005
- C. Coquand, D. Synek, and M. Takeyama. An Emacs-Interface for Type-Directed Support for Constructing Proofs and Programs. In *Proceedings of User Interfaces for Theorem Provers, UITP 2005, Edinburgh, Scotland*. To be published in ENTCS, Elsevier, 2006
- T. Coquand and A. Spiwack. Proof of strong normalisation using domain theory. In *Proceedings of LICS 2006*, 2006
- Fredrik Lindblad and Marcin Benke. A tool for automated theorem proving in agda. In *TYPES 2004*, volume 3839 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2006

- Nils Anders Danielsson, John Hughes, Patrik Jansson, and Jeremy Gibbons. Fast and loose reasoning is morally correct. In *POPL '06: Conference record of the 33rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 206–217, New York, NY, USA, 2006. ACM Press

Talks

- Patrik Jansson. Covertranslator—from haskell to first order logic. Talk given at the TYPES 2006 conference in Nottingham, April 2006
- Bengt Nordström: *Interaction with a (Proof) editor, what but not how.*, JAIST-AIST Workshop on Verification Technology, Senri, Japan, May 2006.

Dissertations

- Carlos Gonzalia. *Relations in Dependent Type Theory.* PhD thesis, Chalmers University of Technology, 2006

8.2 Paris 7

Foundational Research J.-L. Krivine continued his work on programs associated to proofs of mathematical theorems. Concerning axioms, he obtained programs associated to the complete axiom of choice and the continuum hypothesis using read-write instructions on a global variable. He also showed that one can associate a program to each true π^1_1-formula and established in this way a connection between realizability theory and game semantic. He gave a series of lectures on these results at Geocal'06 (see www.pps.jussieu.fr/ krivine/articles/Geocal06.pdf)

M. Parigot worked on the design a classical framework allowing to express constructivity in an internal manner.

S. Lengrand together with R. Dyckhoff and J. McKinna developed a sequent calculus version of Pure Type Systems (PTS), which they showed to be equivalent both from the viewpoints of the derivable sequents and the normalisation procedures. He introduced with A. Miquel a classical version of F_ω and proved its strong normalisation property. He also studied, together with Roy Dyckhoff and Delia Kesner, various term-reduction systems for the depth-bounded intuitionistic sequent calculus of Hudelmaier and showed that they are strongly normalising.

Delia Kesner together with C. Barry Jay developed a pure pattern calculus which generalizes the pure lambda-calculus by basing computation on pattern-matching instead of beta-reduction. As well as supporting a uniform approach to functions, it supports a uniform approach to data structures which underpins two new forms of polymorphism.

Chantal Berline together Antonino Salibra et Giulio Manzonetto worked on the question whether there exists, inside the known semantics, a model of lambda-calculus whose equational theory is recursively enumerable. They gave a negative answer for the stable semantics of Berry and Girard and the strongly

stable semantics of Ehrard. They also gave a partial negative result for Scott continuous semantics.

V. Mogbil together with C. Fouqueré, generalized the ressource sensitive logic programming based on proof nets introduced by J.-M. Andreoli. They showed in particular how the expressive power of exponential linear logic can be used for extending logic programming and dealing with concurrency.

Proof technology Pierre Letouzey has worked on improving the content of the Standard Library of the Coq proof assistant. In particular, he has added to this library several implementations of finite sets and maps a la Ocaml. These certified implementations allow to perform both efficient computation and mathematical reasoning on such sets and maps.

Publications

Refereed journal papers

- Patrick Baillot, Ugo Dal Lago. *On Light Logics, Uniform Encodings and Polynomial Time*. To appear in Mathematical Structures in Computer Science, 2006.
- Chantal Berline, A. Salibra. *Easiness in graph models*, Theor. Comput. Science 354 (2006) 4-23.
- Chantal Berline. *Graph models of lambda-calculus at work, and variations*, Math. Struct. for Comput. Sci. (2006), vol.16, pp. 185-221.
- Delia Kesner, Stephane Lengrand. *Explicit operators for lambda-calculus*. In Juergen Giesl, editor, Information and Computation. Elsevier Publisher (to appear)

Refereed conference papers

- Vincent Atassi , Patrick Baillot, Kazushige Terui. *Verification of Ptime reducibility for system F terms via Dual Light Affine Logic*. To appear in the Proceedings of Computer Science Logic 2006 (CSL'06), LNCS, Springer, 2006.
- C. Barry Jay, Delia Kesner. *Pure Pattern Calculus*. In Proceedings of the European Symposium on Programming (ESOP), LNCS 3924, pages 100-114, Vienna, Austria, 2006.
- Roy Dyckhoff, Delia Kesner, Stephane Lengrand. *Strong cut-elimination systems for Hudelmaier's depth-bounded sequent calculus for implicational logic*. In Proceedings of the 3rd International Joint Conference on Automated Reasoning, LNCS, Seattle, USA, 2006.
- Roy Dyckhoff, Stephane Lengrand. *LJQ, a strongly Focused Calculus for Intuitionistic Logic*. In A. Beckmann, U. Berger, B. LÃűwe, and J. V Tucker, editors, Proceedings of the 2nd Conference on Computability in Europe (CiE'06), volume 3988 of LNCS, pages 173-185. Springer-Verlag, Swansea, UK, July 2006.

- Roy Dyckhoff, Stephane Lengrand, James McKinna. *A Sequent Calculus for Type Theory.* Proceedings of the 15th Conference on Computer Science Logic (CSL'06), volume 4207 of LNCS, pages 441-455. Szeged, Hungary, September 2006.

- C. Raffalli, Paul RoziÃÍre. *PhoX*, The seventeen provers of the World, Freek Wiedijk (editor), LNAI 3600 pages 67-71.

8.3 INRIA- Futurs

Correctness of Computer Systems The work on the Coq proof-assistant is ongoing. The beta-version of V8.1 is now available. It includes compilation of checked code towards state-of-the-art byte-code for fast conversion check.

Foundational Research Gilles Dowek obtained new results on typed lambda-calculus.

Dale Miller pursued his reasearch on the representation of judgements.

Jean-Pierre Jouannaud obtained several theoretical results on rewriting.

Benjamin Werner proposed a proof-irrelevant version of type theories.

Formal Mathematics and Mathematics Education Coq is teached, among others, at Ecole Normale Supérieure de Lyon and MPRI master's course.

We have a strong connection with André Hirschowitz' team of algebraic geometry centered on the use of Coq.

Roland Zumkeller is working on the formal checking of the numerical part of Hales' proof of Kepler's conjecture and has made crucial progress this year.

Benjamin Werner worked with Benjamin Grégoire and Laurent Théry (Sophia) on formal primality proofs.

Proof technology Many of the results above have been made possible by making Coq's conversion test faster and thus use the so called "formal proofs by computation" technology.

Dale Miller had several results on proof-search.

Publications

Refereed journal papers

- G. Dowek, , and Y. Jiang. Eigenvariables, bracketing and the decidability of positive minimal predicate logic. *TCS*, 2006. To appear

- L. Strassburger and F. Lamarche. From proof nets to the free *-autonomous category. *Logical Methods in Computer Science*, 2006. To appear

- Y. Bertot. Affine functions and series with co-inductive real numbers. *Mathematical Structures in Computer Science.* Accepted july 2006

- Horatiu Cirstea, Germain Faure, Maribel Fernández, Ian Mackie, and François-Régis Sinot. New evaluation strategies for functional languages. *Electronic Notes in Theoretical Computer Science*, 2006. to appear

- François-Régis Sinot. Call-by-need in token-passing nets. *Mathematical Structures in Computer Science*, 16(4), 2006

- 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

- François-Régis Sinot. Token-passing nets: Call-by-need for free. *Electronic Notes in Theoretical Computer Science*, 135(3):129–139, March 2006

Refereed conference papers

- Roland Zumkeller. Formal global optimisation with taylor models. In U. Furbach and N. Shankar, editors, *Int. Joint Conf. Automated Reasoning — IJCAR 2006*, volume ? of *Lecture Notes in Computer Science*, pages ?–? Springer-Verlag

- Assia Mahboubi. Proving formally the implementation of an efficient gcd algorithm for polynomials. In U. Furbach and N. Shankar, editors, *Int. Joint Conf. Automated Reasoning — IJCAR 2006*, volume ? of *Lecture Notes in Computer Science*, pages ?–? Springer-Verlag

- Benjamin Werner. On the strength of proof-irrelevant type theories. In U. Furbach and N. Shankar, editors, *Int. Joint Conf. Automated Reasoning — IJCAR 2006*, volume ? of *Lecture Notes in Computer Science*, pages ?–? Springer-Verlag

- Laurent Thery Benjamin Grégoire and Benjamin Werner. A computational approach to pocklington certificates in type theory. In M. Hagiya and P. Wadler, editors, *FLOPS 2006*, volume 3945 of *Lecture Notes in Computer Science*. Springer-Verlag, 2006

- Benjamin Grégoire and Laurent Théry. A purely functional library for modular arithmetic and its application to certifying large prime numbers. In U. Furbach and N. Shankar, editors, *Int. Joint Conf. Automated Reasoning — IJCAR 2006*, volume ? of *Lecture Notes in Computer Science*, pages ?–? Springer-Verlag

- Yves Bertot. Calcul de formules affines et de séries entières en arithmétique exacte avec types co-inductifs. In *Journées Francophones des Langages Applicatifs*, 2006

- Dale Miller. Collection analysis for Horn clause programs. In *Proceedings of PPDP 2006: 8th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming*, July 2006

- Dale Miller. Representing and reasoning with operational semantics. In U. Furbach and N. Shankar, editors, *Proceedings of IJCAR: International Joint Conference on Automated Reasoning*, August 2006

- Dale Miller. Logic and logic programming: A personal account. ALP Newsletter, February 2006. Vol. 19, No. 1

- Dale Miller and Alwen Tiu. A proof theory for generic judgments. *TOCL*, 6(4):749–783, October 2005
- Dale Miller and Alexis Saurin. A game semantics for proof search: Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS)*, 2005
- Alwen Tiu, Gopalan Nadathur, and Dale Miller. Mixing finite success and finite failure in an automated prover. In *Proceedings of ESHOL'05: Empirically Successful Automated Reasoning in Higher-Order Logics*, pages 79 – 98, December 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*, number 3835 in LNAI, pages 352–366, 2005

Dissertations

- H. Herbelin. Habilitation: *C'est maintenant qu'on calcule, au c¡ur de la dualité*. Defended in Orsay in december 2005.
- O. Hermant. PhD: *Méthodes sémantiques en Déduction Modulo*. Director: G. Dowek. Defended at Ecole polytechnique in december 2005.

8.4 INRIA-Sophia

Correctness of Computer Systems Yves Bertot and Laurence Rideau are participating in a French nationally funded effort to prove the correctness of a lightly optimized compiler from a significant subset of C to a mainstream micro-processor.

Formal Mathematics and Mathematics education Yves Bertot, Laurence Rideau, and Laurent Théry are engaging in a study of finite groups that should lead to the verification of major theorems for the classification of finite groups.

Benjamin Grégoire and Laurent Théry studied the feasability of high-speed arithmetic computation as part of reflexive computation inside theorem provers. They applied this to the formal proof of primality for large Mersenne numbers, now reaching the 27th number, with 13000 digits.

Yves Bertot and Nicolas Julien studied the feasability of high-precision computation for real-numbers inside theorem provers. This work should lead to the implementation of a library for general purpose mathematical computation.

Foundational Research Yves Bertot studied the proof techniques for basic domain theory inside a type-theory based theorem prover. In particular, he selected the axioms that are required to perform classical reasoning and make it possible to formalize the semantics of simple programming languages. This should also provide new ways to model recursive functions while avoiding the burden of proving the termination of all functions.

Formal Mathematics and Mathematics Education Loïc Pottier collaborated with the Mathematical departement of Nice to design a user-friendly language to describe mathematical statements and support collections of exercises used in introductory courses in mathematics.

Proof technology Yves Bertot and Julien Forest collaborated to add a command Function to the Coq system that provides a collection of theorems adapted to each new function definition (fix-point equation, induction principles, etc.).

Laurent Théry contributed to the chapter on Coq in the book The seventeen provers of the world, edited by F. Wiedijk.

Publications

Refereed journal papers

- Luigi Liquori and Benjamin Wack. The polymorphic rewriting-calculus: [type checking vs. type inference]. *WRLA: Rewriting Logic and its Applications. Electr. Notes Theor. Comput. Sci.*, 117:89–111, 2005
- Assia Mahboubi. Implementing the cylindrical algebraic decomposition inside the coq system. *Mathematical Structures in Computer Science*, 2006. submitted 12/2005, accepted for publication 07/2006
- Yves Bertot. Affine functions and series with co-inductive real numbers. *Mathematical Structures in Computer Science*, 2006. submitted 12/2005, accepted for publication 07/2006
- Luigi Liquori. irho: the software: [system description]. *DCM: Development in computational Models. Electr. Notes Theor. Comput. Sci.*, 135(3):85–94, 2005

Refereed conference papers

- Assia Mahboubi. Proving formally the implementation of an efficient gcd algorithm for polynomials. In Furbach and Shankar [48]
- Yves Bertot. Calcul de formules affines et de séries entières en arithm étique exacte avec types co-inductifs. In *Journées Francophones des Langages Applicatifs*. INRIA, January 2006

Talks

- Yves Bertot, "co-inductive types and exact real computation", University of Strasbourg, January 2006.

