Activity Report 2016

Project-Team MARELLE

Mathematical, Reasoning and Software

RESEARCH CENTER
Sophia Antipolis - Méditerranée

THEME
Proofs and Verification

Table of contents

Project-Team MARELLE

Creation of the Project-Team: 2006 November 01

Keywords:

Computer Science and Digital Science:

2.1.11. - Proof languages
2.4.3. - Proofs
4.5. - Formal methods for security
5.10.1. - Design
7.4. - Logic in Computer Science
7.6. - Computer Algebra
7.12. - Computer arithmetic

Other Research Topics and Application Domains:

6.1. - Software industry
9.4.1. - Computer science
9.4.2. - Mathematics

1. Members

Research Scientists

Yves Bertot [Team leader, Inria, Senior Researcher, HDR]
Cyril Cohen [Inria, Researcher]
Benjamin Grégoire [Inria, Researcher]
José Grimm [Inria, Researcher]
Laurence Rideau [Inria, Researcher]
Enrico Tassi [Inria, Researcher]
Laurent Théry [Inria, Researcher]

Engineers

Maxime Dénès [Inria]
Matej Košík [Inria]

PhD Students

Cécile Baritel-Ruet [ENS Cachan]
Sophie Bernard [Univ. Nice]
Boris Djalal [Inria]
Damien Rouhling [Min. Ens. Sup. Recherche]

Post-Doctoral Fellow

Anders Mörtberg [Inria, from Nov 2016]

Visiting Scientist

Paul Aaron Steckler [MIT, from Apr 2016 until May 2016]

Administrative Assistant

Nathalie Bellesso [Inria]

Others

Wassim Haffaf [SupElec, intern from Jun 2016 until August 2016]
Rébecca Zucchini [ENS Cachan, intern from Jun 2016 until Jul 2016]

2. Overall Objectives

2.1. Overall Objectives

We want to concentrate on the development of mathematical libraries for theorem proving tools. This objective contributes to two main areas of application: tools for mathematicians and correctness verification tools for software dealing with numerical computation.

In the short term, we aim for mathematical libraries that concern polynomials, algebra, group theory, floating point numbers, real numbers, big integers, probabilities and geometrical objects. In the long run, we think that this will involve any function that may be of use in embedded software for control or robotics (in what is called hybrid systems, systems that contain both software and physical components) and in cryptographical systems. We want to integrate these libraries in theorem proving tools because we believe they will become important tools for mathematical practice and for engineers who need to prove the correctness of their algorithms and software.

We believe that theorem proving tools are good tools to produce highly dependable software, because they provide a framework where algorithms and specifications can be studied uniformly and often provide means to mechanically derive programs that are correct by construction.

We also study the extensibility of interactive theorem proving tools based on decision procedures that free designers from the burden of verifying some of the required properties. We often rely on "satisfiability modulo theory" procedures, which can be connected to theorem proving tools in a way that preserves the trustability of the final results.

3. Research Program

3.1. Type theory and formalization of mathematics

The calculus of inductive constructions is a branch of type theory that serves as a foundation for theorem proving tools, especially the Coq proof assistant. It is powerful enough to formalize complex mathematics, based on algebraic structures and operations. This is especially important as we want to produce proofs of logical properties for these algebraic structures, a goal that is only marginally addressed in most scientific computation systems.

The calculus of inductive constructions also makes it possible to write algorithms as recursive functional programs which manipulate tree-like data structures. A third important characteristic of this calculus is that it is also a language for manipulating proofs. All this makes this calculus a tool of choice for our investigations. However, this language still is the object of improvements and part of our work focusses on these improvements.

3.2. Verification of scientific algorithms

To produce certified algorithms, we use the following approach: instead of attempting to prove properties of an existing program written in a conventional programming language such as C or Java, we produce new programs in the calculus of constructions whose correctness is an immediate consequence of their construction. This has several advantages. First, we work at a high level of abstraction, independently of the target implementation language. Secondly, we concentrate on specific characteristics of the algorithm, and abstract away from the rest (for instance, we abstract away from memory management or data implementation strategies). Therefore, we are able to address more high-level mathematics and to express more general properties without being overwhelmed by implementation details.

However, this approach also presents a few drawbacks. For instance, the calculus of constructions usually imposes that recursive programs should explicitly terminate for all inputs. For some algorithms, we need to use advanced concepts (for instance, well-founded relations) to make the property of termination explicit, and proofs of correctness become especially difficult in this setting.

