IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2011

Project-Team TYPICAL

Types, Logic and computing

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Programs, Verification and Proofs

Table of contents

Project-Team TYPICAL

Keywords: Interactive Theorem Proving, Formal Methods, Safety, Proofs Of Programs, Type Systems

The TypiCal team is hosted by the Laboratoire d'Informatique de l'École Polytechnique (LIX).

1. Members

Research Scientists
Benjamin Werner [Senior ResearcherTeam Leader, HdR]
Bruno Barras [Junior Researcher]
Germain Faure [Junior Researcher]
Assia Mahboubi [Junior Researcher]

Faculty Member
Gilles Dowek [Professor, École Polytechnique, HdR]

Technical Staff
Jean-Marc Notin [Research Engineer]

PhD Students
Alexis Bernadet [PhD student]
Bruno Bernardo [PhD student]
Mathieu Boespflug [PhD student until January 2011]
Cyril Cohen [PhD student]
Chantal Keller [PhD student]
Victor Magron [PhD student]
Pierre Néron [PhD student]
Arnaud Spiwack [PhD student until March 2011]
Qian Wang [from January 2011, Tsinghua University scholarship]

Post-Doctoral Fellows
Revantha Ramanayake [ANR Psi]
Enrico Tassi [ANR Paral-ITP]

Administrative Assistant
Valérie Lecomte [Assistant]

2. Overall Objectives

2.1. Presentation

Mathematics is among the many human activities that have been transformed by the invention of the computer and its broad diffusion in the second half of the 20^{th} century. Mathematicians could, from then on, use a tool allowing to carry out operations that were too long or too tedious to be executed by hand. Like the use of the telescope in astronomy, the use of the computer opened many new prospects in mathematics. One of these prospects is the use of *proof assistants*, *i.e.* computer programs which perform some operations on mathematical proofs. The goal of the research developed in the TypiCal project-team is to develop such *proof assistants*. The main effort of the project-team is to contribute to the development of proof assistants in general and of the Coq system in particular, which has an important community of users in industry and in academia. However, we believe that the development of a proof assistant cannot be accomplished without a joint reflection about the structure of mathematical proofs and about the use of proof assistants in various applicative domains. We also believe that proof assistants should take benefit of the use of automated deduction

tools. Thus, the questions addressed in the team range from questions related to the Coq system, such as “What will be the features of the next version of Coq?”, to more theoretical questions of logic, such as “What is a proof?” and more applied ones, such as “How can I delegate part of the proof search to automated tools?” or “How can we use a proof assistant to check whether a protocol is free of deadlocks?”.

3. Scientific Foundations

3.1. Logical formalisms

A proof system implements a logical formalism in the way a compiler implements a programming language. Similarly, the choice of the formalism is crucial for the success of the proof system. One of the main line of research of the team is to study or invent type theories that are well-adapted to the formalization of mathematics. For instance a crucial property of a proof system is its correctness, hence the importance of the study of the models of the meta-theory of the Coq proof assistant. An other issue is the interoperability of the various proof systems used to formalize mathematics in the world-wide community of users of proof assistants, and the design of a system which could serve as a back-end to front-end implementing various formalisms and proof languages.

3.2. Libraries of formalized mathematics

It is well known that advanced mathematics can play a crucial role in the design and correctness of sophisticated and sometimes critical software. In some cases, using a proof system is the only option to mechanize the correctness of such programs; this can require the formalization of a wide variety of mathematical theories, and a careful design of these formal libraries for them to be maintainable, combinable and reusable. Furthermore, the ability to formalize advanced contemporary mathematics is still a form of ultimate quality tests for proof systems, and also a way to gain visibility. One of our objectives is to make modern and large pieces of mathematics available as usable formal libraries. Recent examples of complex proofs (Four Color Theorem, Kepler conjecture, classification of finite groups, Fermat theorem) challenge the way the mathematical literature is refereed and published. We think that the development of these formal libraries of mathematics may also change the way certain mathematical result become accepted as theorems. Crafting large bodies of formalized mathematics is a challenging task. These libraries obey similar requirements as software : modularity and usability stem from appropriate data-structures, design patterns and corpus of lemmas. But the appropriate methodology leading to the relevant solutions is often far from obvious, and this is where research has to be done and know-how has to be gained. Up to recently, formal developments were seldom collaborative and rarely benefitted from reusable previous work. The maturity of proof assistants is now sufficient to envision a more modern conception of formal software, as required by large scale verification projects like T. Hales’ proof of the Kepler conjecture or the Feit-Thompson theorem. Several members of the TypiCal team are committed in such big formalization projects, or in more specific but related side projects.

3.3. Proof search and automated decision procedures

Interactive proof assistants provide a very expressive logical formalism, rich enough to allow extremely precise descriptions of complex objects like the meta theory of a programming language, a model of C compiler, or the proof of the Four Color Theorem. This description includes logical statements of the properties required by the objects of interest but also their formal proofs, checked by the merciless proof-checker of the system, which should be a small hence trusted piece of code. These systems provide the highest formal guarantee, for instance, of the correctness with respect to the mathematical specification of a code.