8.5 Paris Sud – Grenoble – France Telecom R&D

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" (see `http://why.lri.fr`) 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 (`http://krakatoa.lri.fr`) 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. This tool has been adapted by C. Marché and N. Rousset in order to handle JavaCard transaction mechanism.

J.-C. Filliâtre and C. Marché designed a similar tool called Caduceus for dealing with C programs. This tool is used by the France Telecom R&D subsite in order to analyse use of memory. Y. Moy supervised by P. Crégut and C. Marché is designing a method to automatically generate specifications (loop invariant, precondition) corresponding to an appropriate use of pointers.

J. Andronick worked in the Axalto company on an adaptation of the Caduceus tool in order to specify and prove embedded source code on smart cards, possibly using union types and casts between structures and arrays.

Reasoning on functional programs J. Signoles supervised by J-C. Filliâtre proposed an extension of mini-ML with types seen as ordinary expressions and expressions interpreted as specifications. Using a single extra construction (demonic application), he is able to express powerful specifications and a refinement relation in order to develop correct programs.

M. Sozeau supervised by C. Paulin, designed a language with a subset type (in the spirit of the PVS language) which is convenient for programming with (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. He developed a formal proof of correctness of the translation and designed a prototype implementation available in CoqV8.1.

Reasoning on randomized programs C. Paulin together with Ph. Audebaud (from INRIA Sophia-Antipolis) proposed a method for representing randomized algorithms in Coq using a monadic interpretation translating randomized expressions into distributions. A library has been designed in Coq for representing the interval $[0, 1]$, probabilistic distributions and randomized algorithms.

Applications of proof assistant to security Coq was used in the framework of security for bank applications. The API of IBM's Common Cryptographic Architecture used in most ATMs, was known to be flawed: secrets can

be disclosed using regular function calls and properties of the bitwise exclusive or operator. Courant and Monin showed that this cannot happen in a suitable modification of the API. The proof was designed in Coq: the proof tool played an essential role in the discover of the right invariants.

Floating-point arithmetic Numeric computations use floating-point numbers to approximate exact arithmetic. Unfortunately, this use can falsify a program correct on real numbers. The use of a proof assistant is especially useful as some computations, like polynomial evaluation, are commonplace and as floating-point arithmetic may have unexpected behaviors.

Foundational Research

In the course of the proof of the security API, a new methodology was experimented for expressing a non-trivial function, namely the normalization of terms quotiented by the algebraic properties of xor. This methodology is based on a stacking of dependent types, instead of general results on AC-rewriting relations.

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

S. Conchon designed an automatic proof procedure for first-order logic with equality and arithmetic in order to solve proof obligations generated by checking correctness of programs. His implementation is functional with the goal to integrate it in proof assistants using certification or trace generation.

S. Lescuyer supervised by E. Contejean and S. Conchon designed a method for translating a problem defined in a multi-sorted polymorphic theory into a formula adapted to automatic provers based on mono-sorted logic.

E. Contejean continue her long-term project of cross-fertilizing rewriting techniques and type theory. She is designing a large Coq library (described at `http://www.lri.fr/~contejea/COQ/doc/`) on rewriting, using an efficient representation of terms, similar to the one used in rewriting tools like CiMe. She developed a proof of termination for the RPO order and is currently working on unification.

Pattern matching with dependent types N. Oury supervised by C. Paulin designed a method for analysing pattern-matching completeness with dependent types using techniques derived from abstract interpretation.

Formal Mathematics and Mathematics Education

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

Proof technology

Hermes `http://www-verimag.imag.fr/~Liana.Bozga/home/hermes.html`, is a tool dedicated to the automatic verification of secrecy properties in cryptographic protocols, has been connected to Coq in order to certify the positive results it may produce as output. Basically, Hermes computes a fixed point in an abstract representation of an infinite state system, while providing a Coq proof script which is is verified off-line by Coq.

We collaborated with the LogiCal team (INRIA Futurs) by extending the parameter condition of inductive definitions in the new version V8.1 of the Coq Proof Assistant.

Publications

Refereed journal papers

- Salvador Lucas, Claude Marché, and José Meseguer. Operational termination of conditional term rewriting systems. *Information Processing Letters*, 95:446–453, 2005

- Jean-François Monin and Philippe Chavin. Coq. In H. Habrias and M. Frappier, editors, *Software Specification Methods, An Overview Using a Case Study*, ISTE, chapter 16. Hermès Science, April 2006

Refereed conference papers

- Philippe Audebaud and Christine Paulin-Mohring. Proofs of randomized algorithms in coq. In Tarmo Uustalu, editor, *Mathematics of Program Construction, MPC 2006*, volume 4014 of *Lecture Notes in Computer Science*, Kuressaare, Estonia, July 2006. Springer-Verlag

- Sylvie Boldo. Pitfalls of a full floating-point proof: example on the formal proof of the veltkamp/dekker algorithms. In *Proceedings of the third International Joint Conference on Automated Reasoning (IJCAR)*, Seattle, USA, August 2006

- Sylvie Boldo and César Muñoz. Provably faithful evaluation of polynomials. In *Proceedings of the 21st Annual ACM Symposium on Applied Computing*, volume 2, pages 1328–1332, Dijon, France, April 2006

- Sylvain Conchon and Jean-Christophe Filliâtre. Type-Safe Modular Hash-Consing. In *ACM SIGPLAN Workshop on ML*, Portland, Oregon, September 2006

- Judicaël Courant and Jean-François Monin. Defending the bank with a proof assistant. In *6th International Workshop on Issues in the Theory of Security (WITS '06)*, Vienna, March 2006

- Judicaël Courant and Jean-François Monin. Faire garder la banque par un Coq. In *Actes des dix-septièmes journées francophones des langages applicatifs*, pages 25 – 39, January 2006

- Jean-Christophe Filliâtre. Backtracking iterators. In *ACM SIGPLAN Workshop on ML*, Portland, Oregon, September 2006
- Romain Janvier, Yassine Lakhnech, and Michaël Périn. Certification of Cryptographic Protocols by Abstract Model-Checking and Proof Concretization. In *ITCES'2006*, San Jose, April 2006
- Claude Marché and Christine Paulin-Mohring. Reasoning about Java programs with aliasing and frame conditions. In J. Hurd and T. Melham, editors, *18th International Conference on Theorem Proving in Higher Order Logics*, Lecture Notes in Computer Science. Springer-Verlag, August 2005
- Claude Marché and Nicolas Rousset. Verification of Java Card applets behavior with respect to transactions and card tears. In *4th IEEE International Conference on Software Engineering and Formal Methods (SEFM'06)*, Pune, India, September 2006
- Jean-François Monin and Judicaël Courant. Proving termination using dependent types: the case of xor-terms. In *Trends in Functional Programming 2006*, Nottingham, April 2006
- Nicolas Oury. Extensionality in the Calculus of Constructions. In J. Hurd and T. Melham, editors, *18th International Conference on Theorem Proving in Higher Order Logics*, Lecture Notes in Computer Science. Springer-Verlag, August 2005

Talks

- Sylvie Boldo. Veltkamp & Dekker revisited. TYPES Workshop on Numbers and Proofs, June 2006
- Nicolas Oury. Pattern matching coverage using approximations. TYPES 2006, long talk, April 2006
- Matthieu Sozeau. Subset coercions in Coq. TYPES 2006, long talk, April 2006
- Christine Paulin-Mohring. A library for reasoning on randomized algorithms in Coq. Description of a Coq contribution, Université Paris Sud, January 2006. AVERROES project

Dissertations

- June Andronick. *Modélisation et vérification formelles de systèmes embarqués dans les cartes à microprocessur. Plateforme Java Card et Système d'exploitation.* Thèse de doctorat, Université Paris-Sud, March 2006
- Pierre Corbineau. *Démonstration Automatique en Théorie des Types.* Thèse de doctorat, Université Paris-Sud, September 2005
- Claude Marché. *Preuves mécanisées de Propriétés de Programmes.* Thèse d'habilitation, Université Paris 11, December 2005
- Julien Signoles. *Extension de ML avec raffinement: syntaxe, semantiques et système de types.* Thèse de doctorat, Université Paris-Sud, July 2006

8.6 Munich – LMU

Correctness of Computer Systems Abel has completed a PhD thesis on sized types in a polymorphic functional programming language with higher-order functions. His method can be used to verify termination of computer programs, especially in theorem provers where termination is essential for the correctness of proofs.

Hofmann and Loidl studied foundations for producing resource bounds for the embedded systems language Hume, in collaboration with project *EmBounded* (IST-510255). They started a formalisation of the Hume Abstract Machine (HAM) in the Isabelle/HOL theorem prover, and developed a cost model for the HAM. In joint work with the EmBounded group at St Andrews a cost model for Hume was developed, and cost correspondence between the high- and low-level languages was verified. Loidl continued the development of mHaskell, a mobile variant of the functional programming language Haskell (with Heriot-Watt University, Edinburgh), an of Grid/GUM, a parallel Haskell that can be executed on the Grid.

Hofmann has developed a translation of typing derivations into proofs in Hoare Logic. A new and unexpected result, which is important for security of computer systems, is that secure information flow can also be expressed and reasoned about in Hoare Logic. With Jost (St. Andrews), Hofmann has developed a type system for heap space consumption for class-based imperative object-oriented programming.

Formal Mathematics and Mathematics Education

Proof Technology Urban developed together with Stefan Berghofer from the Types site at the TU Munich the nominal datatype package, which is intended to provide an infrastructure for reasoning about binders in the theorem prover Isabelle/HOL. Using this package, Jesper Bengtson (from Uppsala University) formalised bisimulation theorems of the pi-calculus and Temesghen Kahsai (from Udine University) formalised parts of the spi-calculus. Further, parts of the POPLmark-Challenge were formalised as well as Church-Rosser and strong normalisation results in the lambda-calculus.

Foundational Research Hofmann has found a correctness proof of Light Linear Logic based on realizability semantics. This result provides a basis for extraction of correct programs from proofs in linear logic.

Schwichtenberg has carried out some theoretical studies concerning a semantical basis for a type theory with approximations. The goal is to have a proper context for studying computability in higher types. Rather than using domain theory for this purpose, it turned out to be beneficial to use a representation theory for damins, namely a variant of Scotts theory of information systems. In addition he has done some case studies on extracting computational content from formalized proofs.

Publications

Book Chapters

- Martin Hofmann, Hans-Wolfgang Loidl, and Lennart Beringer. Certification of Quantitative Properties of Programs. In *Logical Aspects of Secure Computer Systems*, Marktoberdorf, Aug 2-13, 2005. IOS Press. Lecture Notes of the Marktoberdorf Summer School 2005. To appear.

Refereed Journal Articles

- H-W. Loidl, A. Rauber Du Bois, P. Trinder. mHaskell: Mobile Computation in a Purely Functional Language. *Journal of Universal Computer Science*, 11(7):1234–1254, 2005. Selected papers from the SBLP'05: 9th Brazilian Symposium on Programming Languages, Recife, Brazil, May 23-25, 2005.
- Klaus Aehlig. Induction and inductive definitions in fragments of second order arithmetic. *The journal of Symbolic Logic*, 70(4):1087–1107, December 2005.
- Wilfried Buchholz. A term calculus for (co-)recursive definitions on streamlike data structures. *Ann. Pure Appl. Logic*, 136(1-2):75–90, 2005.
- Helmut Schwichtenberg. A direct proof of the equivalence between Brouwer's fan theorem and König's lemma with a uniqueness hypothesis. *Journal of Universal Computer Science*, 11(12):2086–2095, 2005.

Refereed Conference Contributions

- Andreas Abel. Implementing a normalizer using sized heterogeneous types. In Connor McBride and Tarmo Uustalu, editors, *Workshop on Mathematically Structured Functional Programming, MSFP 2006, Kuressaare, Estonia, July 2, 2006*, electronic Workshop in Computing (eWiC). The British Computer Society (BCS), 2006.
- Andreas Abel. Polarized subtyping for sized types. In D. Grigoriev, J. Harrison, and E. A. Hirsch, editors, *Computer Science Symposium in Russia (CSR 2006), St. Petersburg, June 8-12, 2006*, volume 3967 of *Lecture Notes in Computer Science*, pages 381–392. Springer-Verlag, 2006.
- Andreas Abel. Semi-continuous sized types and termination. In *Computer Science Logic, 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 21-24, 2006, Proceedings*, volume 4207 of *Lecture Notes in Computer Science*. Springer-Verlag, 2006.
- Andreas Abel. Towards generic programming with sized types. In Tarmo Uustalu, editor, *Mathematics of Program Construction: 8th International Conference, MPC 2006, Kuressaare, Estonia, July 3-5, 2006. Proceedings*, volume 4014 of *Lecture Notes in Computer Science*, pages 10–28. Springer-Verlag, 2006.
- Klaus Aehlig. A finite semantics of simply-typed lambda terms for infinite runs of automata. In Zoltan Esik, editor, *Procedings of the 20th international Workshop on Computer Science Logic (CSL '06)*, 2006. To appear.