3.3. Programming language semantics

To bridge the gap between our high-level descriptions of algorithms and conventional programming languages, we investigate the algorithms that are present in programming language implementations, for instance algorithms that are used in a compiler or a static analysis tool. When working on these algorithms, we usually base our work on the semantic description of the programming language. The properties that we attempt to prove for an algorithm are, for example, that an optimization respects the meaning of programs or that the programs produced are free of some unwanted behavior. In practice, we rely on this study of programming language semantics to propose extensions to theorem proving tools or to verify that compilers for conventional programming languages are exempt from bugs.

4. New Software and Platforms

4.1. Coq

The Coq Proof Assistant
KEYWORDS: Proof - Certification - Formalisation
FUNCTIONAL DESCRIPTION

Coq provides both a dependently-typed functional programming language and a logical formalism, which, altogether, support the formalisation of mathematical theories and the specification and certification of properties of programs. Coq also provides a large and extensible set of automatic or semi-automatic proof methods. Coq's programs are extractible to OCaml, Haskell, Scheme, ...

- Participants: Benjamin Gregoire, Enrico Tassi, Bruno Barras, Yves Bertot, Pierre Boutillier, Xavier Clerc, Pierre Courtieu, Maxime Dénès, Stephane Glondu, Vincent Gross, Hugo Herbelin, Pierre Letouzey, Assia Mahboubi, Julien Narboux, Jean-Marc Notin, Christine Paulin-Mohring, Pierre-Marie Pedrot, Loic Pottier, Matthias Puech, Yann Regis-Gianas, François Ripault, Matthieu Sozeau, Arnaud Spiwack, Pierre-Yves Strub, Benjamin Werner, Guillaume Melquiond and Jean-Christophe Filliatre
- Partners: CNRS - ENS Lyon - Université Paris-Diderot - Université Paris-Sud
- Contact: Matthieu Sozeau
- URL: http://coq.inria.fr/

The Marelle team, in collaboration with the pi.r2 team, plays an important role in the development of Coq. During this year, we contributed to the 8.6 version of Coq, released in December. As the *release manager*, Maxime Dénès led the implementation of a time-based release process, aiming at shorter and more predicitible release cycles. We successfully transitioned to 10-month cycles and hope to soon move to 6-month cycles, making it easier for users to benefit from the latest improvements.

At a more detailed level, members of the Marelle team attended the Coq developer meetings (organized in Paris by Maxime Dénès and Matthieu Sozeau) and contributed to the development of Coq concerning bug fixes for virtual machine execution (Benjamin Grégoire and Maxime Dénès), cleaning up the API for plug-in developers (Matej Košík), improving the State Transaction Machine (Enrico Tassi), setting up a package index based on OPAM (Enrico Tassi), introducing a system to discuss Coq Enhancement Proposals (Enrico Tassi), and implementing a new configurable system of warnings (Maxime Dénès).

We supervise of an engineer working at MIT on questions related to efficient proof construction and proof development environments, in cooperation with researchers from the pi.r2 team. The collaboration with MIT was also an occasion to reflect on the licence framework governing collaborations around the Coq system.

We also prepared the set-up of a consortium to gather intensive users and contributors to the development of Coq. This was an occasion to work with the promotors of the InriaSoft structure which is expected to host the consortium in the long run.

4.2. Easycrypt

FUNCTIONAL DESCRIPTION

EasyCrypt is a toolset for reasoning about relational properties of probabilistic computations with adversarial code. Its main application is the construction and verification of game-based cryptographic proofs. EasyCrypt can also be used for reasoning about differential privacy.

- Participants: Gilles Barthe, Benjamin Gregoire and Pierre-Yves Strub
- Contact: Benjamin Grégoire
- URL: https://www.easycrypt.info/trac/

This year, development on this software system concerned the development of new logical settings to work on differential privay problems: a Hoare logic based on union bound and a logic based on probabilistic couplings.

4.3. Math-Components

Mathematical Components library
FUNCTIONAL DESCRIPTION

The Mathematical Components library is a set of Coq libraries that cover the mechanization of the proof of the Odd Order Theorem.