Proof-search is a central issue in such a formalization of mathematics. It is also a common aspect of automated reasoning and high-level programming paradigms such as Logic programming. However specific applications commonly involve specific logics or theories, like for instance linear arithmetic. Whether or not such a logical framework can express these at all, it is unlikely that its generic proof-search mechanisms can replace the methods that are specific to a logic or theory. Either because this specific domain lies outside the reach of generic proof-search or simply because generic proof-search is less efficient therein than a purpose-made procedure (typically a decision procedure).

But to enlarge the scope where a specific method applies, one can combine both generic proof search mechanisms with specific methods. We hence investigate how to craft formal proof producing decision procedures in the context of an interactive proof assistant. This activity includes understanding the impact of proof-search mechanism (polarization, focusing, etc.), the implementation of efficient connections between domain specific automated decision procedures (SMT solvers, polynomial optimization tools, etc.) with a proof assistant, and the combination of these two aspects in the design a unique logical framework where a generic notion of proof-search could serve each of the above purposes.

4. Application Domains

4.1. Certified decision procedures

Roughly in the last ten years, proof systems have enjoyed a wider and wider audience, having been used by a growing number of researchers and teams for a growing number of applications. We can list a dozen of INRIA teams who have used Coq in an important way. We can also list the various application fields. It comes as no surprise that these fields are often parts of the genuine activities of other related INRIA teams and appear in more detail in their own reports; among others:

- Computer security: from the formalization of security properties of protocols, to the analysis of cryptographic primitives, through questions of privacy.
- Embedded software, with a growing emphasis on real-time, reactive, software.
- Computer arithmetic: certifying the correctness of the implementation of numerical functions, possibly with explicit rounding errors.
- Formally certified automatic demonstration techniques (like SAT/SMT solvers) either for more trustworthy automatic tools, or to use the latter as formal proof techniques.

4.2. Formalized mathematics

The use of computing power has dramatically increased for the past decades, in all fields of human activity, including most branches of sciences, causing a general need for reliable computing. It also often lies the base for new interdisciplinary interactions. This is also true for so called pure mathematics. One can remark that Thomas Hales' proof of Kepler's conjecture, which is an undoubted result of pure mathematics, relies on computations in order to establish thousands of semi-numerical, semi-symbolic inequalities. This is done using techniques of optimization which are typically coming from applied mathematics and have been developed for very concrete applications, often engineering problems. On the other hand, the complete classification of the finite simple groups, also known as the "enormous theorem", does not rely on any machine computation, but is a huge compound piece of published mathematics. Such level of intricacy also raised a controversy on the level of confidence one should have in the correctness of the whole. We thus see that the computer here contributes to blur the lines between what was traditionally considered “fundamental” or “applied”. In such situations, by providing a common mathematical language, formal proof systems may be the only way to provide a safe join between these various tools, through the formalization of proofs whose correctness is difficult to assess through purely human means.

5. Software

5.1. Coq

Participants: Bruno Barras [Contact], Jean-Marc Notin, Arnaud Spiwack, Enrico Tassi.

Coq is a major proof system an the primary object and / or tool of our research. Its development is now mainly coordinated by the πr^2 INRIA Paris-Rocquencourt project-team, and some members of the TypiCal team are active developers of the system.

5.2. Coqfinitgroup

Participants: Cyril Cohen, Assia Mahboubi [Contact].

Coqfinitegroup is the development corresponding to the ongoing effort to formalize the proof of the Feit-Thompson theorem. It is probably the most advanced formal development of group theory today. Its current size is about 80.000 lines of (compact) Coq code. Assia Mahboubi and Cyril Cohen are actively participating to this long term formalization project.

5.3. Dedukti

Participants: Mathieu Boespflug [Contact], Gilles Dowek.

Dedukti is a universal proof checker, based on the $\lambda\pi$-calculus modulo formalism. Mainly developed by Mathieu Boespflug, it is distributed under the GNU licence. The main system includes about 2000 lines of Haskell.

5.4. Ssreflect

Participants: Assia Mahboubi [Contact], Enrico Tassi.

SSReflect is a proof language extension of Coq developed under Georges Gonthier (Microsoft Research). It was originally designed to make the formalization of the Four Color Theorem possible and has been evolving since. It is important to note that it is shipped with redesigned basic proof libraries. Members of the Typical are in charge of the documentation and distribution of this extension.

6. New Results

6.1. Semantics of the Calculus of Inductive Constructions

Participant: Bruno Barras [Contact].

Bruno Barras has formalized the meta-theoretical study of strictly positive inductive types. This was built upon the previous work on specific instances: natural numbers and Brouwer ordinals. The main idea of the model construction is to use the property that every strictly positive inductive definition can be encoded in the parameterized type of trees (the so-called W-types). Such tree-types can themselves be encoded as partial functions from paths to labels. The soundness of this translation gives a way to build the closure ordinal of any strictly positive inductive definition.

Bruno Barras has then modelled the inductive families (also called inductive types with indices). He has been able to prove formally the previously known result that inductive family can be constructed in two steps: first build a carrier type (inductively) which is oblivious of the indices, and then define each member of the family as a subset of the carrier type by enforcing the constraints generated by the indices.

