Activity Report 2017

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:

A2.1.11. - Proof languages
A2.4.3. - Proofs
A4.5. - Formal methods for security
A5.10.3. - Planning
A7.2. - Logic in Computer Science
A7.2.3. - Interactive Theorem Proving
A7.2.4. - Mechanized Formalization of Mathematics
A8.3. - Geometry, Topology
A8.4. - Computer Algebra
A8.10. - Computer arithmetic

Other Research Topics and Application Domains:

B6.1. - Software industry
B9.4.1. - Computer science
B9.4.2. - Mathematics

1. Personnel

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]

Post-Doctoral Fellows

Anders Mörtberg [Inria, until Sep 2017]
Florian Steinberg [Inria, from Oct 2017]

PhD Students

Cécile Baritel-Ruet [Université Côte d'Azur (financement ENS Cachan)]
Sophie Bernard [Université Côte d'Azur]
Boris Djalal [Inria]
Mohamad El Laz [Inria, from Dec 2017]
Damien Rouhling [Université Côte d'Azur (financement ENS Lyon)]

Technical staff

Maxime Dénès [Inria, until Sep 2017]
Matej Košík [Inria, until Sep 2017]

Interns

Maxime Bombar [Ecole Normale Supérieure Paris, from Jun 2017 until Jul 2017]
Luc Chabassier [Ecole Normale Supérieure Paris, from Jun 2017 until Aug 2017]

Clément Sartori [Inria, from Feb 2017 until Jun 2017]

Administrative Assistant
Nathalie Bellesso [Inria]

Visiting Scientist
Vincent Laporte [IMDEA Madrid, from Oct 2017]

External Collaborators
Gilles Barthe [IMDEA Madrid, from Apr 2017, HDR]
Loïc Pottier [Ministère de l'Education Nationale, HDR]
Maxime Dénès [InriaSoft, from Oct 2017]
Pierre-Marie Pédrot [Max-Planck Institute, from Oct 2017]

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. Highlights of the Year

4.1. Highlights of the Year

Our effort to setup a consortium around the Coq system has made significant progress this year as illustrated by two noticeable events: the first engineer was hired by InriaSoft for this consortium (Maxime Dénès) and the first funding was collected from academic partners (the first is Princeton University).

5. New Software and Platforms

5.1. Coq

The Coq Proof Assistant
KEYWORDS: Proof - Certification - Formalisation
SCIENTIFIC DESCRIPTION: Coq is an interactive proof assistant based on the Calculus of (Co-)Inductive Constructions, extended with universe polymorphism. This type theory features inductive and co-inductive families, an impredicative sort and a hierarchy of predicative universes, making it a very expressive logic. The calculus allows to formalize both general mathematics and computer programs, ranging from theories of finite structures to abstract algebra and categories to programming language metatheory and compiler verification. Coq is organised as a (relatively small) kernel including efficient conversion tests on which are built a set of higher-level layers: a powerful proof engine and unification algorithm, various tactics/decision procedures, a transactional document model and, at the very top an IDE.

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, ...

RELEASE FUNCTIONAL DESCRIPTION: Version 8.7 features a large amount of work on cleaning and speeding up the code base, notably the work of Pierre-Marie Pédrot on making the tactic-level system insensitive to existential variable expansion, providing a safer API to plugin writers and making the code more robust.

New tactics: Variants of tactics supporting existential variables "eassert", "eenough", etc. by Hugo Herbelin. Tactics "extensionality in H" and "inversion_sigma" by Jason Gross, "specialize with" accepting partial bindings by Pierre Courtieu.

Cumulative Polymorphic Inductive Types, allowing cumulativity of universes to go through applied inductive types, by Amin Timany and Matthieu Sozeau.

The SSReflect plugin by Georges Gonthier, Assia Mahboubi and Enrico Tassi was integrated (with its documentation in the reference manual) by Maxime Dénès, Assia Mahboubi and Enrico Tassi.

The "coq_makefile" tool was completely redesigned to improve its maintainability and the extensibility of generated Makefiles, and to make "_CoqProject" files more palatable to IDEs by Enrico Tassi.