- Participants: Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, Francois Garillot, Georges Gonthier, Stéphane Le Roux, Assia Mahboubi, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, Laurent Théry and Russell O'Connor
- Contact: Assia Mahboubi
- URL: http://www.msr-inria.fr/projects/mathematical-components-2/

This year we contributed to the library by adding a new module to cover finite sets within potentially infinite finite types, organizing tutorials and schools to teach its usage:

- in January in Sophia Antipolis (one-week format) https://team.inria.fr/marelle/en/advanced-coq-winter-school-2016/ (organized by Enrico Tassi, with contributions by Cyril Cohen, Laurence Rideau, Laurent Théry)
- in August in Nancy (one-day tutorial format, colocated with the ITP conference, organized by Assia Mahboubi and Enrico Tassi, with contributions by Yves Bertot, Cyril Cohen, and Laurent Théry) https://github.com/math-comp/wiki/wiki/tutorial-itp2016
- in November in Sophia Antipols https://team.inria.fr/marelle/en/advanced-coq-winter-school-2016-2017/ (organized by Enrico Tassi, with contributions by Yves Bertot, Cyril Cohen, Laurence Rideau).

4.4. Ssreflect

FUNCTIONAL DESCRIPTION

Ssreflect is a tactic language extension to the Coq system, developed by the Mathematical Components team.

- Participants: Cyril Cohen, Yves Bertot, Laurence Rideau, Enrico Tassi, Laurent Thery, Assia Mahboubi and Georges Gonthier
- Contact: Yves Bertot
- URL: http://ssr.msr-inria.inria.fr/

This year we mainly performed maintenance operations on this software extension to the Coq system (Enrico Tassi).

4.5. Zoocrypt

FUNCTIONAL DESCRIPTION

ZooCrypt is an automated tool for analyzing the security of padding-based public-key encryption schemes (i.e. schemes built from trapdoor permutations and hash functions). This year, we extended the tool to be able to deal with schemes based on cyclic groups and bilinear maps.

- Participants: Benjamin Gregoire, Gilles Barthe and Pierre-Yves Strub
- Contact: Benjamin Grégoire
- URL: https://www.easycrypt.info/zoocrypt/

5. New Results

5.1. Implementing Theorem Proving in Higher Order Logic Programming

Participants: Enrico Tassi, Cvetan Dunchev [University of Bologna], Ferruccio Guidi [University of Bologna], Claudio Sacerdoti Coen [University of Bologna].

We carried on our experiments with extensions of λ-prolog, based on the ELPI tool that we developed, in particular concerning implementations of higher-order logic and type theory in this context. This work lead to publication in June at LFMTP'16 [14] and to a preliminary report [25].

5.2. Coqoon: An IDE for interactive proof development in Coq

Participants: Enrico Tassi, Alexander Faithfull [ITU Copenhagen], Jesper Bengtson [ITU Copenhagen], Carst Tankink.

We carried on our experiments with the Coqoon integrated development environment. This lead to a preliminary report submitted for publication [24]

5.3. A book on mathematical components

Participants: Enrico Tassi, Yves Bertot, Laurence Rideau, Assia Mahboubi, Georges Gonthier.

As an effort to lower the entry barrier to use a structured library of formalized mathematics, we wrote a book explaining the principles of ssreflect and mathematical components. This book-in-the-making is available on github at https://math-comp.github.io/mcb/ and we plan to make it evolve as we teach schools on using the library and we gather feedback from readers and users.

5.4. Proofs of transcendence

Participants: Sophie Bernard, Yves Bertot, Laurence Rideau.

In the previous year, we developed formally verified proofs that e and π are transcendental. This result was published this year at the CPP conference (Certified Programs and Proofs) [12]. Since October, as part of the PhD of Sophie Bernard, we are working on the generalisation of these proofs, in order to prove the Lindemann theorem that states that no algebraic spans of exponentials of algebraic numbers can be equal to zero under some assumptions.

5.5. Cubical type theory and univalent foundations

Participants: Cyril Cohen, Anders Mörtberg, Benedikt Ahrens [ASCOLA project-team, Inria and LINA Nantes], Mark Bickford [Cornell Unversity, USA], Thierry Coquand [Chalmers and Göteborg University, Sweden], Ralph Matthes [CNRS, University of Toulouse].

This work mainly concerns Univalent Foundations and Homotopy Type Theory which builds on recently discovered connections between type theory and abstract homotopy theory. The main question we have been working on lately is finding a computational interpretation for the univalence axiom, the main fruit of this work is a recent paper on, and implementation of, cubical type theory [23] which provides a constructive justification for this axiom. The code is visible at https://github.com/mortberg/cubicaltt. The last year Anders Mörtberg has been working together with Mark Bickford at Cornell University and Thierry Coquand at University of Gothenburg and Chalmers University of Technology on the formal verification of this model in the Nuprl proof assistant, this code is visible at http://www.nuprl.org/wip/Mathematics/cubical!type!theory/index.html.

