IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2012

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

1. Members **1**
2. Overall Objectives **1**
2.1. Presentation 1
2.2. Highlights of the Year 2
3. Research Program **2**
3.1. Logical formalisms 2
3.2. Libraries of formalized mathematics 2
3.3. Proof search and automated decision procedures 2
4. Software and Platforms **3**
4.1. Coq 3
4.2. Coqfinitgroup 3
4.3. Ssreflect 3
5. New Results **3**
5.1. Feit-Thompson 3
5.2. Formal Semantics of Type Theory 4
5.3. Study of Type Theories 4
5.4. Formal and computable algebra 4
5.5. Certifiable real optimization 4
5.6. Binder representation in Coq 4
5.7. SMT and Coq 4
5.8. Automated decision procedures 4
6. Bilateral Contracts and Grants with Industry **5**
7. Partnerships and Cooperations **5**
7.1. Regional Initiatives 5
7.2. National Initiatives 5
7.2.1.1. ParalITP (ANR-11-INSE-001) 5
7.2.1.2. Psi (ANR-09-JCJC-0006) 5
7.3. European Initiatives 6
8. Dissemination **6**
8.1.1. Teaching 6
8.1.2. Supervision 6
9. Bibliography **7**

Project-Team TYPICAL

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

Creation of the Project-Team: 2008 January 01, end of the Project-Team: 2012 December 31.

1. Members

Research Scientists

Bruno Barras [Junior Researcher]
Enrico Tassi [Junior Researcher]
Assia Mahboubi [Junior Researcher]

Faculty Member

Benjamin Werner [Professor, École Polytechnique, Team leader, HdR]

Engineer

Jean-Marc Notin [Research Engineer]

PhD Students

Alexis Bernadet [PhD student]
Bruno Bernardo [PhD student]
Cyril Cohen [PhD student until student until october 2012]
Chantal Keller [PhD student]
Victor Magron [PhD student]
Pierre Néron [PhD student]

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 20th 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?”.

2.2. Highlights of the Year

Assia Mahboubi, Enrico Tassi and Cyril Cohen were among the main participants in the project of formalization of the Feit-Thompson (Odd Order) theorem finally completed in September 2012 by the Mathematical Components team (lead by Georges Gonthier).

Bruno Barras and Assia Mahboubi have been granted fellowships by the Insititute for Advanced Study (Princeton, USA).

3. Research Program

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. Software and Platforms

4.1. Coq

Participants: Bruno Barras [Contact], Jean-Marc Notin, 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.

4.2. Coqfinitgroup

Participants: Cyril Cohen, Assia Mahboubi [Contact], Enrico Tassi.

Coqfinitegroup is the development corresponding to the full formalization of 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 have been actively participating to this long term formalization project.

4.3. 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. Enrico Tassi has worked on an extended language of patterns for term selection now included in the distribution of this extension. Members of the Typical are in charge of the documentation and distribution of this extension.

5. New Results

5.1. Feit-Thompson

The Feit-Thompson is an important theorem stating that every finite group of odd order is solvable. It is an important step in the classification of finite groups. Its proof is remarkable through its difficulty and its length (more than 1000 pages of dense mathematical text).

This proof was entirely formalized in Coq. This effort was started six years ago, as a joint project of the project teams Typical, Marelle (Sophia-Antipolis) and the Inria-MSR joint center, under the supervision of Georges Gonthier. The proof was finished in september 2012 and is considered a remarkable achievement. It also gave birth to several side products, such as enhancements of the SSReflect proof language. For Typical, Assia Mahboubi, Enrico Tassi and Cyril Cohen were instrumental in this effort.

5.2. Formal Semantics of Type Theory

Bruno Barras finished an extensive formalization of Coq's type theory in Coq, as well as a large formalization of set theory. This work includes several new results and insights in the study of Type Theory and is the body of Barras' habilitation thesis to be defended early in 2013.