A lot of other changes are described in the CHANGES file.
NEWS OF THE YEAR: Version 8.7 was released in October 2017 and version 8.7.1 in December 2017, development started in January 2017. This is the second release of Coq developed on a time-based development cycle. Its development spanned 9 months from the release of Coq 8.6 and was based on a public road-map. It attracted many external contributions. Code reviews and continuous integration testing were systematically used before integration of new features, with an important focus given to compatibility and performance issues.

The main scientific advance in this version is the integration of cumulative inductive types in the system. More practical advances in stability, performance, usability and expressivity of tactics were also implemented, resulting in a mostly backwards-compatible but appreciably faster and more robust release. Much work on plugin extensions to Coq by the same development team has also been going on in parallel, including work on JSCoq by Emilio JG Arias, Ltac 2 by P.M-Pédrot, which required synchronised changes of the main codebase. In 2017, the construction of the Coq Consortium by Yves Bertot and Maxime Dénès has greatly advanced and is now nearing its completion.

- Participants: Abhishek Anand, C. J. Bell, Yves Bertot, Frédéric Besson, Tej Chajed, Pierre Courtieu, Maxime Denes, Julien Forest, Emilio Jesús Gallego Arias, Gaëtan Gilbert, Benjamin Grégoire, Jason Gross, Hugo Herbelin, Ralf Jung, Matej Kosik, Sam Pablo Kuper, Xavier Leroy, Pierre Letouzey, Assia Mahboubi, Cyprien Mangin, Érik Martin-Dorel, Olivier Marty, Guillaume Melquiond, Pierre-Marie Pédrot, Benjamin C. Pierce, Lars Rasmusson, Yann Régis-Gianas, Lionel Rieg, Valentin Robert, Thomas Sibut-Pinote, Michael Soegtrop, Matthieu Sozeau, Arnaud Spiwack, Paul Steckler, George Stelle, Pierre-Yves Strub, Enrico Tassi, Hendrik Tews, Laurent Théry, Amin Timany, Vadim Zaliva and Théo Zimmermann
- Partners: CNRS - Université Paris-Sud - ENS Lyon - Université Paris-Diderot
- Contact: Matthieu Sozeau
- Publication: The Coq Proof Assistant, version 8.7.1
- URL: http://coq.inria.fr/

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

5.3. ELPI

Embeddable Lambda Prolog Interpreter
KEYWORDS: Constraint Programming - Programming language - Higher-order logic
FUNCTIONAL DESCRIPTION: ELPI is a lambdaProlog interpreter written in OCaml, easy to embed in software written in the same language.

- Contact: Enrico Tassi

5.4. 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.

RELEASE FUNCTIONAL DESCRIPTION: The library includes 16 more theory files, covering in particular field and Galois theory, advanced character theory, and a construction of algebraic numbers.

- Participants: Alexey Solovyev, Andrea Asperti, Assia Mahboubi, Cyril Cohen, Enrico Tassi, François Garillot, Georges Gonthier, Ioana Pasca, Jeremy Avigad, Laurence Rideau, Laurent Théry, Russell O'Connor, Sidi Ould Biha, Stéphane Le Roux and Yves Bertot
- Contact: Assia Mahboubi
- URL: http://math-comp.github.io/math-comp/

5.5. Semantics

KEYWORDS: Semantic - Programming language - Coq
FUNCTIONAL DESCRIPTION: A didactical Coq development to introduce various semantics styles. Shows how to derive an interpreter, a verifier, or a program analyser from formal descriptions, and how to prove their consistency.

This is a library for the Coq system, where the description of a toy programming language is presented. The value of this library is that it can be re-used in classrooms to teach programming language semantics or the Coq system. The topics covered include introductory notions to domain theory, pre and post-conditions, abstract interpretation, and the proofs of consistency between all these point of views on the same programming language. Standalone tools for the object programming language can be derived from this development.