Anders Mörtberg also recently visited Thierry Coquand to start a collaboration on the formalization of this model in the UniMath system implemented in Coq. Together with Benedikt Ahrens in the Ascola team at Inria Nantes and Ralph Matthes at IRIT in Toulouse, Anders Mörtberg also worked on the formalization of a translation from binding signatures to monads for representing languages with binders in UniMath [21]. This work uses the new possibilities for representing category theory in type theory that univalence provides.

5.6. Formal study of double-word arithmetic algorithms

Participants: Laurence Rideau, Jean-Michel Muller [CNRS and ENS Lyon], Valentina Popescu [CNRS and ENS Lyon].

As part of the ANR Fastrelax project, we have started to formalize double-word arithmetic algorithms, in particular the sum of a double-word and a floating point number and the sum of two double-word numbers described in the article " Tight and rigourous error bounds for basic building blocks of double-word arithmetic" [26].

5.7. Formal foundations of 3D geometry for robot manipulators

Participants: Cyril Cohen, Reynald Affeldt [AIST, Japan].

We formalized the 3D geometry concepts used in the description of kinematics chains, in particular: rotations, rigid body tranformations, screw motions, frame changes, and the Denavit-Hartenberg Convention. This lead to a publication to appear in the internaltional conference CPP 2017 [7].

5.8. Finites sets, finite maps, multisets, order types

Participant: Cyril Cohen.

We extend the Mathematical Components library with a module concerning finite sets (in potentially infinite types), finite maps and multisets. This module plays a crucial role in the formalization of nominal sets, multinomials, semi-algebraic sets, and many experimental developments.

We also extend the Mathematical Components library with a module concerning orders, lattices, and sets. This serves as an abstraction on various libraries, including the finite set library, semi-algebraic sets, finite reunions of intervals, and boolean predicates (in classical theories).

5.9. CoqEAL and modular large scale reflection

Participants: Cyril Cohen, Damien Rouhling.

Extending work by Guillaume Cano, Cyril Cohen, Maxime Dénès, Anders Mörtberg and Vincent Silès, we reimplemented the foundations of the CoqEAL library on Keller and Lasson's parametricity plug-in and provided a more robust translation mechanism. We illustrated the use of this enhanced version of CoqEAL on a new version of the traditional ring tactic. This lead to a publication at JFLA 2017 (Journées Francophones des Langages Applicatifs, the article actually is in English) [17].

5.10. Formalization of semi-algebraic sets

Participants: Yves Bertot, Cyril Cohen, Boris Djalal.

We developed the necessary results about first-order logical formulae to be able to define semi-algebraic sets and semi-algebraic functions in Coq. This required that we provide elements of language to describe quantification over blocks of variables. We show that the equality of semi-algebraic sets is decidable, thanks to the already formalized decision procedure based on quantifier elimination. We then show that our formalized semi-algebraic sets do satisfy general abstract interfaces for sets, as seen in section 5.8

In the long run this work will be instrumental to describe the output of cylindrical algebraic decomposition algorithms. Indeed, this output is usually made of semi-algebraic sets.

5.11. Formalizing the Spectral Theorem

Participant: Cyril Cohen.

We formalize the spectral theorem for normal, hermitian and unitary matrices (this work in progress is available at https://github.com/Barbichu/spectral) These results are useful in the study of rotations and rigid body transformations in dimension 3. This is a key ingredient of the singular value decomposition (useful in inverse kinematics, signal processing, and many other practical applications).

5.12. A formal proof of La Salle's invariance principle

Participants: Yves Bertot, Cyril Cohen, Damien Rouhling.

We started formalizing the proof of La Salle's invariance principle using the Coquelicot library, with the goal of using it to formalize the proof of stability of a control function for the inverted pendulum (a basic exercise that can serve as an introduction to problems in robotics). For now, I have proven a few properties of the set of limit points of a function.

5.13. Formalizing Delaunay triangulations

Participants: Yves Bertot, Wassim Haffaf.

We studied the applicability of the mathematical component library to describe Delaunay triangulation algorithms in the most abstract way. We also formalized a theorem on convex functions known as *Jensen's inequality*.

5.14. Formalizing Quantum Computing

Participant: Laurent Théry.

We have formalized an algorithm proposed by Peter Selinger to synthesize quantum gates. His approach mixes number theoretical notions and linear algebra, two aspects that are well covered by the Mathematical Components Library.