5.3. Study of Type Theories

Bruno Barras finished an extensive formalization of Coq's type theory in Coq, as well as a large formalization of set theory. This work includes several new results and insights in the study of Type Theory and is the body of Barras' habilitation thesis to be defended early in 2013.

Chantal Keller, with Marc Lasson, has presented a notion of parametricity in impredicative type theories, which yields some possible application in proof search [18].

5.4. Formal and computable algebra

Cyril Cohen and Assia Mahboubi have worked on representing various algebraic objects in Coq, in a way that allows computation. In particular, Cohen proposed and developed a representation of algebraic numbers in Coq, as presented in [16]. Assia Mahboubi has collaborated with Frédéric Chyzak (Inria Paris-Roquencourt, Algo team) on the certification of algorithms for D-finite objects.

5.5. Certifiable real optimization

Under the joint supervision of Stéphane Gaubert and Benjamin Werner, with Xavier Allamigeon, Victor Magron is investigating ways to check difficult real inequalities, over bounded domains, in ways which can be re-checked by proof systems like Coq. One such algorithm, combining convex optimization and Max-plus techniques is submitted for publication at ECC 2013.

5.6. Binder representation in Coq

Benjamin Werner has developed a generic tree datatype in Coq, which can encode any language with fixed-arity operators with binders. The application towards smoother formal treatment of such languages is still in progress.

5.7. SMT and Coq

Chantal Keller has enhanced the performances of her SMT-Coq interface based automatic tactic. More precisely, the code has been made more modular which allowed:

- A first interfacing with the renowned Z3 SMT prover from Microsoft Research,
- Extending SMT-Coq to the theory of Coq's native 31 bits integers.

5.8. Automated decision procedures

Assia Mahboubi has woked with members of the Proval team on a new decision procedure for integer arithmetics now intergrated in the Alt-Ergo SMT solver. Assia Mahboubi has worked with Stéphane Lengrand and Mahfuza Farooque on the design of a sequent calculus with focussing and on the conception of a proof search strategy in this calculus which simulates the Davis-Putman-Logemann-Loveland algorithme modulo theory (DPPL(T)) which is implemented by modern SMT-solvers. An implementation developped by Stéphane Lengrand illustrate this approach on standard SMT benchmarks.

6. Bilateral Contracts and Grants with Industry

6.1. Common Research Agreements in the MSR–Inria Joint Centre

Assia Mahboubi, Enrico Tassi and Cyril Cohen are part of the *Mathematical Components* effort in the Inria and Microsoft Research joint centre. The goal is to investigate the design of large-scale, modular and reusable libraries of formalized mathematics. Developed using the Coq proof assistant. This project successfully formalized the proof of the Feit–Thompson theorem, resulting in a corpus of libraries related to various areas of algebra.

7. Partnerships and Cooperations

7.1. Regional Initiatives

Project *Coquelicot*, funded jointly by the Fondation de Coopération Scientifique "Campus Paris-Saclay" and Digiteo.

Goal: Create a new Coq library for real numbers of mathematics.
Leader: S. Boldo (INRIA Saclay, Toccata). Participant: A. Mahboubi.
Website: http://coquelicot.saclay.inria.fr/.

7.2. National Initiatives

7.2.1. ANR

7.2.1.1. ParalITP (ANR-11-INSE-001)

Goal: Improve the performances and the ergonomics of interactive provers by taking advantage of modern, parallel hardware.
Leader: B. Wolff. Participants: A. Mahboubi, E. Tassi.
Website: http://paral-itp.lri.fr/.

7.2.1.2. Psi (ANR-09-JCJC-0006)

Goal: Investigate the theory and the implementation of proof-search methods in the context of specific theories. This project aims at understanding how to combine state-of-the-art proof-theoretic generic methods (DPLL, focusing, ...) with efficient automated-reasoning methods for well-identified theories (linear arithmetic, ...).
Leader: S. Lengrand (CNRS, LiX). Participant: A. Mahboubi.
Website: http://www.lix.polytechnique.fr/~lengrand/PSI/.