- A. Rauber Du Bois, P. Trinder, and H-W. Loidl. Strong Mobility using a Continuation Monad. In *SBLP'06: 10th Brazilian Symposium on Programming Languages*, Itatiaia, Brazil, May 15-17, 2006.
- Martin Hofmann and Steffen Jost. Type-based amortised heap-space analysis. In Peter Sestoft, editor, *Programming Languages and Systems, 15th European Symposium on Programming, ESOP 2006, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2006, Vienna, Austria, March 27-28, 2006, Proceedings*, volume 3924 of *Lecture Notes in Computer Science*, pages 22–37, 2006.
- Martin Hofmann, Hans-Wolfgang Loidl, and Lennart Beringer. Certification of Quantitative Properties of Programs. In *Logical Aspects of Secure Computer Systems*, Marktoberdorf, Aug 2-13, 2005. IOS Press. Lecture Notes of the Marktoberdorf Summer School 2005. To appear.
- Ugo Dal Lago and Martin Hofmann. Quantitative models and implicit complexity. In R. Ramanujam and Sandeep Sen, editors, *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference, Hyderabad, India, December 15-18, 2005, Proceedings*, volume 3821 of *Lecture Notes in Computer Science*, pages 189–200. Springer, 2005.
- Helmut Schwichtenberg. Inverting monotone continuous functions in constructive analysis. To appear in *Logical Approaches to Computational Barriers*, editors: A. Beckmann, U. Berger, B. Loewe, and J. V. Tucker (Proc. CiE 2006, Swansea), pages 490–504, 2006.
- Helmut Schwichtenberg. Minlog. In F. Wiedijk, editor, *The Seventeen Provers of the World*, volume 3600 of *LNAI*, pages 151–157. Springer Verlag, 2006.
- Helmut Schwichtenberg. Recursion on the partial continuous functionals. To appear: Proc. 2005 ASL European Summer Meeting Athens, 2006.
- 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*, pages 25–32, 2005.
- C. Urban and D. Ratiu. Classical logic is better than intuitionistic logic: A conjecture about double-negation translations. In *Proc. of the Workshop on Classical Logic and Computation (CL&C)*.
- A. Al Zain, P. W. Trinder, H-W. Loidl, and G. J. Michaelson. Managing Heterogeneity in a Grid Parallel Haskell. In *PAPP'05: Second International Workshop on Practical Aspects of High-level Parallel Programming*, May 22-25, 2005, Atlanta, USA, 2005.

Theses

- Andreas Abel. *A Polymorphic Lambda-Calculus with Sized Higher-Order Types*. PhD thesis, Ludwig-Maximilians-Universität München, 2006.

Talks by Abel

- *Towards Generic Programming with Sized Types.* July 3, 2006. 8th International Conference on Mathematics of Program Construction, MPC '06, Kuressaare, Estonia, July 3-5, 2006.
- *Implementing a Normalizer Using Sized Heterogeneous Types.* July 2, 2006. Workshop on Mathematically Structured Functional Programming, MSFP 06, Kuressaare, Estonia.
- *Polarized Subtyping for Sized Types.* June 10, 2006. First International Computer Science Symposium in Russia (CSR 06), St. Petersburg, Russia, June 8-12, 2006
- *A Structurally Recursive Normalizer for Simply-Typed Lambda-Terms.* April 28, Functional Programming Lunch, Nottingham University, UK.
- *Higher-Order Subtyping, Revisited.* April 21, 2006. Types Workshop, Nottingham, UK.
- *Sized (Co-)Inductive Types With Applications to Generic Programming.* April 5, 2006. Programming Logics Group, Department of Computer Science, Chalmers University of Technology, Göteborg, Sweden.
- *Untyped Algorithmic Equality for Martin-Löf's Logical Framework with Surjective Pairs.* December 8, 2005. Arbeitstreffen Bern-München, Institut für Mathematik, Universität München.
- *Verifying Haskell Programs Using Constructive Type Theory.* September 30, 2005. Haskell Workshop 2005, Tallinn, Estonia.
- *Termination of Functions that Are Passed to their Arguments.* September 13, 2005. APPSEM II Workshop 2005, Frauenchiemsee, Munich, Germany.

Talks by Aehlig

- *Logic, Automata and Recursion schemes.* August 21, 2006. Second "Mathlogaps" Training Workshop (Leeds).
- *Non-Interleaved Polymorphic Types and Iterated Inductive Definitions.* July 27, 2006. Logic Colloquium (Nijmegen), special session on Proof Theory and Type Theory.

Talks by Loidl

- *A Generic Parallel Runtime-environment for High Performance Computation on Wide Area Networks.* Kolloquium Programmiersprachen und Grundlagen der Programmierung, Fischbachau, Germany, 5-7. Oktober, 2005.
- *EmBounded: Automatic Prediction of Resource Bounds for Embedded Systems.* Research Institute for Symbolic Computation, Univ. of Linz, June 22, 2006.

Talks by Schwichtenberg

- *Program extraction from constructive proofs.* Mathematical Colloqium, Uppsala University, September 22, 2005.
- *Program extraction from normalization proofs.* Logic Seminar Uppsala-Stockholm, November 1, 2005.
- *Minimal logic for computable functionals.* Logic Seminar, Chalmers University, January 2006.
- *Minimal logic for computable functionals.* Algebra, Computation and Logic, Colloquium honouring S. Adian Moskau, February 2006.
- *Logic for computable functionals and their approximations.* Logic Seminar Uppsala-Stockholm, February 15, 2006.
- *Computable functionals over non-flat domains.* Logic seminar, Oslo University, February 23, 2006.
- *Estimating solutions of ODEs.* Logic Seminar, Uppsala University, March 2, 2006.
- *A direct proof of the equivalence between Brouwer's fan theorem and König's lemma with a uniqueness hypothesis.* Trends in Constructive Mathematics, Frauenwoerth, June 2006.
- *Proofs with feasible computational content.* ASL Summer Conference Montreal, May 2006.
- *Inverting monotone continuous functions in constructive analysis.* Computability in Europe, Swansea 2006.

Talks by Urban

- University of Frankfurt (22 June, host: Prof. Schmidt-Schauss)
- PoplMark-Workshop at POPL 2006 (Charleston, South Carolina, 13 - 16 January)
- Carnegie Mellon University (11 November, host: Frank Pfenning)
- University of Pennsylvania (9 - 21 November, hosts: Benjamin Pierce and Steve Zdancewic)
- Workshop on Computational Applications of Nominal Sets in London (CANS, 6 December, hosts: Andrew Pitts and Maribel Fernandez)

8.7 Munich – TU

Correctness of Computer Systems

- Tobias Nipkow and Farhad Mehta have worked on calculi for the verification of pointer programs. The results of this work have been published in the Journal *Information and Computation*.
- Norbert Schirmer has finished his Ph.D. thesis on a verification environment for sequential imperative programs, focussing on a subject of the *C* language.
- Martin Wildmoser has finished his Ph.D. thesis on a verified framework for proof-carrying code.

Foundational Research

- Stefan Berghofer and Christian Urban have developed a package for *nominal datatypes* in Isabelle/HOL, which is already used by Jesper Bengtson from the group of Joachim Parrow at the University of Uppsala to formalize properties of the Pi-calculus. A paper by Christian Urban and Stefan Berghofer about the construction of recursion combinators for nominal datatypes will be presented at IJCAR 2006.
- Several methods for formalizing calculi with variable binding, in particular the nominal and the de Bruijn indices approach, have been compared in a paper by Stefan Berghofer and Christian Urban, which will be presented at the LFMTP 2006 workshop.
- An article about program extraction from Tait-style normalization proofs using the proof assistants Minlog, Coq, and Isabelle by Ulrich Berger (Swansea), Stefan Berghofer, Pierre Letouzey (Paris), and Helmut Schwichtenberg (LMU München) has appeared in the Journal *Studia Logica*.
- Benoit Montagu from the Paris site has done an internship at TU München site from May to July 2006, where he developed a linear type system for Isabelle together with Tobias Nipkow and Alexander Krauss. The type system will be used to generate efficient executable code involving *destructive updates* of data structures such as arrays from specifications written in Isabelle.

Formal Mathematics and Mathematics Education

- In cooperation with Tom Hales and Sean McLaughlin from the University of Pittsburgh, Tobias Nipkow has continued the verification of a program enumerating so-called *tame graphs*, which has been started by his former Ph.D. student Gertrud Bauer. A description of the correctness proof of the graph enumeration algorithm, which forms an integral part of the mechanized proof of the *Kepler conjecture*, has been published in the proceedings of the IJCAR 2006 conference.

- In cooperation with Jesus Aransay from the Departamento de Matemáticas y Computación of the Universidad de La Rioja, Clemens Ballarin and Stefan Berghofer are carrying out research on the extraction of programs from proofs in constructive algebra.

Proof technology

- Markus Wenzel has extended the Isabelle/Isar proof language with an advanced method for proofs by induction, supporting induction with local facts and parameters, definitions, simultaneous goals and multiple rules. It has already been applied successfully by Stefan Berghofer and Christian Urban in their solutions to the PoplMark challenge. A paper describing the design principles and the theory underlying the induction method will appear in the proceedings of the MKM 2006 conference.

Publications

Refereed journal papers

- Farhad Mehta and Tobias Nipkow. Proving pointer programs in higher-order logic. *Information and Computation*, 199:200–227, 2005

Invited journal papers

- Ulrich Berger, Stefan Berghofer, Pierre Letouzey, and Helmut Schwichtenberg. Program Extraction from Normalization Proofs. *Studia Logica*, 82:25–49, February 2006

Refereed conference papers

- Tobias Nipkow and Lawrence C. Paulson. Proof pearl: Defining functions over finite sets. In J. Hurd, editor, *Theorem Proving in Higher Order Logics (TPHOLs 2005)*, volume 3603 of *LNCS*, pages 385–396. Springer, 2005

- Tobias Nipkow and Gertrud Bauer. Flyspeck I: Tame graphs. In Ulrich Furbach and Natarajan Shankar, editors, *Third International Joint Conference on Automated Reasoning (IJCAR 2006)*, volume 4130 of *LNCS*, pages 21–35. Springer, 2006

- Martin Wildmoser and Tobias Nipkow. Asserting bytecode safety. In S. Sagiv, editor, *Programming Languages and Systems (ESOP)*, volume 3444 of *LNCS*, pages 326–341. Springer, 2005

- Markus Wenzel and Lawrence C. Paulson. Isabelle/Isar. In F. Wiedijk, editor, *The Seventeen Provers of the World*, volume 3600 of *LNAI*. Springer, 2006

- Markus Wenzel. Structured induction proofs in Isabelle/Isar. In J. Borwein and W. Farmer, editors, *5th International Conference on Mathematical Knowledge Management, MKM 2006*, volume 4108 of *LNAI*. Springer, 2006

- Christian Urban and Stefan Berghofer. A Recursion Combinator for Nominal Datatypes Implemented in Isabelle/HOL. In Ulrich Furbach and Natarajan Shankar, editors, *Third International Joint Conference on Automated Reasoning (IJCAR 2006)*, LNCS. Springer, 2006

- Stefan Berghofer and Christian Urban. A Head-to-Head Comparison of de Bruijn Indices and Names. In Brigitte Pientka and Alberto Momigliano, editors, *International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP'06)*, ENTCS. Elsevier, 2006

Dissertations

- Norbert Schirmer. *Verification of Sequential Imperative Programs in Isabelle/HOL*. PhD thesis, Institut für Informatik, TU München, 2006

- Martin Wildmoser. *Verified Proof Carrying Code*. PhD thesis, Institut für Informatik, TU München, 2006

8.8 Nijmegen

Foundational Research Geuvers and Loeb have studied further the notion of 'deduction graph' and the connection with proof nets. Loeb has paid a successfull visit to Paris VII to study this. There is a forthcoming publication of Geuvers-Loeb in the journal MSCS and an invited talk in MFCS 2006 (Slowakia).

Niqui has further studied the theory of exact real arithmetic, notably the property of productivity and the coinduction an corecursion principles that atre associated with data types of exact reals.

Spitters has further studied the connections between constructive analysis and formal topolgy, partly in cooperation with Coquand from Chalmers.

Formal Mathematics and Mathematics Education We cooperate with Dutch mathematicians in the Diamant project, where we try to get them interested in formalized mathematics. There has been a 'Diamant day' to discuss some ideas and to explain to the mathematicians what proof formalization amounts to.

O'Connor has made an implementation of exact real arithmetic in Haskell, called 'Few Digits', with which he participated in the Manydigits competition.

Proof technology Kaliszyk has developed a web interface for Coq that will be extended further to act as an interface for Coq in an educational setting. The interface will be tested out in logic courses at the Radboud University Nijmegen and the Free University of Amsterdam.

Pierre Corbineau has developed a 'mathematical mode' for Coq, allowing the uder to do declarative (Mizar style) proofs in Coq (as opposed to the procedural, tactic style, proofs that are standard for Coq).

Lionel Mamane and Herman Geuvers have developed a TexMacs mode for Coq, which provides a mechanism to integrate mathematical documents (edited with TexMacs, a wysiwyg LaTeX style math editor) with formal (Coq) proofs.

Publications

Refereed journal papers

- B. Spitters, Constructive Results on Operator Algebras Journal of Universal computation volume 11, issue 12 2005.
- T. Coquand and B. Spitters, Formal Topology and Constructive Mathematics: the Gelfand and Stone-Yosida Representation Theorems, Journal of Universal computation volume 11, issue 12 2005.
- B. Spitters, A constructive view on ergodic theorems Journal of Symbolic Logic, June 2006, 71(2) pp. 611-623
- B. Spitters, Almost periodic functions, constructively LMCS Volume 1, issue 3, paper 4, 2005.
- T. Coquand and B. Spitters A constructive proof of the Peter-Weyl theorem, Mathematical Logic Quarterly. Vol. 4, 2005, page 351-359.
- B. Spitters, Approximating integrable sets by compacts constructively. in From Sets and Types to Topology and Analysis - Towards Practicable Foundations for Constructive Mathematics, Laura Crosilla and Peter Schuster (eds.), Oxford Univ. Press, 2005.
- H. Barendregt and F. Wiedijk, The Challenge of Computer Mathematics, Transactions A of the Royal Society 363 no. 1835, 2351-2375, 2006.