5.15. Formalizing De Bruijn Sequences

Participant: Laurent Théry.

De Bruijn sequences are combinatorial objects. We have shown how they can be generated by exhibiting a link with irreducible polynomials in finite fields, with a formal proof in Coq.

5.16. Formalizing Hanoi towers

Participant: Laurent Théry.

The problem of Hanoi towers is a standard example to explain recursion. While trying to write a formalization, we discovered that there exists an interesting generalisation. Starting with two arbitrary valid positions, the problem is to find an optimal solution to go from one to the other. The solution is somewhat counter-intuitive, and not always unique. We formalized it in Coq.

5.17. Implementation of Bourbaki's Theory of Sets in Coq

Participant: José Grimm.

A paper describing our implementation of the sets of natural numbers, of rational numbers and of real numbers has been published by the Journal of Formalized Reasoning [6].

We implemented Chapter 3, Section 7 (Inverse Limits and Direct Limits) and the start of Chapter 4 (Structures) of the Theory of Sets of Bourbaki, details are found in the Research Report [19]

5.18. Factorization of ordinal numbers

Participant: José Grimm.

Ordinal numbers have been designed at approximately the same time that the foundations of mathematics were being revisited, in the beginning of the 20th century. These objects cross the boundaries of set theory and pose especially difficult challenges when considering the task of formalizing mathematics. This is the reason why we concentrate on formal proofs concerning these objects.

An ordinal number x is said to be prime if $x > 1$ and for every factorisation $x = ab$, one of a or b is equal to x (the other factor is not necessarily equal to 1). Prime ordinals are of three kinds; a power of a power of ω, the successor of a power of ω, or a prime natural number. Every ordinal can uniquely be written as a product of primes, with the following restriction: if a is followed by b in the factor list then: if b is of the first kind, so is a and $a \geq b$, if a and b are natural numbers, then $a \leq b$. The proof can be found in an updated version of [20]

5.19. New logics for differential privacy

Participants: Benjamin Grégoire, Gilles Barthe [IMDEA], Noémie Fong [ENS], Marco Gaboardi [University at Buffalo], Justin Hsu [University of Pennsylvania], Pierre-Yves Strub [IMDEA].

We proposed new logics to work on examples from the differential privacy literature, a hoare logic based on the union bound [10] and a logic based on the deep connection between differential privacy and probabilistic couplings [11], [9].

5.20. Formalizing counter-measures for differential power analysis

Participants: Benjamin Grégoire, Gilles Barthe [IMDEA], Sonia Belaïd [Thales Communications & Security], François Dupressoir [IMDEA], Sebastian Faust [Ruhr Universität Bochum], Pierre-Alain Fouque [Université de Rennes and Institut Universitaire de France], François-Xavier Standaert [Université Catholique de Louvain], Pierre-Yves Strub [IMDEA], Rébecca Zucchini [ENS Cachan and Inria].

Differential power analysis (DPA) is a side-channel attack in which an adversary retrieves cryptographic material by measuring and analyzing the power consumption of the device on which the cryptographic algorithm under attack executes. We introduced new notions and models allowing to check the correctness of counter measures (known as *masking schemes*) [8], [22]. Based on this idea we have developed a compiler to transform an unmasked program into it masked version.

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR

We are currently members of two projects funded by the French national agency for research funding.

- BRUTUS "Chiffrements authentifiés et résistants aux attaques par canaux auxiliaires", started on October 1st, 2014, for 60 months, with a grant of 41 kEuros for Marelle. Other partners are Université de Rennes 1, CNRS, secrétariat Général de la défense et de la sécurité nationale, and Université des Sciences et Technologies de Lille 1. The corresponding researcher for this contract is Benjamin Grégoire.
- FastRelax, "Fast and Reliable Approximations", started on October 1st, 2014, for 60 months, with a grant of 75 kEuros for Marelle. Other partners are Inria Grenoble (ARIC project-team), LAAS-CNRS (Toulouse), Inria Saclay (Toccata and Specfun project-teams), and LIP6-CNRS (Paris). The corresponding researcher for this contract is Laurence Rideau.

6.2. International Initiatives

6.2.1. Inria International Partners

6.2.1.1. Informal International Partners

We work with the team of Adam Chlipala at MIT, in particular the engineer Paul Steckler, with whom we have regular meetings concerning the optimization of parts of the Coq system with respect to use cases provided by the MIT team, and the design of user-interface tools. This engineer had a visit of 6 weeks in France in April, three weeks in the pi.r2 team (mostly hosted by Matthieu Sozeau) and three weeks in the Marelle team, mostly hosted by Enrico Tassi and Maxime Dénès. The collaboration continues since that visit with a weekly phone conference.