7.3. European Initiatives

7.3.1. FP7 Projects

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 Götegorg (Sweden)

Others partners: Radboud University Nijmegen, (the Netherlands), University of La Rioja, (Spain).

See also: http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath

Abstract: The objective of this project is to develop libraries of formalised mathematics concerning algebra, linear algebra, real number computation, and algebraic topology. The libraries that we plan to develop in this proposal are especially chosen to have long-term applications in areas where software interacts with the physical world. The main originality of the work is to structure these libraries as a software development, relying on a basis that has already shown its power in the formal proof of the four-colour theorem, and to address topics that were mostly left untouched by previous research in formal proof or formal methods.

8. Dissemination

8.1. Teaching - Supervision - Juries

8.1.1. Teaching

Benjamin Werner is president of the Computer Science Department of Ecole Polytechnique and, as such main responsible for CS teaching in this university.

Licence : Benjamin Werner, Ecole Polytechnique, *Algorithmique et Programmation*, lectures, 45 hours *équivalents TDs*.

Master : Benjamin Werner, MPRI (M2), Fondements des Systèmes de Preuves, Ecole Polytechnique et U. Paris 7, 50 heures équivalents TDs.

Master : Assia Mahboubi and Bruno Barras, MPRI (M2), Preuves en Coq, Ecole Polytechnique et U. Paris 7, 50 heures équivalents TDs.

Licence : Victor Magron and Chantal Keller, Ecole Polytechnique, *Algorithmique et Programmation*, TDs, 48 hours *équivalents TDs*.

Master : Chantal Keller, PA Informatique de l'Ecole Polytechnique, Raisonnement mathématique assisté par ordinateur, TDs, 20 hours *équivalents TDs*.

8.1.2. Supervision

PhD & HdR :

PhD : Cyril Cohen, Formalized algebraic numbers: construction and first-order theory, Ecole Polytechnique, november 20th, Assia Mahboubi and Benjamin Werner.

PhD in progress :Chantal Keller, A Matter of Trust New Reflexive Decision Procedures in Coq Using External Tools, since sept. 2009, Benjamin Werner

PhD in progress :Victor Magron, Certifiable automatic proofs of real inequalities, since sept. 2009, Benjamin Werner and Stéphane Gaubert.

PhD in progress: Alexis Bernadet, since 2010. Supervised by Stéphane Lengrand and Benjamin Werner.

9. Bibliography

Major publications by the team in recent years

[1] , *Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science, LICS 2011, June 21-24, 2011, Toronto, Ontario, Canada*, IEEE Computer Society, 2011

[2] J.-P. JOUANNAUD, Z. SHAO (editors). , *Certified Programs and Proofs - First International Conference, CPP 2011, Kenting, Taiwan, December 7-9, 2011. Proceedings*, Lecture Notes in Computer Science, Springer, 2011, vol. 7086

[3] M. KAUFMANN, L. C. PAULSON (editors). , *Interactive Theorem Proving, First International Conference, ITP 2010, Edinburgh, UK, July 11-14, 2010. Proceedings*, Lecture Notes in Computer Science, Springer, 2010, vol. 6172

[4] M. ARMAND, G. FAURE, B. GRÉGOIRE, C. KELLER, L. THÉRY, B. WERNER. *A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses*, in "CPP", J.-P. JOUANNAUD, Z. SHAO (editors), Lecture Notes in Computer Science, Springer, 2011, vol. 7086, pp. 135-150

[5] 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 "LICS", IEEE Computer Society, 2011, pp. 143-151

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

[7] C. KELLER, B. WERNER. *Importing HOL Light into Coq*, in "ITP", M. KAUFMANN, L. C. PAULSON (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 6172, pp. 307-322