Books

- F. Wiedijk (ed.), The Seventeen Provers of the World, foreword by Dana S. Scott, Springer LNAI 3600, 2006.

Refereed conference papers

- B. Spitters, Constructive algebraic integration theory without choice In: Thierry Coquand and Henri Lombardi and Marie-Francoise Roy, Mathematics, Algorithms, Proofs, Dagstuhl Seminar Proceedings 05021, Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany.
- H. Barendregt and R. Statman, Böhm's Theorem, Church's Delta, Numeral Systems, and Ershov Morphisms, In: Processes, Terms and Cycles: Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop on the Occasion of His 60th Birthday, Eds. A. Middeldorp, V. van Oostrom and F. van Raamsdonk, Springer LNCS, vol. 3838, 2005, 40-54.

- A. Asperti, H. Geuvers, I. Loeb, L. Mamane and C. Sacerdoti Coen An Interactive Algebra Course with Formalised Proofs and Definitions to appear in the Proceedings of the Fourth Conference Mathematical Knowledge Management, MKM 2005 (Bremen, July 2005), Springer LNCS.

Talks

- Reflecting proofs in first-order logic with equality Pierre Corbineau, Cooperation of Deduction Tools QSL, Loria, Nancy, April, 2006
- M. Niqui Coinductive Field of Exact Real Numbers and General Corecursion, 8th International Workshop on Coalgebraic Methods in Computer Science, Vienna, 2006.
- B. Spitters, Observational integration theory Invited lecture at the ASL Meeting in Montreal 2006.
- F. Wiedijk, Computer algebra inside a proof assistant, small Types workshop, Nijmegen, 2005-10-03.
- F. Wiedijk, An introduction to the formalization of mathematics and decision procedures, Diamant day, Nijmegen, 2005-10-28.
- H.Barendregt The interaction of computing and proving in Computer Mathematics, DIAMANT/EIDMA symposium 2005
- Bas Spitters Constructive mathematics and the algebraization of analysis, DIAMANT/EIDMA symposium 2005
- Russell O'Connor Machine Verification of Incompleteness of PA, DIAMANT/EIDMA symposium 2005
- H. Barendregt, Progress in Computer Mathematics, Nederlands Mathematisch Congres 2006.
- H. Geuvers, From Deduction Graphs to Proof Nets: Boxes and Sharing in the Graphical Presentation of Deductions, Invited talk at MFCS 2006 31st International Symposium on Mathematical Foundations of Computer Science.
- L. Mamane, Surreal Numbers in Coq, in Types for Proofs and Programs: International Workshop, Types 2004, Jouy-en-Josas, France, December 15-18, 2004, Selected Papers, J.-C. Filliatre, C. Paulin-Mohring, B. Werner, editors, LNCS 3839, Pages 170 - 185.
- H. Geuvers, L. Mamane, A Document-Oriented Coq Plugin for TeXmacs, to appear in proceedings of the MathUI workshop at the MKM 2006 conference, Wokingham, UK, 10 August 2006.
- M Niqui, Formalising Exact Arithmetic in Type Theory, In S. Barry Cooper, Benedikt Löwe, Leen Torenvliet (Eds.), New Computational Paradigms: First Conference on Computability in Europe, CiE 2005, Amsterdam, The Netherlands, 2005, LNCS 3526.

8.9 Bialystok

Formal Mathematics and Mathematics Education The MIZAR system has been used in two undergraduate courses: *Introduction to Logic and Set Theory* and *Formalizing Mathematics* for computer science students at the University of Bialystok. Another MIZAR-based course has been scheduled for the next year: *Software Verification*.

Since September 2005, the MIZAR Mathematical Library (MML) has been extended with 37 new articles (including the completion of the project to formalize the proof of the Jordan Curve Theorem by Artur Kornilowicz).

Proof technology The strength of the MIZAR checker has been improved by implementing additional computer algebra mechanisms concerning the arithmetic of complex numbers. The MIZAR language has been extended with several new features, including the new semantics of the `equals` construct which allows for automatic definition expansion of terms. The newly implemented mechanisms have enabled a number of MML revisions. MML has been divided into two parts: *abstract* (involving the notion of structure) and *concrete* (based on pure set theory).

Publications

Refereed journal papers

- Adam Naumowicz, *An Example of Formalizing Recent Mathematical Results in* MIZAR. In press: C. Benzmueller (ed.), Special Issue on Mathematics Assistance Systems, Journal of Applied Logic, Elsevier, 2006.

8.10 Royal Holloway, University of London

The Types-related main scientific work includes:

Foundational Research

- Zhaohui Luo, together with Robin Adams, has been studying a type-theoretic framework for formalisation of mathematical theories with different logical foundations. This theory is being used in formalisation of Weyl's classical predicative mathematics (see below) and verification of program properties such as those of security protocols.
- Zhaohui Luo and Sergei Soloviev have worked on further development on coerceive subtyping and given a joint talk at WIT'05 at Toulouse in 2005.
- Zhaohui Luo and Robin Adams have worked on coercive subtyping for parameterised inductive types in the presence of certain extensional equality rules.

Formal Mathematics and Proof technology

- Robin Adams and Zhaohui Luo have been studying how to use a type-theoretic framework to formalise Weyl's work on classical predicative mathematics. A formalisation of Weyl's work on calculus has been done in Plastic, with the help from Paul Callaghan. A talk on this topic has been given in Types'06.

The Types-related publications/presentations after Sep 1, 2005 include

Refereed journal papers

- R. Adams. *Pure Type Systems with Judgemental Equality.* Journal of Functional Programming 16(2): 219-246, March 2006. First published online 28 October 2005.
- J. Pang, P. Calllaghan and Z. Luo. *LFTOP: an LF-based approach to domain-specific reasoning.* Journal of Computer Science and Technology, 20(4), pp 526-535. 2005.
- Zhaohui Luo and Robin Adams. *Subtyping for Inductive Types and Extensional Equality Rules.* Submitted. 2006.

Refereed conference papers

- R. Adams. *A Formalization of the Theory of Pure Type Systems in Coq.* In Filiatre, Paulin-Mohring and Werner (eds.), Types for Proofs and Programs, International Workshop, Types 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers. LNCS 3839. Springer, 2006. 1-16.

Talks

- R. Adams and Z. Luo. *Weyl's predicative math in type theory.* Types'06, 2006.
- A. Adams. *The Equivalence of Convertibility and Judgemental Equality.* Types'06, 2006.
- Z. Luo and S. Soloviev. *Coercive subtyping: PAL$^+$ and beyond.* WIT'05, Toulouse, Oct. 2005.

Dissertations

- J. Pang. *LFTOP: An LF based approach to domain-specific reasoning.* PhD thesis. University of Durham. 2006. (Supervisors: P. C. Callaghan and Z. Luo.)

8.11 Edinburgh

Correctness of Computer Systems As part of our work with the MOBIUS project we have contributed to a program logic for Java bytecode. This logic is formalised in the Coq proof assistant, and is proved sound w.r.t. an operational semantics of the Java Virtual Machine, also formalised in Coq.

Foundational Research Cheney, Momigliano, Pollack, Power: Reasoning about languages with binding and nominal logic. Currently a hot topic in the programming language research community, thus extending the impact of Types to other researchers. We have given talks, published papers and organised a Types workshop.

Formal Mathematics and Mathematics Education

Proof technology Aspinall and others: Proof General, a widely used generic interface for proof assistants. Existing version used by several of the Types research tools. A new version based on modern technology (Eclipse) is available in beta-release.

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.

Publications

Refereed journal papers

- L. Dixon and J. D. Fleuriot. A proof-centric approach to mathematical assistants. *Journal of Applied Logic: Special Issue on Mathematics Assistance Systems*, 2005. To appear
- Cheney. Completeness and herbrand theorems for nominal logic. *Journal of Symbolic Logic*, 71(1), 2006
- Conor McBride, Healfdene Goguen, and James McKinna. A few constructions on constructors. In *Post Conference Proceedings, 2004 TYPES Workshop*, volume 3839 of *LNCS*, pages 252–267. Springer Verlag, 2006
- Healfdene Goguen, Conor McBride, and James McKinna. Eliminating dependent pattern matching. In *Algebra, Meaning and Computation, a Festschrift for Joseph Goguen*, volume 4060 of *LNCS*. Springer Verlag, 2006

Refereed conference papers

- Sannella, Hofmann, Aspinall, Gilmore, Stark, Beringer, Loidl, MacKenzie, Momigliano, and Shkaravska. Mobile resource guarantees; evaluation paper. In *Trends in Functional Programming, 2005*, September 2005. Refereed proceedings to appear

- Stéphane Lengrand, Roy Dyckhoff, and James McKinna. Type theory in sequent calculus. In *Proceedings of Computer Science Logic, CSL'06*, LNCS. Springer Verlag, 2006
- Miki Tanaka and John Power. A unified category-theoretic formulation of typed binding signatures. In *Proceedings of the 3rd workshop on MEchanized Reasoning about Languages with variable bINding, MERLIN'05*, September 2005
- Robert Atkey. Parameterised notions of computation. In Conor McBride and Tarmo Uustalu, editors, *Proceedings of Workshop on Mathematically Structured Functional Programming (MSFP 2006)*, BCS Electronic Workshops in Computing, pages 31–45, July 2006
- Cheney. The semantics of nominal logic programs. In *International Conference on Logic Programming, ICLP 2006*, August 2006
- Cheney. Towards a general theory of names, binding and scope. In *Proceedings of the 3rd workshop on MEchanized Reasoning about Languages with variable bINding, MERLIN'05*, September 2006

Talks

- James McKinna. Why dependent types matter. In *Proceedings 33rd ACM SIGACT/SIPLAN Symposium on Principles of Programming Languages*, page 1. ACM, ACM Press, 2006. Invited Talk Abstract
- John Power. The universal algebra of computational effects: Lawvere theories and monads, July 2006. Invited talk at Workshop on Mathematically Structured Functional Programming, MSFC'06
- Aspinall, Beringer, and Momigliano. Optimisation validation. Technical Report EDI-INF-RR-0509, Edinburgh University, February 2006. Talk given at Compiler Optimisation Meets Compiler Verification, COCV 2006
- Johansson, Bundy, and Dixon. Best-first Rippling. In *Workshop on Strategies in Automated Deduction, IJCAR'06*, 2006. To appear
- Ornaghi, Fiorentini, and Momigliano. Snapshots generation via constructive logic. In *MoVeLog'05*, October 2005

Dissertations

- L. Dixon. *A Proof Planning Framework for Isabelle.* PhD thesis, University of Edinburgh, 2005

8.12 Manchester

Formal Mathematics and Mathematics Education

Peter Aczel designed a case-study for a 'machine-checked proof with gaps' of the Fundamental Theorem of Algebra that is intended to formalise the classical Algebraic Topology proof that uses the result that the fundamental group of the circle is the additive group of integers.

Foundations

Joao Belo has continued into the second year of his PhD work on the general theory of dependently sorted logic. The main attention has been on the formulation and proof of the interpolation theorem for that logic, which seems to raise interesting new problems.

Peter Aczel has continued to work on Constructive Set Theory and the development of Constructive Mathematics. In particular he has completed work on a constructive proof of a result in descriptive set theory and has been working on two applications of sheaf models for constructive set theory.

Visits to other sites

- Aczel attended the small workshop on Constructive analysis, types and exact real numbers. 3/4 October 2005, Nijmegen, the Netherlands.
- Aczel made regular visits to the Royal Holloway site in connection with the Pythagoras project, particularly during January and February, 2006.
- Aczel visited the Nijmegen site during March and April, 2006, and the LMU, Munich site during May and June, 2006.
- Joao Belo visited the Nijmegen site in March 2006 and the LMU Munich site in June, 2006. 2006.

Meeting Aczel organised a Constructive Mathematics Day on December 9th, 2006, in Manchester. Five invited talks were given on a variety of topics in constructive mathematics. The speakers from Types sites were Peter Schuster (Munich LMU), Giovanni Sambin (Padua) and Steve Vickers (Birmingham).

The CM Day talks

Algebraic Set Theory for CST , by Nicola Gambino (LaCIM, Université du Québec a Montréal, visiting Manchester)

Classifying categories as classes , by Steve Vickers (Birmingham)

Brouwerian principles and constructive set theory , by Michael Rathjen (Leeds)

The meaning of topological definitions in a predicative setting , by Giovanni Sambin (Padova)

Problems as Solutions , by Peter Schuster (Munich - LMU)

Talks

Aczel, *An Introduction to Constructive Set Theory* and *The constructive notion of set*, two invited talks at the meeting "Set Theory in the Third Millenium" in Brussels, December, 2005.

Aczel, *A constructive version of the Lusin Separation Theorem*, invited talk at the Amsterdam/Utrecht Workshop on Constructive Set Theory, March, 2006.

Aczel, *Dependently sorted/typed intuitionistic predicate logic as a setting for the discussion of foundations.*, invited talk at the meeting "Les Theories Modernes des Types", Paris, March, 2006.