6.3. International Research Visitors

6.3.1. Visits of International Scientists

We had visits by Gilles Barthe (IMDEA, Madrid, Spain) for 2 weeks, Benedikt Schmidt (IMDEA), for 2 weeks, François-Xavier Standaert (Université Catholique de Louvain, Crypto Group, Belgium), for 1 week, Sebastian Faust (Ruhr-University Bochum, Germany) for 1 week, François Dupressoir (IMDEA) for 1 week, Pierre-Yves Strub (IMDEA), for 1 week, and Peter Schwabe (Radboud University, Nijmegen, the Netherlands) for 3 days.

6.3.2. Visits to International Teams

Benjamin Grégoire visited IMDEA (Madrid, Spain) for two one-week trips.

Yves Bertot, Maxime Dénès, and Enrico Tassi visited Princeton University in June for the kick-off meeting of the *Expedition in Computing* entitled “the science of deep specification” funded by the NSF foundation.

Enrico Tassi visited the team of Jesper Bengtson at the IT-University of Copenhagen, Denmark.

Anders Mörtberg visited the team of Thierry Coquand at Chalmers and University of Göteborg in Sweden.

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Selection

7.1.1.1. Chair of Conference Program Committees

Yves Bertot is program co-chair, with Viktor Vafeiadis from MPI-SWS in Germany for the ACM conference *Certified Programs and Proofs* (CPP) to be held in Paris in January 2017. Most of the editorial activities took place in 2016.

7.1.1.2. Member of the Conference Program Committees

- Yves Bertot and Laurent Théry were members of the conference program committee for the conference *Interactive Theorem Proving* (ITP) and *User-Interfaces for Theorem Provers* (UITP).
- Cyril Cohen was a member ot the program committee for the 8th Coq workshop.

7.1.1.3. Reviewer

Cyril Cohen was reviewer for the conferences CSL 2016 and ITP 2016. Laurent Théry was a reviewer for the conferences TACAS'17 and CPP'17. Benjamin Grégoire was a reviewer for TACAS. Benjamin Grégoire was a reviewer for PoPL 2017.

7.1.2. Journal

7.1.2.1. Reviewer - Reviewing Activities

Cyril Cohen was a reviewer for *Journal of Automated Reasoning*. Laurent Théry was a reviewer for *Journal of Automated Reasoning* and *Journal of Symbolic Computation*. Yves Bertot was a reviewer for *Journal of Automated Reasoning* and *Computational Geometry: Theory and Applications*.

7.1.3. Invited Talks

Laurent Théry gave an invited talk at MAP'16 (*Mathematics, Algorithms, and Proofs*).

Cyril Cohen gave an invited talk at the ELFIC seminar on the Paris-Saclay campus (Elfic stands for *Éléments finis formellement vérifiés*).

7.1.4. Leadership within the Scientific Community

Yves Bertot and Maxime Dénès have been working on setting up a Consortium of users for the Coq system. The consortium should start in the early days of 2017. Yves Bertot, Enrico Tassi, and Maxime Dénès were invited to the kick-off meeting of the *Expedition in Computing* entitled "the science of deep specification" funded by the NSF foundation, along with three other developers from the pi.r2 project-team, as expert developers of the Coq system. This kick-off meeting took place in June.

7.1.5. Scientific Expertise

- Laurent Théry evaluated projects for the French national agency for research funding (ANR),

7.1.6. Research Administration

- José Grimm is a member of the local committee for Hygiene and Work safety,
- Cyril Cohen served several times as secretary for the local committee of project-team leaders,
- Benjamin Grégoire is a member of the committee on computer tools usage (CUMI) for the Sophia-Antipolis Méditerranée Inria center.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence : Cyril Cohen, mathematics oral exam, 30 hours, Classes préparatoires aux grandes écoles

Master : Laurent Théry gave a course at ENS Lyon (9 hours), a course at École des Mines (3 hours), and a course at University de Marseille (3 hours). Yves Bertot gave a one-week introductory course on Coq at University of Nice (21 hours). Enrico Tassi organized a one-week advanced course on Coq and Mathematical Components for students of ENS Lyon and University of Nice (30 hours). There were two instances of this school, in January and in November, teachers for this course were Enrico Tassi, Yves Bertot, Cyril Cohen, Laurence Rideau, and Laurent Théry.