- Participants: Christine Paulin and Yves Bertot
- Contact: Yves Bertot
- URL: http://www-sop.inria.fr/members/Yves.Bertot/proofs/semantics_survey.tgz

5.6. Ssreflect

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

- Participants: Assia Mahboubi, Cyril Cohen, Enrico Tassi, Georges Gonthier, Laurence Rideau, Laurent Théry and Yves Bertot
- Contact: Yves Bertot
- URL: http://math-comp.github.io/math-comp/

5.7. AutoGnP

KEYWORDS: Formal methods - Security - Cryptography

FUNCTIONAL DESCRIPTION: autoGnP 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 years we extended the tool to be able to deal with schemes based on cyclic groups and bilinear maps.

- Participants: Benjamin Grégoire, Gilles Barthe and Pierre-Yves Strub
- Contact: Gilles Barthe
- URL: https://github.com/ZooCrypt/AutoGnP

6. New Results

6.1. Implementing Theorem Proving in Higher Order Logic Programming

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

We are designing a Coq plugin named elpi providing an extension language based on λ-prolog to write new commands and tactics. This year, we re-designed the constraint handling engine of the elpi interpreter. Luc Chabassier illustrated the use of this extension on the problem of generating automatically equality test functions for arbitrary recursive types, together with their proof of correctness.

Another experiment was conducted by Cyril Cohen on using elpi to compute genericity theorems. For now the unary and binary cases have been covered in a concise fashion.

An article on this topic has been submitted to MSCS [19], a presentation will also be given at the CoqPL workshop [21].

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

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

The work of previous years on Coqoon has been published in an international journal [6].

6.3. Proofs of transcendence

Participants: Sophie Bernard, Yves Bertot, Laurence Rideau.

Sophie Bernard completed a proof of the Lindemann-Weierstrass theorem concerning the algebraic independence of spans of exponentials of rationally dependent numbers. This result required that we extend the theory of symmetric multivariate polynomials in order to formalize the notion of conjugates of a polynomial. This was described in an article presented at an international conference [13] and at a workshop associated to ANR project FastRelax.

6.4. 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], Simon Huber [Chalmers University, Sweden], Ralph Matthes [CNRS, University of Toulouse].

This work mainly concerns Univalent Foundations and Homotopy Type Theory, especially in the form of cubical type theory. The code is visible at https://github.com/mortberg/cubicaltt. This year, Anders Mörtberg has been working on formalizing cubical set models in univalent type theory and on extending cubical type theory with a general class of higher inductive types, in collaboration with Cyril Cohen, Thierry Coquand and Simon Huber.

Anders Mörtberg extended work with Ralph Matthes, Benedikt Ahrens and Vladimir Voevodsky on the representation of syntax of programming languages using category theory in univalent type theory. This paper was accepted for publication in JAR.

Anders Mörtberg also prepared a series of lectures introducing to cubical type theory. this lead to invited talks at the workshops "Type Theory based Tools (TTT)", and "Syntax and Semantics of Type Theory".

6.5. Formal study of double-word arithmetic algorithms

Participants: Laurence Rideau, Erik Martin-Dorel [IRIT Toulouse], 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" [24]. The formalization is progressing. A notable event is that we detected a small error in the article proof, which required a correction by the authors.

6.6. Formal study of comparisons between numbers in different formats

Participants: Laurent Théry, Arthur Blot, Jean-Michel Muller [CNRS and ENS Lyon].

We show how a library of formalized mathematics about continuous functions can be used to derive an algorithm that compares two floating point number one in base 2 and one in base 10 [14].

6.7. A formal study of the towers of Hanoi

Participant: Laurent Théry.

The towers of Hanoi is a classical example that illustrates the power of recursive programming. Proving that the recursive program solves the problem is elementary but proving that it is a minimal solver is harder. This is even more difficult if we consider the general problem that considers arbitrary starting and final positions. We present the formalisation of this problem in the Mathematical Component Library [22].

6.8. Formaly study of algorithms to compute π

Participants: Yves Bertot, Laurence Rideau, Laurent Théry.

We studied formal proofs for several algorithms used to computed π to very high precisions, the famous BBP formula and an algorithm derived from it and another algorithm based on arithmetic-geometric means that is used in the MPFR library. These results show that Coq can be used directly to compute a million decimals or the billionth hexa-decimal in isolation [5].

6.9. Formal foundations of 3D geometry for robot manipulators

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

We resumed our collaboration with the team at AIST for the formal description of robotics aspects [7]. Reynald Affeldt visited Sophia Antipolis for 10 days during which we improved the connection between our library for algebra and the Coquelicot library for analysis.