Belo, *Dependently Sorted Logic*, seminar talk, Nijmegen, March 2006.

Aczel, *Another case study on the FTA*, seminar talk, Nijmegen, April, 2006.

Aczel, *The σ-Completeness Principle*, two seminar talks, Munich LMU, May, 2006.

Aczel, *Constructive Mathenatics and the σ-Completeness Principle*, Colloquium talk, Munich - LMU, June, 2006.

Belo, *Interpolation for Dependently Sorted Logic*, seminar talk, Munich, June 2006.

Aczel, *A constructive version of the Lusin Separation Theorem*, talk at the Bern-Munich workshop "Deductive Aspects of Proof Theory and Informatics", June, 2006.

Aczel, *Two possible principles for constructive set theory*, invited talk, at the Workshop "Trends in Constructive Mathematics", Frauenwörth (Chiemsee, Bavaria, Germany), June 2006.

Refereed Journal Papers

Aczel, *Aspects of General Topology in Constructive Set Theory*, The proceedings of the second workshop of Formal Topology in a special issue of the Annals of Pure and Applied Logic, 137 (2006) 3-29.

Gambino and Aczel, *The Generalised Type-theoretic Interpretation of Constructive Set Theory*, in the Journal of Symbolic Logic, Volume 71, Number 1, March (2006), 67-103.

PhD Dissertation

Fox, *Point-set and Point-free Topology in Constructive Set Theory*, University of Manchester, 2005.

Refereed Book Chapters These are essentially books based on conference proceedings.

Aczel and Fox, *Separation properties in Constructive Topology*, in "From Sets and Types to Topology and Analysis - Towards Practicable Foundations of Constructive Mathematics" (L. Crosilla, P. Schuster, eds.), Oxford Logic Guides, Oxford University Press, pp 176-192, October 2005.

Aczel, *A constructive proof of the Lusin separation theorem*, to appear in the book *"Logicism, Intuitionism and Formalism - What has become of them?"*, (S. Lindström, E. Palmgren, K. Segerberg, and V. Stoltenberg-Hansen eds.), 200?

8.13 Torino

The Torino site has given important contributions in the area of typing for concurrent, functional and object oriented programming languages. The main achievements have been obtained in the field of type systems and static analysis tools for these languages. More recently, the site's interests have focused on types for formal proofs, in the case a (possibly partial) formal certification of the involved components and tools is then necessary to guarantee their good behavior and to provide a basis for checking the consistency of the whole system or of substantial parts of it. Another area of interest is the development of languages and tools for global and ubiquitous computing. The team has given significant contributions to the study of specification and implementation languages for global computing components, including the related aspects of typing, security, code mobility, access control, and communication protocols.

Our goals include developing primitives for safe and efficient communication protocols The variety of mobile communication devices demands for innovative approaches and tools for the specification, analysis, and synthesis of safe and efficient communication protocols. We are also interested in formal certification of program properties. One of the goals consists in building a set of methodological tools for studying the classical complexity from a new perspective, and at the same time for analyzing all constraints, both qualitative and quantitative, originated from the need that the program interacts correctly with the execution environment. The certification can be done by statically assigning types to programs at compile time, where the type structure carries the information about the desired properties.

Publications

1. S. van Bakel, U. de' Liguoro, "Subtyping Object and Recursive Types Logically", in ICTCS'05, LNCS 3701, pp. 66-80, 2005.

2. M. Coppo, F. Cozzi, M. Dezani-Ciancaglini, E. Giovannetti and R. Pugliese. A Mobility Calculus with Local and Dependent Types, Processes, Terms and Cycles: Steps on the Road to Infinity, In Middeldorp, A. and van Oostrom, V. and van Raamsdonk, F. and de Vrijer, R. ed(s)., LNCS 3838, pages 404–444, 2005, Springer-Verlag.

3. P. Coppola, U. Dal Lago and S. Ronchi Della Rocca. Elementary Affine Logic and the Call by Value Lambda Calculus, TLCA'05, In P. Urzyczyn ed(s)., LNCS 3461, pages 131-145, 2005, Springer-Verlag.

4. M. Dezani-Ciancaglini, D. Mostrous, N. Yoshida and S. Drossopoulou. Session Types for Object-Oriented Languages, ECOOP'06, In Dave T. ed., LNCS 4067, pages 328–352, 2006, Springer-Verlag.

5. M. Dezani-Ciancaglini, N. Yoshida, A. Ahern and S. Drossopoulou. Ldoos: a Distributed Object-Oriented language with Session types, TGC 2005, In R. De Nicola and D. Sangiorgi ed(s)., LNCS 3705, pages 299-318, 2005, Springer-Verlag.

6. P. Garralda, A. Compagnoni and M. Dezani-Ciancaglini. BASS: Boxed Ambients with Safe Sessions, PPDP'06. In M. ed(s)., pages 61-72, 2006, ACM Press.

8.14 Udine – Padova

Correctness of Computer Systems In [HLR06], Honsell, Lenisa and Redamalla extended Reichel-Jacobs coalgebraic account of objects and classes in Object Oriented Programming to (*generalized*) *binary methods*. These are methods that take more than one parameter of a class type. Class types include products, sums and powerset type constructors. In order to take care of class *constructors*, classes are modeled as *bialgebras*.

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

Ciaffaglione, Hennessy, Rathke devised tractable proof techniques for proving behavioural equivalence of mobile, distributed systems, modeled within the Distributed pi-calculus. Using these methods, thye addressed the correctness of sample protocols, such as crossing a firewall and the interaction between a server and its clients.

The Theory of Contexts is a type-theoretic axiomatization aiming to give a metalogical account of the fundamental notions of variable and context as they appear in Higher Order Abstract Syntax. In [BHHMS06], we prove that this theory is consistent by building a model based on functor categories. By means of a suitable notion of forcing, we prove that this model validates Classical Higher Order Logic, the Theory of Contexts, and also (parametrised) structural induction and recursion principles over contexts. Our approach, which we present in full detail, should also be useful for reasoning on other models based on functor categories.

In [MSH06], we have studied the relation between Nominal Logic and the Theory of Contexts, two approaches for specifying and reasoning about datatypes with binders. We have presented a translation of terms, formulas and judgments of an intuitionistic nominal logic, called NINL, into terms and propositions of CIC, via a weak HOAS encoding. It turns out that the (translation of the) axioms and rules of NINL are derivable in CIC extended with the Theory of Contexts (CIC/ToC), and that in the latter we can prove also sequents which are not derivable in NINL. Thus, CIC/ToC can be seen as a strict extension of NINL.

Foundational Research M.E. Maietti and G. Sambin studied the meaning of a "proofs-as-programs" foundation for constructive mathematics, usually identified with a type theory, like that introduced by Martin-Loef or the Calculus of Constructions by T. Coquand, by characterizing it via mathematical logical principles (M.E. Maietti gave a talk on this at Types '06 Nottingham entitled "Type theory as a solution to the "proofs-as-programs" problem). They argued that a proofs-as-programs foundation for constructive mathematics should be equipped with two levels: an intensional level of programs represented by a type theory, and an extensional level where to introduce extensional concepts and to develop mathematical proofs. In this minimal foundation we can formalize most of formal topology developed in Padova and surely all the work on "Basic Picture" introduced by G. Sambin.

Sambin and others developed the study of topological properties by means of formal topology (introduced by G. Sambin and P. Martin-Loef in the eighties)

expecially about exponentiation [M05], about the binary positivity predicate in [ST05], [V05], about the spatiality of inductively generated formal topologies in [V06], about the set-presentation of formal points of a compact regular formal topology and uniform spaces in [C06].

Publications

Refereed journal papers

- Alberto Ciaffaglione, Pietro Di Gianantonio "A Certified, Corecursive Implementation of Exact Real Numbers" Theoretical Computer Science 351(1), Special issue on Real Numbers and Computers, 2005
- G. Battilotti, G. Sambin, Pretopologies and a uniform presentation of suplattices, quantales and frames, in Annals of Pure and Applied Logic, 137, 1-3, pp. 30-61
- G. Boniolo, S. Valentini, Vagueness, Kant and Topology. to appear in the Journal of Philosophical Logic, 2006.
- G. Curi, "On the collection of points of a formal space". Ann. Pure Appl. Logic 137, 1-3, 2006, pp. 126-146.
- M.E. Maietti, Modular correspondence between dependent type theories and categorical universes, including pretopoi and topoi, Mathematical Structures in Computer Science, 15(6):1089–1149, 2005
- G.Sambin and G.Trentinaglia. On the meaning of positivity relations for formal spaces. to appear in Constructivity, computability and logic. A collection of papers in honour of the 60th birthday of Douglas Bridges, C.S.Claude, H.Ishihara eds., 2006
- S. Valentini, The problem of the formalization of constructive topology. Archive for Mathematical Logic, vol. 44 (1),(2005), pp. 115-129
- S. Valentini, Every countably presented formal topology is spatial, classically. To appear in the Journal of Symbolic Logic, 2006.
- [BHHMS06] Anna Bucalo, Martin Hofmann, Furio Honsell, Marino Miculan, Ivan Scagnetto. Consistency of the Theory of Contexts. Journal of Functional Programming, Volume 16, Issue 03, May 2006, pp 327-395

Refereed conference papers

- [Mai05] M.E. Maietti. Predicative exponentiation of locally compact formal topologies over inductively generated ones. In L. Crosilla and P. Schuster, editor, From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics, number 48 in Oxford Logic Guides, pages 202–222, Oxford University Press, 2005.
- [MS05] M.E. Maietti, G. Sambin, Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editor, From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics, number 48 in Oxford Logic Guides, pages 91–114. Oxford University Press, 2005.

- [CHR05] Alberto Ciaffaglione, Matthew Hennessy, Julian Rathke "Proof Methodologies for Behavioural Equivalence in Distributed pi-calculus" Best Paper Award. In Proceedings of FORTE, Taipei (Taiwan) Lecture Notes in Computer Science 3731, 2005

- [HLR06] F. Honsell, M. Lenisa, R. Redamalla: "Coalgebraic Description of Generalized Binary Methods", *Developments in Computational Models (DCM'05)* Workshop Proceedings, M. Fernandez et al eds., ENTCS **135**(3), 2006 , 73–84.

- [CHL06] D. Cancila, F. Honsell, M. Lenisa: "Functors Determined by Values on Objects", *MFPS XXII* Conference Proceedings, S. Brookes and M. Mislove ed., ENTCS **158**, 2006, 151–169.

- [CHL06a] D. Cancila, F. Honsell, M. Lenisa: "Some Properties and Some Problems on Set Functors", *Coalgebraic Methods in Computer Science (CMCS'06)* Workshop Proceedings, ENTCS (to appear).

- [MSH06] M. Miculan, I. Scagnetto, F. Honsell: "Translating Specifications from Nominal Logic to CIC with the Theory of Contexts". In R. Pollack, editor, Proceedings of MERLIN'05. ACM DL, 2005.

Invited Talks

- G. Curi ("On some peculiar aspects of the category of formal spaces") M.E.Maietti ("Towards a minimal two-level foundation for constructive mathematics") and G. Sambin (" Basic picture as invariance") had been invited at the Workshop "Trends in Constructive Mathematics" Chiemsee, Germany, 18-23/6/2006.

- Marino Miculan, "Behind the name: the many faces of atomic terms". Invited talk at the Theory Days, 3–5 February 2006, Koke, Estonia.

- G. Sambin "The dynamics between foundation and implementation of mathematics", Invited Lecture at "Logic, Models and Computer Science", Camerino (Italy), 20-222 April 2006.

- G. Sambin, "Dynamics in foundations", Invited lecture at the Department of Mathematics, University of Ljubliana, 10 May 2006

8.15 Warsaw

The Applied Logic Group is a part of the Institute of Informatics of Warsaw University. The group participated in the previous Types project Computer-Assisted Reasoning based on Type Theory in 1999-2003.

The expertise of the group as a whole is mostly in logics of programs, typed lambda calculi, type inference, finite model theory, theory of tree automata and mu calculus. Recently there is a growing interest towards proof assistants, especially the Coq system.

Correctness of Computer Systems We made a case study on using program annotation and extended static checking tools to eliminate common programming errors. It turned out that the amount of effort needed to write the annotatations is considerable but the results are satisfactory. We also developed a tool to propagate one kind of type annotations.

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

We proved that the lambda definability problem limited to regular fourth order types is decidable in any finite domain. As an additional effect we may observe that for certain types there is no finite context free grammar generating all closed terms. We prove also that probability that randomly chosen fourth order type (or type of the order not grater then 4) which admits decidable lambda definability problem is zero.

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

Formal Mathematics and Mathematics Education An experimental extension to the Coqide environment was developed. It displays a natural language hints to the user about possible next proof steps, therefore teaching him how to use the proof environment.