He also started to investigate advanced features of inductive definitions, like the possibility to have non-uniform parameters. When this feature was introduced in Coq , it was thought as a conservative one, but the formal analysis showed that this was not obvious. The consistency model could be extended (with one auxiliary result not yet encoded formally). This shows that non-uniform parameters do not extend much the expressivity of Coq , but the strict equivalence remained as an open problem.

6.2. Relative Strengths of set theory and type theory

Participants: Bruno Barras [Contact], Benjamin Werner.

Bruno Barras also formalized common translations in proof theory: negated translations and Friedman's A-translation. This was used to build a model of (classical) ZF set theory in Coq extended with one axiom called TTDA (Type-Theoretical Description Axiom). This was done in two steps: first build a model of IZF_C (ZF with the collection axiom but not the excluded-middle) in Coq extended with TTDA, and then encode ZF in IZF_C, as shown by Friedman.

The converse result: an interpretation of Coq +TTDA in ZF (with one inaccessible cardinal!) seems not possible, as TTDA in a classical setting gives a (weaker) form of the axiom of choice. Bruno Barras as devised a new axiom (called the Type-Theoretical Collection Axiom) that still allow the ZF interpretation above, but he hopes that its consistency can be proved in ZF extended with one inaccessible cardinal.

Benjamin Werner has worked with Gyesik Lee on set-theoretical models of Coq 's type theory. This work is described in a paper published in the LMCS journal [18].

6.3. A Consistency model of Coq extended with decision procedures

Participants: Bruno Barras [Contact], Qian Wang.

Bruno Barras and Qian Wang are working on the construction of a model for the Calculus of Constructions extended with the type of natural numbers. The definitional equality has been extended to include all equations derivable in Presburger arithmetic. Compared to previous work, this model can support strong eliminations. Since strong eliminations and extensions of the definitional equality with non-satisfiable equations (for instance $0 = 1$) leads to non-normalizing terms, it was necessary to give a precise account of Presburger arithmetic, seen as a specific instance of first-order logic. This work is described in a paper published in the proceedings of the LICS conference [21].

6.4. Towards a concurrent architecture for the Coq kernel

Participants: Bruno Barras [Contact], Enrico Tassi.

In the context of the Paral-ITP ANR project, Bruno Barras and Enrico Tassi have started to implement a kernel of Coq where the process of constructing and checking the proof of a lemma can be executed in a parallel thread.

6.5. Physics of computation

Participant: Gilles Dowek.

Together with Pablo Arrighi, Gilles Dowek has extended Gandy's theorem to quantum physics, by giving a new definition of the notion of finite density of information in this setting. This work has been presented at the congress QIPC [13].

6.6. Binders

Participant: Gilles Dowek.

Together with Jamie Gabbay, Gilles Dowek has given a translation of permissive nominal logic to Higher-order logic and proved its soundness and completeness. This work is described in a paper published in the Transactions on Computational Logic [15].

6.7. Interfacing Coq with SMT solvers

Participants: Germain Faure, Chantal Keller [Contact], Assia Mahboubi, Benjamin Werner.

This is work in close collaboration with the Marelle team (INRIA Sophia Antipolis). The starting point of this work is to note that SMT solvers, deciding the Satisfiability Modulo Theories, are in constant evolution to take into account new decision procedures as well as theories. These systems are rather complex and it is now clearly established that they all contain bugs. The standard approach is to ask the SMT solver to append to the decision result a certificate that can be checked by another tool.

In this context, we are using Coq to check the certificate. The approach is based on computational reflection. The checker is written in Coq , and its architecture is modular and extensible.

We are now able to check certificates coming from the ZChaff SAT solver and from the veriT SMT solver developed at INRIA Nancy – Grand - Est. Proofs established by the SMT tool for the theories of congruence closure and linear arithmetic are checked in short time, overtaking the state of the art in terms of time performance. We also use certificates to build a new Coq tactic that can safely call an external SMT solver, thus increasing Coq 's automation. This tactic is new since it is a decision procedure that combines both linear integer arithmetic and equality of uninterpreted functions. This work is described in a paper published in the proceedings of the CPP2011 conference [25].

6.8. SMT techniques for optimization problems

Participant: Germain Faure [Contact].

The TypiCal team has collaborated with the sysmo team at the Laboratoire d'Informatique de l'École Polytechnique in order to integrate the use of automated tools like SMT solvers in the resolution of optimization problems. The case study was a problem of large scale energy management with various constraints, proposed at the ROADEF 2010 challenge won by the sysmo team. We investigated how to delegate to the SMT tool part of the resolution of constraints. A first conclusion of this experiment is that solving optimization problems represents a more important part of the computation time than first expected. As SMT solvers are not geared toward this class of problems, their performance were not satisfactory. This nonetheless opens new perspectives for the development of SMT tools in order to adapt their internal decision procedures to this new kind of benchmarks. We consider that significant progress in that direction could be easily obtained.

6.9. Formal correctness of embedded programs

Participants: Gilles Dowek [Contact], Pierre Néron.