6.10. Formalization of Analysis concepts

Participants: Cyril Cohen, Damien Rouhling.

To study problems in control, we worked on the notion of compacts and showed how to express it using filters, as in Coquelicot.

We experimented with sets of notations to make computing with limits simpler. We also generalized the notion of "big enough" that can usually be found when reasoning about functions at infinity (or sequences) so that it now works with arbitrary filters. Finally, we started experimenting with a new point of view on "small o" notations.

We also started work on formalizing in Coq the Cauchy-Lipschitz theorem (also known as Picard-Lindelöf), which proves the existence and uniqueness of solutions to differential equations.

We expect all these small advances to prepare the ground for work on various aspects of robotics and control. Part of this work was published in an international conference [20].

6.11. Formalization of proofs in control theory

Participants: Damien Rouhling, Cyril Cohen.

We worked on dynamical systems and differential equations. Damien Rouhling fully formalized in Coq LaSalle's invariance principle with the help of Cyril Cohen. This principle uses Lyapunov functions to prove the stability of a dynamical system defined by a differential equation. We wrote a paper about this formalization, which has been published in the proceedings of the ITP 2017 conference [15].

We improved this formalization to apply this principle to an example of robotics and control theory. We formalized in Coq the correctness of a control function for an inverted pendulum. Damien Rouhling wrote a paper about this, accepted for publication at an international conference in early 2018 [20].

6.12. Formalization of graph algorithms

Participants: Yves Bertot, Cyril Cohen, Ran Chen [Chinese Academy of Science], Jean-Jacques Lévy [Pi.r2 and Chinese Academy of Science], Clément Sartori, Laurent Théry.

We studied algorithms to compute strongly connected components in graphs, as a way to prepare a comparative study with the work of Levy and Chen: "A Semi-Automatic Proof of Strong Connectivity" [23].

In a similar vein, Yves Bertot and Clément Sartori have been studying the combinatorial aspects of triangulations, and in particular Delaunay triangulations, seen as graphs. In the long run, we expect this effort to contribute to formal descriptions of Voronoi diagrams and uses in robot motion planning.

6.13. Extension of the CoqEAL library

Participants: Cyril Cohen, Enrico Tassi.

The CoqEAL library provides a framework to connect efficient executable functional programs to the algorithms that are described formally using the mathematical components library. Key aspects rely on the capacity to refine abstract views of the algorithms and data into concrete views, where the efficiency can be fine-tuned. For this refinement, we also need to rely on properties of programming languages such as parametricity. We experimented on relying on the ELPI plugin to implement this parametricity feature. In the long run, this means that the ELPI plugin should play an instrumental role in making CoqEAL easy to use and to extend.

6.14. Formalizing Exterior Algebras

Participants: Maxime Bombar, Cyril Cohen.

We formalized exterior algebras as vector spaces with dimension 2^n. This provides an alternative representation to that constructed earlier by Laurent Théry and Laurent Fuchs. The new representation is closer to the objects found in the mathematical components library.

6.15. Formalizing Cylindrical Algebraic Decomposition

Participants: Boris Djalal, Yves Bertot, Cyril Cohen.

Our study of cylindrical algebraic decomposition requires that we find a good representation of semi-algebraic sets, which are usually determined by a collections of comparisons between polynomial formulas. We wrote an article on this topic, which has been accepted for publication at an international conference to be held in early 2018 [18].

6.16. Formal study of probabilistic programs

Participants: Benjamin Grégoire, Gilles Barthe [IMDEA], François Dupressoir [University of Surrey], Thomas Espitau [UPMC Paris 6], Sebastian Faust [Ruhr Universitat Bochum], Justin Hsu [University of Pennsylvania], Vitor Pereira [INESC TEC], François-Xavier Standaert [Université Catholique de Louvain].

This year, we proposed new logics to make a link between "probabilistic Relationnal Hoare Logic" and the traditionnal notion of couplings from probability theory [12]. We have also showed that coupling can be use to prove non-relationnal properties like uniformity and probabilistic independence [11].