7.2.2. Supervision

PhD in progress : Boris Djalal, started in October 2015, supervised by Yves Bertot and Cyril Cohen

PhD in progress : Cécile Baritel-Ruet, started in October 2016, supervised by Yves Bertot and Benjamin Grégoire

PhD in progress : Sophie Bernard, started in October 2016, supervised by Yves Bertot and Laurence Rideau

PhD in progress : Damien Rouhling, started in October 2016, supervised by Yves Bertot and Cyril Cohen.

7.2.3. Juries

Yves Bertot was member of the defense committee for the thesis of Jacques-Henri Jourdan.

7.3. Popularization

Laurent Théry gave talks in the context of “Fête de la science”.

8. Bibliography

Major publications by the team in recent years

[1] G. BARTHE, B. GRÉGOIRE, S. HERAUD, S. Z. BÉGUELIN. *Computer-Aided Security Proofs for the Working Cryptographer*, in "Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings", Lecture Notes in Computer Science, Springer, 2011, vol. 6841, pp. 71-90, Best Paper Award

[2] Y. BERTOT, G. GONTHIER, S. O. BIHA, I. PAŞCA. *Canonical Big Operators*, in "Proceedings of the 21st International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2008)", Lecture Notes in Computer Science, Springer, August 2008, vol. 5170, pp. 12–16, http://hal.inria.fr/inria-00331193/

[3] G. GONTHIER, A. ASPERTI, J. AVIGAD, Y. BERTOT, C. COHEN, F. GARILLOT, S. LE ROUX, A. MAHBOUBI, R. O'CONNOR, S. OULD BIHA, I. PASCA, L. RIDEAU, A. SOLOVYEV, E. TASSI, L. THÉRY. *A Machine-Checked Proof of the Odd Order Theorem*, in "ITP 2013, 4th Conference on Interactive Theorem Proving", Rennes, France, S. BLAZY, C. PAULIN, D. PICHARDIE (editors), LNCS, Springer, 2013, vol. 7998, pp. 163-179 [*DOI :* 10.1007/978-3-642-39634-2_14], http://hal.inria.fr/hal-00816699

[4] G. GONTHIER, A. MAHBOUBI, L. RIDEAU, E. TASSI, L. THÉRY. *A Modular Formalisation of Finite Group Theory*, in "Proceedings of the 20th International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2007)", K. SCHNEIDER, J. BRANDT (editors), LNCS, Springer-Verlag, September 2007, vol. 4732, pp. 86-101, http://hal.inria.fr/inria-00139131

Publications of the year

Articles in International Peer-Reviewed Journals

[5] G. CANO, C. COHEN, M. DÉNÈS, A. MÖRTBERG, V. SILES. *Formalized Linear Algebra over Elementary Divisor Rings in Coq*, in "Logical Methods in Computer Science", June 2016 [*DOI :* 10.2168/LMCS-12(2:7)2016], https://hal.inria.fr/hal-01081908

[6] J. GRIMM. *Implementation of Bourbaki's Elements of Mathematics in Coq: Part Two, From Natural Numbers to Real Numbers*, in "Journal of Formalized Reasoning", 2016, vol. 9, n^{o} 2, 52 p. [*DOI :* 10.6092/ISSN.1972-5787/4771], https://hal.inria.fr/hal-01415375

International Conferences with Proceedings

[7] R. AFFELDT, C. COHEN. *Formal Foundations of 3D Geometry to Model Robot Manipulators*, in "Conference on Certified Programs and Proofs 2017", Paris, France, January 2017, https://hal.inria.fr/hal-01414753

[8] G. BARTHE, S. BELAÏD, F. DUPRESSOIR, P.-A. FOUQUE, B. GRÉGOIRE, P.-Y. STRUB, R. ZUCCHINI. *Strong Non-Interference and Type-Directed Higher-Order Masking*, in "23rd ACM Conference on Computer and Communications Security", Vienne, Austria, October 2016, pp. 116 - 129 [*DOI :* 10.1145/2976749.2978427], https://hal.inria.fr/hal-01410216

[9] G. BARTHE, N. FONG, M. GABOARDI, B. GRÉGOIRE, J. HSU, P.-Y. STRUB. *Advanced Probabilistic Couplings for Differential Privacy*, in "23rd ACM Conference on Computer and Communications Security", Vienne, Austria, October 2016, pp. 55 - 67 [*DOI :* 10.1145/2976749.2978391], https://hal.inria.fr/hal-01410196