Pierre Néron is working on program transformations that remove the operations which create most of the approximations during the computation on floating point numbers, namely square roots and divisions. This kind of formal tool aims at increasing the confidence in embedded programs. The idea of this transformation comes from the elimination of the quantifier on real closed fields, hence the first task is to define a minimal but useful language on which the transformation will apply and then to extend this transformation on formulas to this whole language. Keeping the size of the code produced by this transformation in an acceptable range was a challenging issue in this work. The next objective is to write a formal proof ensuring that the transformation is correct. This work will be done in collaboration with the NASA Langley research center in the Formal Method team: Pierre Néron will visit this center for one month in January 2012.

This work is described in a submitted paper [30].

6.10. Formal proofs for convex optimization problems

Participants: Benjamin Werner [Contact], Victor Magron.

Victor Magron is working on the integration of tools that can deal with inequalities on semi-symbolic expressions with real numbers inside proof assistants like Coq.

In particular, he is working on new means to provide formally established bounds for multivariate inequalities, using methods inspired from the convex optimization literature like sums of squares (SOS) and the related semi-definite programming (SDP) relaxation.

He has implemented in OCaml a new algorithm which detects and computes automatically the possible bounds of a given expression. He has tested the approach using benchmarks largely built from inequalities issued from the formal proof of Kepler conjecture (by Thomas Hales). The algorithm computes approximation of transcendental functions by solving sum of squares problems, delegated to an external, dedicated tool. The next step of this project is to certify the correctness of these computations using the Coq system.

He has also improved a Coq tactic based on the external computation of decompositions into sums of squares originally developed by Fréderic Besson (INRIA Rennes - Bretagne Atlantique). The improvement consists in linking this tactic with a tool developed by David Monniaux (Verimag).

6.11. Formal proof in real algebraic geometry

Participants: Assia Mahboubi [Contact], Cyril Cohen.

Cyril Cohen and Assia Mahboubi have completed the first formal proof of quantifier elimination for the theory of real closed fields. This work includes a significant part of infrastructure code for ordered algebraic theories, intervals, and polynomials. This work is described in a submitted paper [29].

Cyril Cohen has implemented in Coq a construction of real algebraic numbers and proved it had a structure of discrete Archimedian real closed field, in the sense of the previous proof of quantifier elimination. Beside the computational interest of real algebraic numbers, this construction both legitimates the abstraction chosen for the proof of quantifier elimination and provides a basis for complex algebraic numbers needed for the completion of the formal proof of the Feit-Thompson theorem. This work is described in a paper to appear in the proceedings of the JFLA2011 conference.

6.12. Constructive mathematics

Participant: Cyril Cohen [Contact].

In collaboration with Thierry Coquand, Cyril Cohen has come up with a constructive proof of a generalization of the fundamental theorem of Algebra. This work show how to formalize the algebraic closure of an arbitrary real closed field. In particular, it can serve as a basis for the construction of complex algebraic numbers from the real algebraic numbers. This work is described in a submitted paper [28].

6.13. Intersection types

Participants: Alexis Bernadet [Contact], Stéphane Lengrand [(CNRS, Lix)].

Alexis Bernadet and Stéphane Lengrand have studied a typing system for the λ-calculus with non-idempotent intersection types. As it is the case in (some) systems with idempotent intersections, a λ-term is typable if and only if it is strongly normalizing. Non-idempotency brings some further information into typing trees, such as a bound on the longest β-reduction sequence reducing a term to its normal form. These results are presented in Klop's extension of λ-calculus, where the bound that is read in the typing tree of a term is refined into an exact measure of the longest reduction sequence. This complexity result is, for longest reduction sequences, the counterpart of de Carvalho's result for linear head-reduction sequences. This work is described in a paper published in the prooceedings of the FOSSACS 2011 conference [22].

Alexis Bernadet and Stéphane Lengrand have also revisited models of typed λ-calculus based on filters of intersection types. By using non-idempotent intersections, they simplify a methodology that produces modular proofs of strong normalization based on filter models. Non-idempotent intersections provide a decreasing measure proving a key termination property, simpler than the reducibility techniques used with idempotent intersections. Such filter models are shown to be captured by orthogonality techniques: we formalize an abstract notion of orthogonality model inspired by classical realizability, and express a filter model as one of its instances, along with two term-models (one of which captures a now common technique for strong normalization). Applying the above range of model constructions to Curry-style System F describes at different levels of detail how the infinite polymorphism of System F can systematically be reduced to the finite polymorphism of intersection types. This work is described in a paper published in the prooceedings of the CSL 2011 conference [23].

6.14. A simple presentation of the effective Topos

Participants: Alexis Bernadet [Contact], Stéphane Lengrand [(CNRS, Lix)].

We introduce here an alternative definition of Hyland's effective topos, based on a realizability framework with two levels of abstraction: a low level and a high level. With this definition, the proof that this framework forms a topos is almost as simple as proving that the category of sets is a topos. Moreover, the high level of the framework can be directly used as a model of higher-order intuitionistic systems. We can then craft a programming language based on topos theory, which can be given a constructive semantics. In such a programming language, we can only write functions that terminate, as in proof assistants like Coq, so the language cannot be Turing-complete. The main advantage of having a programming language based on topos theory over more usual intuitionistic systems such as Martin-Loef type theory is the notion of equality: it is extensional, has proof-irrelevance, and allows the axiom of unique choice.

This work has been presented at the Chocola-Ens Lyon seminar in December 2011.