We used Easycrypt to prove the security of Secure Function Evaluation (SFE) based on garble circuits [9].

6.17. Generating Efficient Resistant Code

Participants: Benjamin Grégoire, José Bacelar Almeida [INESC TEC], Manuel Barbosa [INESC TEC], Gilles Barthe [IMDEA], Arthur Blot [ENS Lyon], Vincent Laporte [IMDEA], Tiago Oliveira [INESC TEC], Hugo Pacheco [INESC TEC], Benedikt Schmidt [Google Inc.], Pierre-Yves Strub [Ecole Polytechnique].

We develop a certified compiler named Jasmin to generate high-speed and high-assurance cryptographic code.

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/models allowing to check the correctness of counter measures (masking schemes) [10].

6.18. Formal Security Proof in EasyCrypt: case studies and extensions

Participants: Cécile Baritel-Ruet, Benjamin Grégoire.

We completed a formal proof of security for CMAC, a scheme for cipher-based message authentication code. A publication is being submitted on this topic. We also experimented on a formal study of the forking lemma, which is present in many security proofs for signing schemes that rely on lattice problems.

The lessons derived from these experiments lead us to proposing new tools for matching instructions and unifying formulas with meta-variables in EasyCrypt.

6.19. Formalizing Bourbaki-style mathematics

Participant: José Grimm.

Most of the work described here is inspired by the experiment of giving formal proofs in Coq of the exercises found in Bourbaki's exposition of set theory. However, some of the results go beyond what can be found in Bourbaki.

We studied order relations by proving several properties about the *length* and *width* of order relations, for instance showing that when a set has $nm + 1$ elements, the lengh or the with of any order on this set is larger than either n or m. We then considered similar theorems on the set of all parts of a given set, ordered by inclusion. In particular, this gives formal proofs of results by Dilworth and Erdös and Zserkeres.

We also studied ordinal addition, which is non-commutative. Given a finite sequence of ordinals, one can compute the number of different results of the sum of these elements, depending on the order in which this sequence is taken. There is an explicit formula for this number, with a proof that we formalized.

Last, we studied a footnote from Bourbaki, that indicates that 1 is a notation for a term whose normal form has several tens of thousands of signs. We compute this size (about 10^{13} or 10^{60} depending on whether some constructs are given by axioms or by definitions) and provide statistics on the distributions of signs in the normal form.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

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

- TECAP "Analyse de protocoles, Unir les outils existants", starting on October 1st, 20117, for 60 months, with a grant of 89 kEuros. Other partners are Inria teams PESTO (Inria Nancy grand-est), Ecole Polytechnique, ENS Cachan, IRISA Rennes, and CNRS. The corresponding researcher for this contract is Benjamin Grégoire.
- SafeTLS "La sécurisation de l'Internet du futur avec TLS 1.3" started on October 1st, 2016, for 60 months, with a grant of 147kEuros. Other partners are Université de Rennes 1, and secrétariat Général de la Défense et de la Sécurité Nationale. The corresponding researcher for this contract is Benjamin Grégoire.
- 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.

7.2. European Initiatives

7.2.1. Collaborations with Major European Organizations

We have sustained collaborations with the team of Thierry Coquand at Chalmers and the University of Göteborg in Sweden and with the team of Gilles Barthe at IMDEA in Spain.

7.3. International Initiatives

7.3.1. Informal International Partners

In September, we organized a meeting on formal proofs for cryptography, with the following attendants: Manuel Barbosa (Portugal), Gilles Barthe (Spain), Vincent Laporte (Spain), Jose Carlos Bacelar Almeida (Portugal), Pierre-Yves Strub (France), Ko Stoffelen (the Netherlands), Benoit Viguier (the Netherlands), Chitchanok Chuengsatiansup (France).

We have frequent visits by Gilles Barthe, François Dupressoir (IMDEA, Madrid) and visits of Benjamin Grégoire at IMDEA Madrid.

Benjamin Grégoire visited University of Minho in May to work on the Jasmin compiler with Manuel Barbosa.

In our activity to setup the Coq consortium, we have frequent interaction with A. Appel (U. Princeton), B. Pierce (U. Penn), Zhong Shao (Yale University), A. Chlipala (MIT), and G. Morrissett (Cornell University).