Publications

Books

- M.H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 2006

Refereed journal papers

- M. Zaionc. Probabilistic approach to the lambda definability for fourth order types. 140, 2005
- M. Zaionc. Probability distribution for simple tautologies. *Theoretical Computer Science*, 355(2), 2006
- P. Waszkiewicz. Banach domains: computational models of banach spaces. *Topology Proceedings*. to appear
- P. Waszkiewicz. Partial metrizability of continuous posets. *Mathematical Structures in Computer Science*. to appear

Refereed conference papers

- A. Gąsienica-Samek, T. Stachowicz, J. Chrząszcz, and A. Schubert. KOTEK: Clustering of The Enterprise Code. In *Software Engineering: Evolution and Emerging Technologies*, volume 130. IOS Press, 2005
- J. Chrząszcz and J.-P. Jouannaud. From OBJ to ML to Coq. In *Goguen Festschrift*, volume 4060 of *LNCS*. Springer, 2006
- D. Walukiewicz-Chrząszcz and J. Chrząszcz. Consistency and completeness of rewriting in the calculus of constructions. In *International Joint Conference on Automatic Reasonning 2006*, volume 4130 of *LNAI*. Springer, 2006
- M. Cielecki, J. Fulara, K. Jakubczyk, Ł. Jancewicz, J. Chrząszcz, A. Schubert, and Ł. Kamiński. Propagation of JML non-null annotations in Java programs. In *International Conference on Principles and Practices of Programming in Java*, Mannheim, 2006. ACM Press
- A. Schubert and J. Chrząszcz. ESC/Java2 as a Tool to Ensure Security in the Source Code of Java Applications. In *Software Engineering Techniques 2006*, LNCS, Warsaw, 2006. Springer
- J. Chrząszcz, A. Gąsienica Samek, A. Schubert, and T. Stachowicz. Minik: A Tool for Maintaining Proper Java Code Structure. In *Software Engineering Techniques 2006*, LNCS, Warsaw, 2006. Springer

Talks

- Daria Walukiewicz-Chrząszcz gave a talk "Consistency and completeness of rewriting in the Calculus of Constructions" (joint work with Jacek Chrząszcz) at Types meeting in Nottingham, UK in April 2006.
- Marek Zaionc gave a talk "On the density of types with decidable lambda definability problem", at Types meeting in Nottingham, UK in April 2006.
- Marek Zaionc gave a talk "Asymptotic densities in logic", at the conference "Computability in Europe" in Swansea, UK in July 2006.

8.16 Tallinn

Correctness of Computer Systems A. Saabas and T. Uustalu extended their work on compositional semantics and logics for low-level languages to a language with a stack and a possibility of abnormal terminations. They developed an abstracted semantics and type system for stack safety and non-interference. They also extended the work of P. Laud et al on dataflow analyses as type systems demonstrated that program optimizations can be usefully described as type systems with a transformation component. O. Shkaravska worked on logics and type systems for resource control.

Foundational Research T. Uustalu and V. Vene worked on the metatheory of their comonadic semantics of dataflow computation and attribute evaluation. Together with N. Ghani and M. Hamana they developed a representation of cyclic datatypes via nested datatypes based on a de Bruijn syntax for explicit fixpoint operators.

T. Uustalu together with T. Altenkirch worked on the monadic semantics of partiality from non-termination. T. Uustalu and V. Vene with T. Altenkirch studied the semantics of interactive input-output based on resumptions.

Publications

Refereed journal papers

- N. Ghani, T. Uustalu, V. Vene. Generalizing the augment combinator. In H.-W. Loidl, ed., Trends in Functional Programming 5, pp. 65-78. Intellect, 2006.
- T. Uustalu, V. Vene. Comonadic functional attribute evaluation. In M. van Eekelen, ed., Trends in Functional Programming 6, Intellect, to appear.

Refereed conference papers

- O. Shkaravska. Types with semantics: soundness proof assistant. In A. Momigliano, R. Pollack, eds., Proc. of 3rd ACM SIGPLAN Wksh. on Mechanized Reasoning about Languages with Variable Binding, MERλIN'05 (Tallinn, Sept. 2005), pp. 50-57. ACM Press, 2005.
- T. Uustalu, V. Vene. The essence of dataflow 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 Comput. 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), . 156, n. 1 of Electron. Notes in Theor. Comput. Sci., pp. 151-168. Elsevier, 2006.
- A. Saabas, T. Uustalu. Compositional type systems for stack-based low-level languages. In B. Jay, J. Gudmundsson, eds., Proc. of 12th Computing, Australasian Theory Symp., CATS 2006 (Hobart, Jan. 2006), v. 51 of Confs. in Research and Practice in Inform. Techn., pp. 27-39. Australian Comput. Soc., 2006.
- T. Uustalu, V. Vene. The essence of dataflow programming (full version). In Z. Horváth, ed., Revised Lectures from Central-European Functional Programming School, CEFP 2005 (Budapest, July 2005), Lect. Notes in Comput. Sci., Springer-Verlag, to appear.

Other

- O. Shkaravska. Amortized heap-space analysis for first-order functional programs. In M. van Eekelen, ed., Proc. of 6th Symp. on Trends in Functional Programming, TFP'05 (Tallinn, Sept. 2005), pp. 281-296. Inst. of Cybern., 2005.
- T. Uustalu, V. Vene. Comonadic functional attribute evaluation. In M. van Eekelen, ed., Proc. of 6th Symp. on Trends in Functional Programming, TFP'05 (Tallinn, Sept. 2005), pp. 33-43. Inst. of Cybern., 2005.
- N. Ghani, M. Hamana, T. Uustalu, V. Vene. Representing cyclic structures as nested datatypes. In H. Nilsson, ed., Proc. of 7th Symp. on Trends in Functional Programming, TFP 2006 (Nottingham, Apr. 2006), pp. 173-188. Univ. of Nottingham, 2006.

Edited journal issues / proceedings

- C. McBride, T. Uustalu, eds. Proc. of Wksh. on Mathematically Structured Functional Programming, MSFP 2006 (Kuressaare, July 2006), Electron. Wkshs. in Computing. British Comput. Soc., 2006.

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

- T. Uustalu, talk A compositional natural semantics and Hoare logic for low-level languages (coauthor A. Saabas), NADA dept seminar, KTH, 19 Sept. 2005
- T. Uustalu, talk Partiality is an effect (coauthors T. Altenkirch, V. Capretta), IFIP WG 2.2 Meeting #22, Kalvi, 1-4 Oct. 2005
- V. Vene, talk The essence of dataflow programming (coauthor T. Uustalu), IFIP WG 2.2 Meeting #22, Kalvi, 1.-4 Oct. 2005
- A. Saabas, talk Compositional natural semantics, Hoare logics and type systems for low-level languages (coauthor T. Uustalu), CSL seminar, Dept. of Comput. Engin. and Comput. Sci., Australian Nat Univ, Canberra, 24 Jan. 2006
- T. Uustalu, talk Natural semantics and logics/type systems for low-level languages and program optimizations (coauthor A. Saabas), Dagstuhl-seminar 06281 The Challenge of Software Verification, Dagstuhl, 9-13 July 2006
- T. Uustalu, talk Representing cyclic structures as nested datatypes (coauthors N. Ghani, M. Hamana, V. Vene), IFIP WG 2.8 Meeting #23, Dedham near Boston, 16-21 July 2006

8.17 Bergen

Correctness of Computer Systems We have further 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. Parallel composition has been added to the language, and the type systems have been extended accordingly. Also, the feature of safe deallocation has been added.

Foundational Research Among other things a new translation of first-order logic to coherent logic has been found and the soundness/completeness of a simple proof procedure for coherent logic has been proved.

Proof technology The foundational research described in the previous paragraph facilitates the incorporation of the proof engine of coherent logic in proof assistants such as Coq (Paris-Sud), Isabelle (TU Munich/Cambridge) and others. An experimental CL prover has been coupled to a Coq backend, and some initial experiments with an Isabelle backend have been done.

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. This research has been described in a report that has been accepted by the Workshop on Automated Deduction and Geometry (ADG), with formal publication date in the next project period.

Publications

Refereed conference papers

- H.A. Truong and M.A. Bezem, *Finding resource bounds in the presence of explicit deallocation.* In D.V. Hung and M. Wirsing, editors, *Proceedings ICTAC 2005*, LNCS 3722, pages 227–241, Springer-Verlag, 2005.
- M.A. Bezem and T. Coquand, *Automating Coherent Logic.* In G. Sutcliffe and A. Voronkov, editors, *Proceedings LPAR-12*, LNCS 3835, pages 246–260, Springer-Verlag, Berlin, 2005.
- M.A. Bezem, *On the Undecidability of Coherent Logic.* In A. Middeldorp e.a., editors, *Processes, Terms and Cycles: Steps on the Road to Infinity*, LNCS 3838, pages 6–13, Springer-Verlag, Berlin, 2005.
- M. Walicki, M.A. Bezem and W. Szajnkenig. *A Strongly Complete Logic of Dense Time Intervals.* In T. Agotnes and N. Alechina, editors, *Proceedings ESSLLI Workshop on Logics for Resource Bounded Agents*, Malaga, Spain, August 2006.

Talks

- M. Bezem, *On the mechanization of the proof of Hessenberg's Theorem*, Orsay, 30.09.2006.

- H.A. Truong, *Finding resource bounds in the presence of explicit deallocation*, ICTAC, Hanoi, 19.10.2005.
- H.A. Truong, *Type Systems for Resource Use of Component Software*, Types, Nottingham, 20.04.2006.
- M. Bezem, *Automating Coherent Logic*, LPAR, Jamaica, 04.12.2006.
- M. Bezem, *Decidability and completeness of sequent logics*, Logic Seminar, Oslo, 27.04.2006.
- M. Bezem, *A Strongly Complete Logic of Dense Time Intervals*, ESSLLI, Malaga, 08.08.2006.

Dissertations

- H.A. Truong, *Type Systems for Resource Use of Component Software*, PhD dissertation, Bergen University, 15.05.2006.

8.18 Helsinki

The small Helsinki subsite has continued work on proof theory and its applications. Most important among the latter are the applications to modal logic and related systems such as temporal logic by Sara Negri. A second area of application is in proof systems for mathematical theories, including lattice theory and elementary geometry (projective and affine geometry). By methods developed in Helsinki, it has become possible to give, in principle, a complete combinatorial analysis of formal proofs with the axioms of these theories. These methods have further led to positive results on the decision problem as restricted to derivations with the axioms. The geometric theories mentioned are of special relevance for the Types project, because of the implementation work that is going on in several sites of Types.

Publications

Refereed journal papers

- S. Negri, Proof analysis in modal logic, J. Philosophical Logic, vol. 34, 2005, pp. 507–544.
- S. Negri, Permutability of rules in linear lattices, J. Univ. Comp. Sci., vol. 11, 2005.
- R.Dyckhoff and S. Negri, Decision methods for linearly ordered Heyting algebras, Arch. Math. Logic, vol. 45, 2006, pp. 411–422.
- J. von Plato, Normal derivability in modal logic, Math. Logic. Quarterly, vol. 51, 2005, pp. 632–638.
- J. von Plato, A constructive approach to Sylvester's conjecture, J. Univ. Comp. Sci., vol. 11, 2005, pp. 2165–2178.

Refereed conference papers

- S. Negri and J. von Plato, The duality of classical and constructive notions and proofs, in L. Crosilla and P. Schuster, eds, From Sets and Types to Topology and Analysis, pp. 149–161, Oxford U.P. 2005.

8.19 Minho

Foundational Research J. Espírito Santo, M.J. Frade and L. Pinto continued work on the generalised multiary lambda-calculus LambdaJm. In particular, they performed a combined study of reduction and permutative conversions. They identified various classes of combined normal forms, some of which correspond to well-know classes of derivations in sequent calculus and some of which are new classes. These ideas, alongside with a computational explanation for the variety of combined normal forms obtained, are to be presented in *RTA'06*.

In collaboration with T. Uustalu (Tallinn), L. Pinto carried on their work on propositional bi-intuitionistic logic, aiming at improving the decision method they established for finding proofs or counter-models in the logic. This work was presented at the meeting *Days in Logic'06* and a paper on it is under preparation.

Correctness of Computer Systems With T. Uustalu and A. Saabas (Tallinn), M.J. Frade initiated work on the development of a foundational approach to classical dataflow analysis, a program logic for speaking about transition traces, into which the type systems for particular analysis can be embedded.

Publications

Refereed conference papers

- J. Espírito Santo, M.J. Frade and L.Pinto, *Structural proof theory as rewriting*, RTA'06, LNCS 4098, Springer (2006)

Talks

- J. Espírito Santo, *Issues in a calculus of multiary sequent terms*, talk at Days in Logic'06, Coimbra, January 2006 (joint work with M.J. Frade and L. Pinto).
- J. Espírito Santo, *Simple proofs of cut-elimination*, talk at the Types Annual Meeting, Nottingham, April 2006.
- L. Pinto, *Combined normal forms in sequent calculus*, talk at the Types Annual Meeting, Nottingham, April 2006 (joint work with J. Espírito Santo and M.J. Frade).

8.20 Novi Sad – Belgrade

Foundational Research We investigate different aspects of the role of union and intersection types in the setting of classical lambda calculus. Type preservation under reduction (subject reduction) turns out to be a rather complex problem. We continue research in categorial proof theory. Another line of research is the separability of terms in different settings of classical lambda calculus. Also, we develop an intersection types system for sequent lambda calculus. Our goal is to characterise strong normalisation in this system.

Formal Mathematics and Mathematics Education Novi Sad has started a bilateral project with Mathematics Department, University of Maribor, Slovenia, Distance learning in the area of computer supported mathematical education. Within this project it is forseen to involve formal methods developed in the Types project.

Publications

Refereed journal papers

- K.Došen, Z.Petrić *Negation and Involutive Adjunction, We Will Show Them*, Sergei N. Artmov, Howard Barringer, Artur S. d'Avila Garcez, Lus C. Lamb, John Woods (Eds.), Essays in Honour of Dov Gabbay on his 60th Birthday, vol. 1, 577-585 (2005), College Publications, London (available at: http://arXiv.org/math.LO/0506302).