6.15. A formal proof of the Feit-Thompson theorem

Participant: Assia Mahboubi [Contact].

Assia Mahboubi has pursued her work in the Mathematical Component team lead by Georges Gonthier at the Microsoft Inria Joint Centre. She has finished the formalization of the Wielandt fixpoint theorem, which is one of the key results at the interface between the two components (local analysis and character theory) of the published revised proof of the Feit-Thompson theorem. The proof of the Wielandt theorem was difficult to formalize because it requires a challenging combination of advanced theories with sophisticated constructive formalization: group representation, module theory, linear algebra and characters.

The documentation of this formalization, as well as the current state of the whole formal proof can be found on the webpage of the Mathematical Components project.

6.16. A formal library for polynomial arithmetics

Participant: Assia Mahboubi [Contact].

Assia Mahboubi has worked on a modular formal library devoted to the divisibility theory of polynomials. The aim of this library is to provide a solid basis for further formal developments involving algorithms on polynomials, an in particular to cover the cases when the coefficients of the polynomials involved are equipped with a structure weaker that the structure of field required by the standard Euclidean algorithm.

The documentation of this formalization can be found on the webpage of the Mathematical Components project.

6.17. Weak Memory Models

Participant: Assia Mahboubi [Contact].

Assia Mahboubi has collaborated with Jade Alglave (Oxford University) and has programmed a complete formalization in Coq of the semantic proposed by Jade Alglave in a PhD for weak memory models. This work is described in [27].

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Digiteo Paso

Participants: Assia Mahboubi, Benjamin Werner [Contact].

The PASO project (Preuves, Interprétation abstraite, and Optimisation cal properties of programs, arising in particular from the modeling of complex systems with critical security issues. It gathers computer scientists from CEA-LIST/MeASI, INRIA Saclay/Typical and LIX and specialists from Optimization or Control theory from LIX/MeASI, INRIA Saclay/Maxplus and CMAP, and Supelec/L2S. The goal of this exploratory project is to cross-fertilize these fields, by applying advanced algorithms or techniques inspired by global optimization, by the analysis and identification of dynamical systems, or by zero-sum game theory, in order to improve the precision or the scalability of current methods in proof and static analysis. These applications coming from computer science turn out to raise new challenges for the applied mathematicians. The project started in October 2008 and ended in November 2011.

7.1.2. Digiteo Coquelicot

Participant: Assia Mahboubi [Contact].

Coquelicot is a 3 years Digiteo project that started in September 2011. Sylvie Boldo (INRIA, project-team ProVal) is the principal investigator of this project. The Coquelicot project aims at creating a modern formalization of the real numbers in Coq, with a focus on practicality. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

7.2. National Initiatives

7.2.1. ANR DeCert

Participants: Germain Faure, Chantal Keller, Assia Mahboubi [Contact].

This project is funded by the call Domaines Emergents 2008, a program of the Agence Nationale de la Recherche. It started in January 2009 and will end in December 2012. The objective of the DECERT project is to design an architecture for cooperating decision procedures, with a particular emphasis on fragments of arithmetic, including bounded and unbounded arithmetic over the integers and the reals, and on their combination with other theories for data structures such as lists, arrays or sets. To ensure trust in the architecture, the decision procedures will either be proved correct inside a proof assistant or produce proof witnesses allowing external checkers to verify the validity of their answers.

7.2.2. ANR PSI

Participants: Germain Faure, Assia Mahboubi [Contact], Revantha Ramanayake.

This project is is funded by the call Jeunes Chercheurs Jeunes Chercheuses 2009, a program of the Agence Nationale de la Recherche. It started in September 2009 and will end in September 2013. The PSI project aims at investigating how to take into account the specificities of a given theory when designing proof search methods, both in the theory of proof search and in the design of automated tools.

7.2.3. ANR Paral-ITP

Participants: Bruno Barras [Local coordinator for Inria Saclay – Île - de - France], Germain Faure, Assia Mahboubi, Enrico Tassi.

This project is is funded by the call Ingénierie Numérique et Sécurité 2011, a program of the Agence Nationale de la Recherche. The Paral-ITP project intends to overcome the sequential model for Coq, to make the resources of multi-core hardware available for even larger proof developments. Beyond traditional processing of proof scripts as sequence of proof commands, there is a large space of possibilities and challenges for pervasive parallelism. Coq shall be connected to a uniform document model that integrates parallel and asynchronous evaluation processes with notions of history and change management, over the rich structure of formal content. This can then serve as a basis for an editor document model in direct user interaction, and background library management with continuous proof checking, in the style of modern IDEs like Eclipse or Netbeans. Ultimately, the general document model and front-end technology will accommodate end-users and builders of add-on tools. One typical instance is the add-on that imports proofs constructed by automated deduction systems (SAT and SMT solvers).

7.3. European Initiatives

7.3.1. FP7 Projet

7.3.1.1. FORMATH

Title: FORMATH

Type: COOPERATION (ICT)

Defi: FET Open

Instrument: Specific Targeted Research Project (STREP)

Duration: March 2010 - February 2013

Coordinator: Univ Gothenburg (Sweden)

Others partners: University of Gothenburg, Radboud University Nijmegen, Universidad de la Rioja, INRIA.