[10] G. BARTHE, M. GABOARDI, B. GRÉGOIRE, J. HSU, P.-Y. STRUB. *A program logic for union bounds*, in "The 43rd International Colloquium on Automata, Languages and Programming", Rome, Italy, July 2016 [*DOI :* 10.4230/LIPIcs.ICALP.2016.107], https://hal.inria.fr/hal-01411095

[11] G. BARTHE, M. GABOARDI, B. GRÉGOIRE, J. HSU, P.-Y. STRUB. *Proving Differential Privacy via Probabilistic Couplings*, in "Thirty-First Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)", New York, United States, July 2016, pp. 749 - 758 [*DOI :* 10.1145/2933575.2934554], https://hal.inria.fr/hal-01411097

[12] S. BERNARD, Y. BERTOT, L. RIDEAU, P.-Y. STRUB. *Formal Proofs of Transcendence for e and π as an Application of Multivariate and Symmetric Polynomials*, in "Certified Programs and Proofs", St Petersburg, Florida, United States, J. AVIGAD, A. CHLIPALA (editors), ACM Press, January 2016, 12 p. , https://hal.inria.fr/hal-01240025

[13] C. COHEN, B. DJALAL. *Formalization of a Newton Series Representation of Polynomials*, in "Certified Programs and Proofs", St Petersburg, Florida, United States, J. AVIGAD, A. CHLIPALA (editors), January 2016, https://hal.inria.fr/hal-01240469

[14] C. DUNCHEV, C. SACERDOTI COEN, E. TASSI. *Implementing HOL in an Higher Order Logic Programming Language*, in "Logical Frameworks and Meta Languages: Theory and Practice", Porto, Portugal, LFMTP '16, ACM, June 2016, 10 p. [*DOI :* 10.1145/2966268.2966272], https://hal.inria.fr/hal-01394686

[15] A. FAITHFULL, J. BENGTSON, E. TASSI, C. TANKINK. *Coqoon An IDE for interactive proof development in Coq*, in "TACAS", Eindhoven, Netherlands, April 2016, https://hal.inria.fr/hal-01242295

[16] B. GRÉGOIRE, E. TASSI. *Boolean reflection via type classes*, in "Coq Workshop", Nancy, France, August 2016, https://hal.inria.fr/hal-01410530

National Conferences with Proceedings

[17] C. COHEN, D. ROUHLING. *A refinement-based approach to large scale reflection for algebra*, in "JFLA 2017 - Vingt-huitième Journées Francophones des Langages Applicatifs", Gourette, France, January 2017, https://hal.inria.fr/hal-01414881

Research Reports

[18] G. GONTHIER, A. MAHBOUBI, E. TASSI. *A Small Scale Reflection Extension for the Coq system*, Inria Saclay Ile de France, 2016, n^{O} RR-6455, https://hal.inria.fr/inria-00258384

[19] J. GRIMM. *Implementation of Bourbaki's Elements of Mathematics in Coq: Part Three Structures*, Inria Sophia Antipolis, 2016, n^{O} RR-8997, 115 p. , https://hal.inria.fr/hal-01412037

[20] J. GRIMM. *Implementation of Bourbaki's Elements of Mathematics in Coq: Part Two; Ordered Sets, Cardinals, Integers*, Inria Sophia Antipolis ; Inria, 2016, n^{O} RR-7150, 730 p. , https://hal.inria.fr/inria-00440786

Other Publications

[21] B. AHRENS, R. MATTHES, A. MÖRTBERG. *From signatures to monads in UniMath*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01410487

[22] G. BARTHE, F. DUPRESSOIR, S. FAUST, B. GRÉGOIRE, F.-X. STANDAERT, P.-Y. STRUB. *Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01414009

[23] C. COHEN, T. COQUAND, S. HUBER, A. MÖRTBERG. *Cubical Type Theory: a constructive interpretation of the univalence axiom*, October 2016, Accepted for publication in LIPIcs, https://hal.inria.fr/hal-01378906

[24] A. FAITHFULL, J. BENGTSON, E. TASSI, C. TANKINK. *Coqoon An IDE for interactive proof development in Coq*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01410450

[25] F. GUIDI, C. SACERDOTI COEN, E. TASSI. *Implementing Type Theory in Higher Order Constraint Logic Programming*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01410567

References in notes

[26] M. JOLDES, V. POPESCU, J.-M. MULLER. *Tight and rigourous error bounds for basic building blocks of double-word arithmetic*, July 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01351529