- K.Došen, Z.Petrić, Kovijanić *A new proof of the faithfulness of Brauer's representation of Temperley-Lieb algebras*, to appear in the International Journalof Algebra and Computation (available at: http://arXiv.org/math.GT/0204214).

- K.Došen, Z.Petrić *Coherence for Star-Autonomous Categories*, Annals of Pure and Applied Logic 141, 225-242 (2006). (available at: http://arXiv.org/math.CT/0503306).

- K.Došen, Z.Petrić *Associativity as Commutativity*, The Journal of Symbolic Logic, vol. 71, 1, 217-226 (2006). (available at: http://arXiv.org/math.CT/0506600).

- K.Došen, Z.Petrić *Coherence of Proof-Net Categories*, Publications de l' Institut Mathematique, tome 78 (92), 1-33 (2005), (available at: http://arXiv.org/math.CT/0503301).

Refereed conference papers

- D.Dougherty, S.Ghilezan, P.Lescanne, S.Likavec *Strong normalization of the dual classical sequent calculus* The 12th International Conference on Logic Programming and Artificial Reasoning LPAR'2005, Lecture Notes in Computer Science 3835 169-183 (2005).

- S.Likavec, P.Lescanne *On untyped Curien-Herbelin calculus* 1st workshop on Classical Logic and Computation (CLaC'06) (2006).

8.21 Savoie

The Logic team of the LAMA wii have two new researchers next year: Guillaume Theyssier (which was already ATER this year) and Pierre Hyvernat. Both will work on thematic connected to the type project.

P. Thevenon and F. Ruyer are finishing there phd. thesis (both defenses will happen next fall).

Foundational Research K. Nour, G. Theysser and C. Raffalli works on the probability of normalization in lambda-calculus. They have a candidate counter-example for a 0-1 law (which would mean that all lambda-terms have probability 0 or 1 to normalize when we choose randomly the redex). We are also considering a 0-1 law theorem in simply typed lambda-calculus with fix-point combinator. However, both problems seems very hard from the point of vue of probability.

K. Nour went to Edinburgh for 6 month and started to work with F. Kamareddine aud J. Wells on type-checking algorithm for lambda-calculus with intersection types. This algorithm could be used to solve some problems with typing of modules in ML-like languages. Two publications are in preparation.

Proof technology P. Thevenon is working in the demonat (DEMOnstration in NATural languages) project and developed in is phd a new algorithm for lambda-calculus with two arrows (linear and non linear) which shall be used in the current work of P. DeGroote about ACG (abstract categorical grammar). Another part of P. Thevenon's phd is devoted to a new automated prover for PhoX based on the inverse method and which is optimized to prove the "easy" statement generated by the linguistic analysis of natural language. The prover is actually implemented and tested.

F. Ruyer developed using the System ST framework of C. Raffalli the tool to encode complex programming languages. The completeness of system ST ensures no limitation in theory. F. Ruyer demonstrates that it can be used in practice, by fully specifying and proving inside System ST an ML-like language with modules, abstract types and abstract values. This language also allow to specify and prove programs. Moreover, most of the proof were machine checked using an encoding of system ST in PhoX (which is rather heavy). This means that a new proof assistant implementing directly system ST would be a very good tool to design correct computer languages.

C. Raffalli is starting to develop a new proof assistant based on an ML like language with very strict typing. Pierre Hyvernat and a new phd. Student will probably also work on this project next year.

Publications

Refereed journal papers

- K. Nour, R. David, *Why the usual candidates of reducibility do not work for the symetric lambda-mu-calculus*, to appear in Electronic Notes in Theoretical Computer Science, 2005

- K. Nour, K. Saber, *A semantics of realisability for the classical propositional natural deduction*, to appear in Electronic Notes in Theoretical Computer Science, 2005

Refereed conference papers

- K. Nour, R. David, *Arithmetical proofs of strong normalization results for the symmetric lambda-mu-calculus* TLCA 2005, LNCS 3461, pp. 162-178, 2005
- C. Raffalli, Paul RoziÃÍre, *PhoX*, The seventeen provers of the World, Freek Wiedijk (editor), LNAI 3600 pages 67-71.

8.22 Swansea

Correctness of Computer Systems Markus Roggenbach, Andy Gimblett have in collaboration with Holger Schlingloff (Berlin) formalised in the formal specification language CSP-CASL major parts of the electronic payment system EP2, a new international standard for which first terminals are just beeing installed.

Foundational Research Markus Roggenbach (Swansea) has worked out the mathematical foundations of two reactive extensions of the algebraic specification language CASL: CSP-CASL adds the process algebra CSP [50], while CoCASL offers additional co-algebraic mechanism for specification [85].

Anton Setzer (Swansea) has developed concepts for formalising concepts from object-oriented programming in dependent type theory [99]. This is a first step towards the development of an object-oriented programming language based on dependent types.

Anton Setzer, Ulrich Berger and Rose H. Abdul Rauf [2, 94] have developed a translation of an extension of C++ by functional concepts into ordinary C++. They have shown the correctness of this translation w.r.t. the typed λ-calculus. Furthermore they have shown how to represent lazy concepts in C++.

Ulrich Berger has developed a domain-theoretic method for proving strong normalisation of lambda-calculi and higher type rewrite system. The method is able to prove termination of recursion schemes that occur in computational interpretations of classical second-order arithmetic.

Monika Seisenberger is doing research in the formalisation, verification and synthesis of security protocols.

Markus Michelbrink has proved a final coalgebra theorem in intensional type theory. His work shows that coalgebraic concepts necessary for the implementation of interaction in dependent type theory can be formulated in a predicative framework given by e.g. Martin-Löf Type Theory augmented with some weak instances of induction recursion.

Markus Michelbrink has developed a generalised form of interfaces. The generalisation uncovers the relation of interfaces to games.

Markus Michelbrink and Magne Haveraaen have developed a translation of the simply typed lambda calculus into C++-templates.

Formal Mathematics and Mathematics Education Anton Setzer was teaching a combined third year and MSc module on "Interactive Theorem Proving". This module is mainly an introduction to the theorem prover Agda developed mainly by the Chalmers site.

Ulrich Berger was teaching the modules "Functional Programming" (second year) and "Programming with Abstract data Types" (third year). The former contained achapter on simple type theories, the latter contained a chapter on the Formulas-as-Types paradigm and discussed methods of synthesising programs from formal proofs.

Proof technology Markus Roggenbach has extended CSP-Prover by a package for deadlock analysis.Furthermore, for the CSP stable failures model a complete axiomatic semantics has been developed and implemented in CSP-Prover.

Andy Gimblett and Markus Roggenbach have been working on tool support for CSP-CASL – in particular a parser/static analyser to be integrated with the HETS toolset for CASL-related languages (in Haskell).

Publications

Refereed journal papers

- U. Berger and P. Oliva. Modified bar recursion. *Mathematical Structures in Computer Science*, 16:163–183, 2006
- Markus Roggenbach. CSP-CASL — a new integration of process algebra and algebraic specification. *Theoretical Computer Science*, 354:42 – 71, 2006

Refereed papers in book

- Ulrich Berger and Monika Seisenberger. Applications of inductive definitions and choice principles to program synthesis. In *From Sets and Types to Topology and Analysis Towards practicable foundations for constructive mathematics*, volume 48 of *Oxford Logic Guides*, pages 137–148. Oxford University Press, 2005

Refereed conference papers

- Rose H. Abdul Rauf, Ulrich Berger, and Anton Setzer. Functional concepts in C++. In *Conference Proceedings of TFP 2006.*, 2006
- Anton Setzer. Object-oriented programming in dependent type theory. In *Conference Proceedings of TFP 2006*, 2006
- Yoshi Isobe, Markus Roggenbach, and Stefan Gruner. Towards the verification of systolic arrays. In *Proceedings of FOSE 2005*, Japanese Lecture Notes Series, pages 257–266. Kindai-kagaku-sha, 2005
- Andy Gimblett, Markus Roggenbach, and Holger Schlingloff. Towards a formal specification of an electronic payment system in CSP-CASL. In *Recent Trends in Algebraic Development Techniques. Proceedings of WADT*

2004, volume 3423 of *Lecture Notes in Computer Science*, pages 61–78. Springer-Verlag, 2005

- Christoph Lueth, Markus Roggenbach, and Lutz Schroeder. CCC – the CASL consistency checker. In *Recent Trends in Algebraic Development Techniques. Proceedings of WADT 2004*, volume 3423 of *Lecture Notes in Computer Science*, pages 94–105. Springer-Verlag, 2005

- Markus Michelbrink and Anton Setzer. State-dependent IO-monads in type theory. In *Proceedings of the 10th Conference on Category Theory in Computer Science (CTCS 2004)*, volume 122 of *Electronic Notes in Theoretical Computer Science*, pages 127–146. Elsevier, 2005

- Rose Abdul Rauf. Integrating functional programming into C++: Implementation and verification. In *Logical Approaches to Computational Barriers. Second Conference on Computability in Europe, CiE 2006, Swansea, UK*, volume # CSR 7-200 of *Department of Computer Science, University of Wales Swansea, Report Series*, pages 2–11, 2006

Talks

- Ulrich Berger *Denotational semantics - what and why?* Seminar talk, Swansea University, March 2006.

- Ulrich Berger *A domain-theoretic strong normalisation proof for higher type rewrite systems.* Oberwolfach workshop "Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics", Oberwolfach, Germany, 2005. (Participation by invitation only).

- Markus Michelbrink: *Containers, Interfaces, Games.* Cambridge Logic and Semantics Seminar 2005. Computer Laboratory. University of Cambridge. Cambridge, November 2005

- Markus Roggenbach: *Deadlock Analysis with CSP-Prover.* 2 November 2006, Colloquium, Dept. of Mathematics and Computer Science, University of Bremen, Germany.

- Markus Roggenbach: *CSP-CASL: Semantics, Application, Tools.* June 2006, IFIP WG 1.3 meeting, Namur, Belgium.

- Markus Roggenbach: *Structured CSP - a Process Algebra as an Institution.* June 2006, WADT 2006, Namur, Belgium.

- Monika Seisenberger: *Programm extraction from classical proofs in the Minlog system.* Workshop CL&C 2006 - Classical Logic and Computation, San Servolo, Venice, July 2006.

- Anton Setzer: *Inductive-recursive definitions.* Seminar Talks, Proof theory, Complexity and Verification Seminar, Department of Comptuter Science, Swansea, 2006. (2 sessions).

- Anton Setzer: *Inductive-recursive definitions.* Seminar Talk, National Institute of Informatics, Tokyo, Japan, 2005.

- Anton Setzer: *Ordinal Systems.* Seminar Talk, Graduate School of Science and Technology, Kobe, Japan, 2005.
- Anton Setzer: *Towards a more algebraic treatment of ordinal notation systems.* Oberwolfach workshop "Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics", Oberwolfach, Germany, 2005. (Participation by invitation only).
- Anton Setzer: *Towards a more algebraic treatment of ordinal notation systems.* PCC 2005, Lissabon, Portugal.
- Anton Setzer: *Inductive-recursive definitions and generic programming.* Seminar Talk, University of Leicester, England, 2005.
- Anton Setzer: *Indexed inductive-recursive definitions.* Seminar Talk, Dept. of Mathematics, University of Munich, 2005.
- Anton Setzer: *Inductive-recursive definitions and generic programming.* Seminar Talk, University of Bath, England, 2005.
- Anton Setzer: *Ordinal Systems.* Seminar Talk, Dept. of Computer Science, University of Wales Swansea, Swansea, Wales, 2005.

8.23 Birmingham

Correctness of Computer Systems

- Ritter, Adetoye and Ryan are developing type systems to characterise information flow. A policy framework for specifying the degree of permissible information flow has been developed.
- Ryan and Mukhamedov have improved protocols for allowing users of a service to remain anonymous, while providing the possibility that the service owner can break the anonymity in exceptional circumstances, such as to assist in a criminal investigation. They also show that a certain protocol for multi-party contract signing which is optimistic in the sense that the trusted party is only contacted in the case of failure is inherently unfair and hence seriously flawed.

Foundational Research and Proof Technology

- Pym and Ritter develop a games semantics for classical proofs which gives rise to a full completeness result with respect to Pym and Führmann's classical categories. This games semantics also provides a model for well-known proof search strategies like resolution.

Publications

Refereed conference papers

- A. Mukhamedov and M. Ryan. Resolve-Impossibility for a Contract-Signing Protocol. Proc. of 19th Computer Security Foundations Workshop. IEEE Compuer Society Press. 2006.
- A. Mukhamedov and M. Ryan. On Anonymity with Identity Escrow. Proceedings of the Third International Workshop on Formal Aspects in Security and Trust, LNCS3866, pp 235–243. 2005.

8.24 Nottingham

Foundational Research

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

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

Continuous Functions on Final Coalgebras [Ghani and Hancock] We have developed a presentation of 'live' processes which consume and produce infinite data structures, generalising from streams to arbitrary containers. The processes are themselves represented via datatypes which are mutually coinductive (guaranteeing that writing will eventually start) and inductive (guaranteeing that reading will evantually stop).

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

Publications

Refereed journal papers

- Peter Hancock* and Pierre Hyvernat, *Programming interfaces and basic topology* in Annals of Pure and Applied Logic, Vol 136, Jan 2006.
- Conor McBride* and Ross Paterson, *Applicative Programming with Effects* to appear in Journal of Functional Programming, 2006.