See also: FORMATH

Abstract: This project proposes to develop libraries of formalized mathematics concerning algebra, linear algebra, real number computation, and algebraic topology.

7.4. International Initiatives

7.4.1. Visits of International Scientists

7.4.1.1. Internship

Gilles Dowek has been the advisor of Jianhua Gao (University of Tsinghua, Beijing, China), who spent a year in Paris as part of its Doctoral degree.

8. Dissemination

8.1. Organization of scientific events

- Assia Mahboubi has organized the national conference Journées Francophones des Langages Applicatifs 2012, which wil ltake place in Carnac (France) on February 4th-7th.
- Germain Faure and Assia Mahboubi have co-organized with Stéphane Lengrand the PSATTT workshop, satellite of the CADE 2011 conference, which took place in Wroclaw (Poland) on August 1st.

8.2. Program chairs

- Assia Mahboubi has served as vice-president of the program committee of the JFLA 2011 national conference.
- Assia Mahboubi has served as president of the program committee of the JFLA 2011 conference.

8.3. Program committees

- Assia Mahboubi served in the program committees of the CICM/Calculemus 2011, ITP 2011 and ITP 2012 international conferences.
- Assia Mahboubi served in the program committees of the JFLA 2011 and JFLA 2012 national conferences.

8.4. Participation to thesis committees

- Benjamin Werner was member of the PhD committees of Arnaud Spiwack and François Garillot.

8.5. Reviews

- Bruno Barras has served as reviewer for the LICS 2011, CSL 2011 and TLCA 2011 international conferences.
- Bruno Barras has served as reviewer for the Logical Methods in Computer Sciences journal.
- Germain Faure has served as reviewer for the STACS11 international conference.
- Assia Mahboubi has served as reviewer for the international conferences ISSAC 2011, CAI 2011, Cicm/Calculemus 2011, ITP 2011.
- Assia Mahboubi has served as referee for the Journal of Automated Reasoning.

8.6. Invited talks

- Bruno Barras has given a talk at the Gallium seminar (May) in Rocquencourt entitled “Formalisation d’un modèle ensembliste du Calcul des Constructions Inductives”.
- Alexis Bernaded has given a talk entitled “A simple presentation of the effective Topos” at the Rencontres Chocola ENS Lyon in December 2011.
- Gilles Dowek has participated to the Congress of Logic methodology and Philosophy of Science, where he has given two invited talks, one in the Workshop Analysing programs entitled “Logic to the rescue” and another in the workshop entitled “The meaning of axioms”.
- Gilles Dowek has participated to the congress DIDAPRO where he has given an invited talk.
- Gilles Dowek has participated to the Ideals of Proof Workshop "Logic, Proof, and Computation" in Notre Dame University where he has given an invited talk.
- Chantal Keller has given talk at the Z3 Special Interest Group Meeting 2011 on the cooperation between SMT solvers and the Coq proof assistant.
- Chantal Keller has given a talk at the Deducteam seminar on the encoding of HOL-Light proofs in Coq.
- Chantal Keller has given a talk at the INRIA Microsoft Research Joint Centre seminar on the cooperation between SMT solvers and the Coq proof assistant.
- Assia Mahboubi gave a talk at the GGJJ conference in the honor of Gerard Berry and Jean-Jacques Lévy in February 2011 entitled “A formal proof of the Feit-Thompson Theorem”.
- Assia Mahboubi gave a talk at the Microsoft Research - Inria Forum in April 2011 presenting the Mathematical Component team.

- Assia Mahboubi gave a talk at the PPS (Paris 7 University) seminar in July 2011 entitled “Constructive quantifier elimination for real numbers and complex numbers, in a proof assistant”.

8.7. Collective responsibilities

- Gilles Dowek has been a member of the expert group who has proposed a curriculum for the specialty "Informatique et sciences du numériques" in high schools. This program has been published on the Bulletin officiel on October, 13th 2011.
- Gilles Dowek has been a member of the recruiting committee of the University of Paris 13.
- Assia Mahboubi is coordinator of the first Workpackage of the FORMATH European project.
- Assia Mahboubi was elected representant of researchers at Inria Saclay – Île - de - France’s Comité de Centre until September 2011.
- Assia Mahboubi has been elected representant of researchers at LIX’ Conseil de Laboratoire.
- Assia Mahboubi is a member of Inria Saclay – Île - de - France’s Comité de Suivi Doctoral.
- Assia Mahboubi has served as “correcteur au concours d’entrée à l’École Polytechnique” (computer science examiner for the entrance exam at École Polytechnique)
- Benjamin Werner is head of the Computer Science department of École Polytechnique. He is the main person in charge of the Computer Science cursus; he teaches and organizes the main undergraduate course together with François Pottier.

8.8. Popular Science

- Cyril Cohen represented Inria Saclay–Île-de-France for popularizing computer sciences at the "Faites de la science" days (October 2011).
- Assia Mahboubi has given a talk at the Lycée Molière (Rio de Janeiro, Brazil) in the context of the Semaine de la Science (October 2011).

8.9. Teaching

8.9.1. Undergraduate teaching

Licence : Practical programing in Coq (L3), Cyril Cohen (32h). École Polytechnique. France.