[8] G. LEE, B. WERNER. *Proof-irrelevant model of CC with predicative induction and judgmental equality*, in "Logical Methods in Computer Science", 2011, vol. 7, n^{o} 4

[9] B. WERNER. *On the Strength of Proof-irrelevant Type Theories*, in "Logical Methods in Computer Science", 2008, vol. 4, n^{o} 3

[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, pp. 408-422

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] C. COHEN. , *Formalized algebraic numbers: construction and first-order theory*, Ecole Polytechnique, 2012

Articles in International Peer-Reviewed Journals

[12] A. ASPERTI, W. RICCIOTTI, C. S. COEN, E. TASSI. *A Bi-Directional Refinement Algorithm for the Calculus of (Co)Inductive Constructions*, in "Logical Methods in Computer Science", 2012, vol. 8, n^{o} 1

[13] A. ASPERTI, W. RICCIOTTI, C. S. COEN, E. TASSI. *Formal Metatheory of Programming Languages in the Matita Interactive Theorem Prover*, in "J. Autom. Reasoning", 2012, vol. 49, n^{o} 3, pp. 427-451

[14] C. COHEN, A. MAHBOUBI. *Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination*, in "Logical Methods in Computer Science", February 2012, vol. 8, n^{o} 1:02, pp. 1-40 [*DOI :* 10.2168/LMCS-8 (1:02) 2012], http://hal.inria.fr/inria-00593738

International Conferences with Proceedings

[15] F. BOBOT, S. CONCHON, E. CONTEJEAN, M. IGUERNELALA, A. MAHBOUBI, A. MEBSOUT, G. MELQUIOND. *A Simplex-Based Extension of Fourier-Motzkin for Solving Linear Integer Arithmetic*, in "6th International Joint Conference on Automated Reasoning", Manchester, United Kingdom, B. GRAMLICH, D. MILLER, U. SATTLER (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7364, pp. 67-81 [*DOI :* 10.1007/978-3-642-31365-3_8], http://hal.inria.fr/hal-00687640

[16] C. COHEN. *Construction of real algebraic numbers in Coq*, in "ITP - 3rd International Conference on Interactive Theorem Proving - 2012", Princeton, United States, L. BERINGER, A. FELTY (editors), Springer, August 2012, http://hal.inria.fr/hal-00671809

[17] G. GONTHIER, E. TASSI. *A Language of Patterns for Subterm Selection*, in "ITP", 2012, pp. 361-376

[18] C. KELLER, M. LASSON. *Parametricity in an Impredicative Sort*, in "CSL - 26th International Workshop/21st Annual Conference of the EACSL, CSL 2012", Fontainebleau, France, P. CÉGIELSKI, A. DURAND (editors), Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, September 2012, vol. 16, pp. 381-395 [*DOI :* 10.4230/LIPICS.CSL.2012.399], http://hal.inria.fr/hal-00730913

National Conferences with Proceedings

[19] C. COHEN. *Construction des nombres algébriques réels en Coq*, in "JFLA - Journées Francophones des Langages Applicatifs - 2012", Carnac, France, February 2012, http://hal.inria.fr/hal-00665965

Scientific Books (or Scientific Book chapters)

[20] F. POTTIER, B. WERNER. , *Algorithmique et Programmation*, Ecole Polytechnique, 2012

Research Reports

[21] M. FAROOQUE, S. LENGRAND, A. MAHBOUBI. , *Two simulations about DPLL(T)*, Inria, March 2012, http://hal.inria.fr/hal-00690044

Other Publications

[22] X. ALLAMIGEON, S. GAUBERT, V. MAGRON, B. WERNER. , *Certification of inequalities involving transcendental functions: combining SDP and max-plus approximation*, Submitted for publication

[23] M. FAROOQUE, S. LENGRAND, A. MAHBOUBI. , *Simulating the DPLL(T) procedure in a sequent calculus with focusing*, http://hal.inria.fr/hal-00690392