Refereed conference papers

- Thorsten Altenkirch* and James Chapman*, *Tait in one big step*, in proceedings of the Types Small Workshop on Mathematically Structured Functional Programming, Kuressaare, Estonia, July 2006.
- James Chapman*, Thorsten Altenkirch* and Conor McBride*. *Epigram Reloaded: A Standalone Typechecker for ETT*, revised version in post-proceedings of TFP 2005.
- Neil Ghani*, Peter Hancock* and Dirk Pattinson
  Continuous Functions on Final Coalgebras
  in Proceeding of the Workshop on Coalgebraic Methods in Computer Science
- Catherine Hope* and Graham Hutton*
  Compact Fusion
  in proceedings of the Types Small Workshop on Mathematically Structured Functional Programming, Kuressaare, Estonia, July 2006.

Talks

- Thorsten Altenkirch
  - April 2006, Swansea, BCTCS talk, 'Stop thinking about bottoms when writing programs!'
  - June 2006, Cambridge, seminar, 'Beauty in the Beast: Functional specifications of effects'
  - June 2006 Chiemsee, workshop Trends in Constructive Mathematics, 'Should Extensional Type Theory be considered harmful?'
- Neil Ghani
  - November 2005, Swansea, seminar, 'Containers 2'
- Peter Hancock
  - December 2005, Cambridge, seminar, 'Dependently typed programming and imperative interfaces'
  - June 2006 Chiemsee, workshop Trends in Constructive Mathematics, 'Representations of continuous functions on final coalgebras'

- Conor McBride
  - October 2005, IFIP WG2.8, Kalvi, Estonia, talk, 'Erasing the static parts of dependently typed programs'
  - March 2006, IFIP WG2.1, Antalya, Turkey, talks, 'Datatypes from Containers', 'Indexed Containers'
  - June 2006, Cambridge, seminar 'Observational Type Theory'

8.25 Sheffield

At Sheffield, Types funding has been instrumental in bringing together a new group of theoreticians to work on the theory and applications of Type Theory. The Types-active personnel at Sheffield currently include: Simon Foster, Andrew Hughes, Edwin Lewis-Kelham, and Mike Stannett (subsite co-ordinator).

Application of types to timed mobile process calculus Typed Nomadic Time (TNT) is a new Timed Mobile Process Calculus being developed by Andrew Hughes as part of his PhD work within the Department. He is attempting to model the addition of mobility constructs to CaSE (a timed process calculus developed at Sheffield), by adding ideas from research on the Ambient Calculus. The constructions are very powerful, and Andrew has found the addition of a novel type system to be useful in controlling the complexity of the relevant descriptions and the behaviours of the processes.

Type Theory in Semantic Web Services This work is being carried out by Simon Foster as part of his PhD work within the Department. Simon is using the CaSE timed calculus to generate a consistent model of semantic web services, in collaboration with leading researchers in the field at the Knowledge Media Institute (KMi) at the Open University. The representations are highly complex, and it is becoming clear that behavioural types will play an important role in controlling the complexity of these representations. In particular, Simon is investigating the applicability of TNT (described above) to the modelling and implementation of semantic web services.

Multi-level Lax Logic This work, carried out by Edwin Lewis-Kelham for his PhD, is now essentially complete; Ed has recently completed corrections to his thesis work. Originally supervised by Matt Fairtlough, Edwin has benefited from detailed conversations with Michael Mendler (Bamberg), and is now supervised by Mike Stannett. Edwin has developed a novel extension to the standard theory of Lax Logic, in which it is possible to express the idea that p_1 is a proof that p_2 is a proof that $\ldots p_n$ is a proof of the proposition P, where each proof level includes its own (unknown) constraint term. By applying the techniques developed by Ed in his thesis work, it is possible to extract constraints one at a time, thereby avoiding the combinatorial explosion that would normally arise if all constraints were considered to exist 'on the same level'. This work was presented at the Types 2006 meeting.

Lax Types This work is being carried out by Mike Stannett, in collaboration with Michael Mendler (Bamberg). Lax Logic is typically used to express specifications that can be only be satisfied subject to some (unknown) constraint; by applying Lax Logical techniques, the unknown constraints can be identified semi-automatically. During a talk by Simon Peyton-Jones on Generalised Abstract Data Types (GADTs) at the Types 2006 meeting, Mendler and Stannett realised that these techniques might profitably be re-cast in terms of type theory to give a new Theory of Lax Types. These are expected to have wide relevance to the theory of functional programming languages; they can, in particular, be used to give a succinct and novel analysis of GADTs.

Publications

Talks

- Edwin Lewis-Kelham and Mike Stannett, *Multi-level Lax Logic*, Types 2006, Nottingham, April 2006.

Dissertations

- Edwin Lewis-Kelham, *Multi-level Lax Logic*, PhD Thesis, Sheffield University, Department of Computer Science (2005, 2006).

8.26 Stockholm – Uppsala

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

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

Category theory and dependent types Work on quasi-equational theories and initial models of such inside cartesian categories has been carried out by E. Palmgren and S. Vickers. These are related to Cartmell's generalised algebraic theories (under which Martin-Löf type theory fall). PhD-student Olov Wilander is currently working on proof-theoretic aspects of such theories.

The group has been joined by post-doc Richard Garner from Cambridge who is working on categorical models of intensional type theory.

Publications

Refereed journal papers

- P. Martin-Löf. 100 years of Zermelo's axiom of choice: What was the problem with it? The Computer Journal, vol 49, No.3, 2006.

- E. Palmgren. Internalising the modified realisability in constructive type theory. *Logical Methods in Computer Science.* vol. 1, iss. 2, 2005. (Publ. Oct 5, 2005.)
- E. Palmgren. Quotient spaces and coequalisers in formal topology. *Journal of Universal Computer Science,* 11 (2005), 1996-2007. (Publ. Dec 2005)
- E. Palmgren and P. Schuster. Apartness and formal topology. *New Zealand Journal of Mathematics,* 34(2005), 1-8.
- E. Palmgren. Maximal and partial points in formal spaces. *Annals of Pure of Applied Logic,* 137 (2006), 291 - 298.
- E. Palmgren. Regular universes and formal spaces. *Annals of Pure of Applied Logic,* 137 (2006), 299 - 316.
- Hajime Ishihara and E. Palmgren. Quotient topologies in constructive set theory and type theory. *Annals of Pure of Applied Logic,* 141 (2006), 257 - 265.
- Peter Aczel, Laura Crosilla, Hajime Ishihara, Erik Palmgren, Peter Schuster) Binary refinement implies discrete exponentiation. *Studia Logica,* accepted for publication.
- J. Carlström. A constructive version of Birkhoff's theorem. submitted for publication.
- Erik Palmgren and Steve J. Vickers. Partial Horn logic and cartesian logic. Submitted for publication.

Refereed conference papers

- F. Dahlgren. Partial Continuous Functions and Admissible Domain Representations (extended abstract) (Logical Approaches to Computational Barriers, Lecture Notes in Computer Science vol. 3988, 2006.)
- E. Palmgren. Predicativity problems in point-free topology. In: V. Stoltenberg-Hansen and J. Väänänen eds. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, held in Helsinki, Finland, August 14-20, 2003, Lecture Notes in Logic 24, ASL, AK Peters Ltd, 2006.
- E. Palmgren. From intuitionistic topology to formal topology: on the foundation of homotopy theory. Submitted for publication.

Talks

- J. Brage. A BHK semantics that justifies classical logic. *Types Meeting,* Nottingham 18-21 April 2006.
- J. Carlström. A constructive version of Birkhoff's theorem. *Trends in Constructive Mathematics,* Frauenwörth 19-23 June 2006, Germany.

- F. Dahlgren. Effective Distribution Theory. *Trends in Constructive Mathematics,* Frauenwörth 19-23 June 2006, Germany.
- F. Dahlgren. Partial continuous functions and admissible domain representations. *Computability in Europe,* Swansea, 30 June - 5 July, 2006
- J. Granström. Eager evaluation in type theory. *Spring school in Logic in Cmputer Science,* Fischbachau 20-23 April 2006.
- P. Martin-Löf. The two layers of logic. *The Seventeenth Annual Gödel Lecture, Annual Meeting of the Association for Symbolic Logic, Montreal,* 17-21 May 2006.
- P. Martin-Löf. The type-theoretic logic of existence. *Les théories modernes des types,* Paris, 24-25 March 2006.
- P. Martin-Löf. Logical Necessity. *Workshop on Philosophy of Mathematics Today.* Pisa, 23-27 January, 2006.
- E. Palmgren. Locally compact metric spaces as formal topologies. *Trends in Constructive Mathematics,* Frauenwörth 19-23 June 2006, Germany.
- E. Palmgren. Constructive problems in elementary homotopy theory. *Small Types workshop: Constructive analysis, types and exact real numbers.* Nijmegen, 3-4 October 2005.
- E. Palmgren. Internalising the modified realisability in constructive type theory. *Types Meeting,* Nottingham 18-21 April 2006.
- E. Palmgren. Intuitionism, Bishop's constructivism and point-free thinking. Plenary Lecture. *Logic Colloquium '06.* Nijmegen, 27 July - 2 August, 2006.

Dissertations

- G. Hamrin. *Effective Domains and Effective Domain Representations.* Dissertation in Mathematics. Uppsala University 2005. Defended 29 september 2005.
- J. Brage. *A Natural Interpretation of Classical Proofs.* Dissertation in Mathematics. University of Stockholm 2006. Defended 6 April 2006.

8.27 Toulouse

Foundational Research In joint work of F. Barral, D. Chemouil and S. Soloviev (and a paper by Barral and Soloviev) results on extensions of rewrite systems preserving strong normalization and Church-Rosser property were obtained. This also contributes to the correctness of computer systems (extended systems can be used for verification).

Ralph Matthes moved from LMU Munich to Toulouse. After having worked over years on higher-order impredicative programming, he finally moved into dependently-typed programming and verification. In particular, his contribution

at the small Types workshop MSFP in Tallinn opens the way for verification of programs involving truly nested datatypes in intensional type theory. All of his published work started in Toulouse has been verified in the Coq theorem prover.

Formal Mathematics and Mathematics Education In joint work of L. Mehats and S. Soloviev (Coherence in SMCC's and equivalences on derivations in IMLL with unit. Submitted to Annals of Pure and Applied Logics, 82 pp.) was shown how the proof-theoretical methods can be used to obtain coherence theorems and describe in fine details the equivalence relations on derivations generated by interpretations in non-free categorical models. This work also was presented in L. Mehats PhD thesis (december 2005). This work also contributes to the domains of proof technology. At the moment another PhD student is working on the computer algebra algorithms based on this work in official collaboration with the Mathematical Institute of the University of Toulouse.

Publications

Dissertations

- Laurent Mehats. Theorie de la Preuve des Categories Monoidales Symetriques Fermees: coherence et equivalences de derivations. PhD thesis (december 2005, Toulouse).

Refereed Journal Papers

- Sergei Soloviev. Foreword. Special Issue on Isomorphisms of Types, Mathematical Structures in Computer Science, v. 15, N 5 (2005), pp.821–825.
- Mehats L., Soloviev S. Permutability of Inferences and Categorical Equivalence of Derivations in IMLL. (English) – Vestnik Tverskogo Gosudarstvennogo Universiteta (Communications of the Tver State University, Russia), 6(12), 2005, pp. 27–44.

Refereed Conference Papers

- O. Antonova, S. Soloviev. About Wittgenstein's mathematical epistemology. Accepted for publication in pre-proceedings of 29-th annual symposium of the ALWS, Austria, Kirchberg am Wechsel, 6–12.08.2006. 5pp.
- Ralph Matthes. Stabilization—An Alternative to Double-Negation Translation for Classical Natural Deduction. Proceedings of the Logic Colloquium 2003, pp 167–199. 2006.
- Ralph Matthes. A Datastructure for Iterated Powers. Mathematics of Program construction. Proceedings. LNCS4014, pp 299–315, 2006.

Refereed Workshop Papers

- Ralph Matthes. Verification of programs on truly nested datatypes in intensional type theory. Workshop on Mathematically Structured Functional Programming (MSFP '06), Kuressaare, Estonia, 02/07/2006. 2006.

Talks

- Ralph Matthes. Generic definition and proof in intensional type theory of map fusion for nested datatypes. Spring School on Data-Generic Programming (April 2006), Nottingham, UK.

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.

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

- 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).

- There has been a press release, see `http://www.uib.no/info/dr_grad/2006/Truong_Hoang.html` on the occasion of the PhD graduation of H.A. Truong. Truong was subsequently interviewed by Aftenposten, a major

norwegian newspaper. The interview with Aftenposten appeared in the Friday supplement of 26.05.2006.

- Barendregt and Wiedijk has written a popular science article for high school students in the Netherlands (Bewijzen: romantisch of cool, Euclides, 2006. ('Proofs: romantic or cool')).
- Wiedijk has written "On the usefulness of formal methods" in the Newsletter of the NVTI (Dutch union for theoretical computer science), 14-23, 2006.
- IoC Tallinn was visible in the press (magazines, radio) in connection to TFP/ICFP/GPCE 2005 (incl. MERλIN 2005) and MPC/AMAST 2006 (incl. MSFP 2006). MERλIN 2005 and MSFP 2006 were Types-affiliated workshops.

A.3 Publishable results

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