Licence : Practical programing in Java (L3), Cyril Cohen (32h). École Polytechnique. France.

Licence :Fundamentals of programming (L3), Chantal Keller (32h). École Polytechnique. France.

Licence :Fundamentals of programming and algorithms (M1), Chantal Keller. École Polytechnique. France.

Licence :Fundamentals of programming (L3), Victor Magron (32h). École Polytechnique. France.

Licence :Fundamentals of programming and algorithms (M1), Victor Magron. École Polytechnique. France.

Master : Gilles Dowek has given a course together with Maël Pegny on Church’s thesis at the Pontifícia Universidade Católica do Rio de Janeiro (Brazil).

Training of High school teachers : Gilles Dowek has given a course to volunteer high school teachers on the principle of programming languages. The course aims at training high-school teachers, since computer science will be taugh in high school starting September 2012.

Master Parisien de Recherche en Informatique (MPRI): “Proof Assistants” (M2), Bruno Barras (16h), Assia Mahboubi (9h). École Polytechnique, France.

8.9.2. Research Schools

MAP Invited Course Map conference (8h), University de la Rioja. Spain. Assia Mahboubi

CEA-EDF-Inria School Modelization and Verification of Algorithms in Coq, an introduction. (14h), Inria. France. Assia Mahboubi

8.9.3. Internships

Gilles Dowek has supervised the Master level (M1) internship of Tomás Lugenstrass.

8.9.3.1. Defenses

PhD : Mathieu Boespflug, Conception d'un noyau de vérification de preuves pour le $\lambda\Pi$-calcul modulo, École Polytechnique, January 2011, Gilles Dowek.

PhD : François Garillot, Generic Proof Tools and Finite Group Theory, École Polytechnique, December 2011, Benjamin Werner

PhD : Arnaud Spiwack, Calculs vérifiés en algèbre homologique, École Polytechnique, March 2011, Thierry Coquand, Benjamin Werner

8.9.3.2. In progress

PhD in progress : Bruno Bernardo, An Implicit Calculus of Inductive Constructions, started in September 2006. Advisors: Bruno Barras, Gilles Dowek.

PhD in progress : Cyril Cohen, Formalisation des nombres algébriques en Coq, started in September 2009. Advisors: Assia Mahboubi, Benjamin Werner

PhD in progress : Chantal Keller, Formal proofs with SMT, started in September 2009. Advisors: Germain Faure, Benjamin Werner

PhD in progress : Victor Magron, Formal proofs of inequalities and semi-definite programming, started in September 2010. Advisors: Stéphane Gaubert (Maxplus project-team), Benjamin Werner

PhD in progress : Pierre Néron, Program transformations for embedded programs, started in September 2010. Advisor: Gilles Dowek.

PhD in progress : Qian Wang, An extension of the Calculus of Constructions with decidable theories, started in September 2011. Advisors: Bruno Barras, Jean-Pierre Jouannaud (Formes, Inria Beijing)

9. Bibliography

Major publications by the team in recent years

[1] G. DOWEK. *Les Métamorphoses du Calcul*, Le Pommier, 2007.

[2] G. DOWEK, O. HERMANT. *A Simple Proof That Super-Consistency Implies Cut Elimination*, in "Term Rewriting and Applications, 18th International Conference, RTA", F. BAADER (editor), Lecture Notes in Computer Science, Springer, 2007, vol. 4533, p. 93-106.

[3] G. DOWEK, B. WERNER. *Proof normalization modulo*, in "J. Symb. Log.", 2003, vol. 68, n^{o} 4, p. 1289-1316.

[4] G. GONTHIER, A. MAHBOUBI, L. RIDEAU, E. TASSI, L. THÉRY. *A Modular Formalisation of Finite Group Theory*, in "Theorem Proving in Higher Order Logics, 20th International Conference", K. SCHNEIDER, J. BRANDT (editors), Lecture Notes in Computer Science, Springer, 2007, vol. 4732, p. 86-101.

[5] B. GRÉGOIRE, L. THÉRY, B. WERNER. *A Computational Approach to Pocklington Certificates in Type Theory*, in "Functional and Logic Programming, 8th International Symposium", M. HAGIYA, P. WADLER (editors), Lecture Notes in Computer Science, Springer, 2006, vol. 3945, p. 97-113.

[6] H. HERBELIN, S. GHILEZAN. *An approach to call-by-name delimited continuations*, in "Proceedings of the 35th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL", G. C. NECULA, P. WADLER (editors), ACM, 2008, p. 383-394.

[7] H. HERBELIN. *C'est maintenant qu'on calcule, au cœur de la dualité*, Université Paris-Sud, 2005, Habilitation à diriger des recherches.

[8] A. MIQUEL. *Le Calcul des Constructions Implicites : syntaxe et sémantique*, Université Paris VII, 2001.

[9] J. NARBOUX. *Mechanical Theorem Proving in Tarski's Geometry*, in "Automated Deduction in Geometry, 6th International Workshop, ADG", F. BOTANA, T. RECIO (editors), Lecture Notes in Computer Science, Springer, 2006, vol. 4869, p. 139-156.

[10] R. ZUMKELLER. *Formal Global Optimisation with Taylor Models*, in "Automated Reasoning, Third International Joint Conference, IJCAR", U. FURBACH, N. SHANKAR (editors), Lecture Notes in Computer Science, Springer, 2006, vol. 4130, p. 408-422.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. BOESPFLUG. *Conception d'un noyau de vérification de preuves pour le λΠ-calcul modulo*, Ecole Polytechnique, January 2011.

[12] A. SPIWACK. *Calculs vérifiés en algèbre homologique*, Ecole Polytechnique, March 2011, http://hal.inria.fr/pastel-00605836/en.

Articles in International Peer-Reviewed Journal

[13] P. ARRIGHI, G. DOWEK. *The physical Church-Turing thesis and the principles of quantum theory*, in "International Journal of Foundations of Computer Science", 2011, to appear.

[14] Y. BERTOT, F. GUILHOT, A. MAHBOUBI. *A formal study of Bernstein coefficients and polynomials*, in "Mathematical Structures in Computer Science", 2011, vol. 21, n^{o} 04, p. 731-761, http://hal.inria.fr/inria-00503017/en.

[15] G. DOWEK, M. J. GABBAY. *Permissive Nominal Logic (journal version)*, in "Transactions on Computational Logic", 2011, to appear, http://www.gabbay.org.uk/papers/pernl-jv.pdf.

[16] G. DOWEK, O. HERMANT. *A simple proof that super-consistency implies cut elimination*, in "Notre Dame Journal of Formal Logic", 2011, to appear.

[17] G. DOWEK, Y. JIANG. *On the expressive power of schemes*, in "Inf. Comput.", 2011, vol. 209, n^{o} 9, p. 1231-1245.

[18] G. LEE, B. WERNER. *Proof-irrelevant model of CC with predicative induction and judgmental equality*, in "Logical Methods in Computer Science", 2011, to appear.

[19] C. ROCHA, C. MUÑOZ, G. DOWEK. *A formal library of set relations and its application to synchronous languages*, in "Theor. Comput. Sci.", 2011, vol. 412, n^{O} 37, p. 4853-4866.

International Conferences with Proceedings

[20] M. ARMAND, G. FAURE, B. GRÉGOIRE, C. KELLER, L. THÉRY, B. WERNER. *Verifying SAT and SMT in Coq for a fully automated decision procedure*, in "PSATTT'11: International Workshop on Proof-Search in Axiomatic Theories and Type Theories", Wroclaw, Poland, Germain Faure, Stéphane Lengrand, Assia Mahboubi, 2011, http://hal.inria.fr/inria-00614041/en.

[21] B. BARRAS, J.-P. JOUANNAUD, P.-Y. STRUB, Q. WANG. *CoqMTU: a higher-order type theory with a predicative hierarchy of universes parametrized by a decidable first-order theory*, in "Twenty-Sixth Annual IEEE Symposium on "Logic in Computer Science"", Toronto, Canada, 2011, http://hal.inria.fr/inria-00583136/en.

[22] A. BERNADET, STÉPHANE. LENGRAND. *Complexity of strongly normalising λ-terms via non-idempotent intersection types*, in "Proceedings of the 14th international conference on Foundations of Software Science and Computation Structures (FOSSACS'11)", M. HOFMANN (editor), LNCS, Springer-Verlag, March 2011, vol. 6604, p. 88–107.

[23] A. BERNADET, STÉPHANE. LENGRAND. *Filter models: non-idempotent intersection types, orthogonality and polymorphism*, in "Proceedings of the 20th Annual conference of the European Association for Computer Science Logic (CSL'11)", M. BEZEM (editor), Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, September 2011.

[24] J. GAO. *Clausal Presentation of Theories in Deduction Modulo*, in "PSATTT'11: International Workshop on Proof-Search in Axiomatic Theories and Type Theories", Wroclaw, Poland, Germain Faure, Stéphane Lengrand, Assia Mahboubi, 2011, http://hal.inria.fr/inria-00614251/en.

[25] C. KELLER, M. ARMAND, G. FAURE, B. GRÉGOIRE, L. THÉRY, B. WERNER. *A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses*, in "Certified Programs and Proofs 2011", Howard Beach Resort Kenting, Taiwan, Province Of China, J.-P. JOUANNAUD, Z. SHAO (editors), Springer, December 2011, http://hal.inria.fr/hal-00639130/en.

Books or Proceedings Editing

[26] G. DOWEK (editor). *Introduction à la science informatique*, CRDP de Paris, 2011.

Other Publications

[27] J. ALGLAVE, A. MAHBOUBI. *A Generic Formalised Framework for Reasoning About Weak Memory Models*, 2011, draft, http://hal.inria.fr/inria-00604656/en.

[28] C. COHEN, T. COQUAND. *A constructive version of Laplace's proof on the existence of complex roots*, 2011, submitted, http://hal.inria.fr/inria-00592284/en.

[29] C. COHEN, A. MAHBOUBI. *Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination*, 2011, submitted, http://hal.inria.fr/inria-00593738/en.

[30] P. NÉRON. *Eliminating Division and Square Root in Embedded Programs*, 2011, Submitted, http://www.lix.polytechnique.fr/~neron/Publi/Elimsqrt/Elimsqrt.pdf.