We received Reynald Affeldt from AIST for a 10-days visit in November.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Member of the Organizing Committees

- Anders Mörtberg was an organizer of the 3rd workshop on Homotopy Type Theory and Univalent Foundations in Oxford, 8-9 September.

8.1.1.2. Chair of Conference Program Committees

- Yves Bertot was program committee co-chair for CPP'17 (Certified Programs and Proofs), in Paris, in January 2017.
- Yves Bertot is program committee co-chair for CoqPL'18 (Coq for Programming Lanugages), in Los Angeles, in January 2018.

8.1.1.3. Member of the Conference Program Committees

- Laurence Rideau was member of the program committee for JFLA'2018 (Journées francophones des langages applicatifs).

8.1.1.4. Reviewer

- Members of the team reviewed papers for JFLA (Journées Francophones des Langages Applicatifs), PoPL (Principles of Programming Languages), CPP (Certified Programs and Proofs), ITP (Interactive Theorem Proving), LPAR (Logic for Programming, Artificial Inteligence, and Reasoning), TACAS (Tools and Algorithms for the Construction and Analysis of Systems).

8.1.2. Journal

8.1.2.1. Reviewer - Reviewing Activities

- Members of the team reviewed papers for JAR (Journal of Automated Reasoning), and MSCS (Mathematical Structures in Computer Science).

8.1.3. Invited Talks

- Anders Mörtberg gave an invited talk at TTT (Type-Theory based Tools) in Paris in January and an invited talk at the workshop on Syntax and Semantics of Type Theory in Ljubljana in February.
- Cyril Cohen was invited for a talk at the workshop on Real Verification in South Korea in July.
- Damien Rouhling gave an invited talk at a meeting of the ANR-funded FastRelax project.

8.1.4. Scientific Expertise

- Yves Bertot performed a project review for the Dutch research funding agency (NWO).

8.1.5. Research Administration

- Yves Bertot is a member of the "Bureau du comité des projets".
- Yves Bertot is a member of the scientific committee for Academy "RISE" of University Côte d'azur.
- Yves Bertot was a member of the national working group for the strategic plan of Inria.
- Benjamin Grégoire is a member of the committee on the computer tool usage (CUMI) for the Sophia-Antipolis Méditerranée Inria center.
- José Grimm is a member of the local committee for hygiene and work safety.
- Laurence Rideau was a member of the Jury for hiring new researchers at Inria Sophia Antipolis (Jury d'admissibilité de chargés de recherche, Inria Sophia Antipolis Méditerranée).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Doctorat: Enrico Tassi organized an advanced school on Coq and the Mathematical Components library, where Laurence Rideau, Cyril Cohen, Laurent Théry, and Yves Bertot gave lectures and supervised laboratory sessions. This school took place in December and had 12 attendants.

Doctorat: Enrico gave a course "Type Theory, The Coq proof assistant", at the University of Padova in June.

Master: Yves Bertot organized an introductory school on Coq. This school took place in January and had 12 attendants.

Licence: Sophie Bernard gave 54 hours of lectures on probabilities at University of Nice Sophia Antipolis.

Licence: Damien Rouhling taught about 60 hours at University Nice Sophia Antipolis: differential calculus, Fourier analysis, and C programming (First year students).

Licence: Boris Djalal taught 4 hours of computer science for first year students in a "classe préparatoire aux grandes écoles".

Licence: Cécile Baritel-Ruet taught 30 hours of computer science for first year students at Université de Nice, and 12 hours of lectures on computer science history.

Licence: Laurence Rideau taught 10 hours of computer science in a "classe préparatoire aux grandes écoles"

Licence: Cyril Cohen gives mathematics exercises in a "classe préparatoire aux grandes écoles".

Master: Laurent Théry taught 3 hours on "introduction to computer verified proof" at Ecole des Mines de Paris,

8.2.2. Supervision

PhD in progress : Cécile Baritel-Ruet, "Formal verification of Security with EasyCrypt", started October 2016, supervised by Benjamin Grégoire and Yves Bertot,

PhD in progress : Sophie Bernard, "Formal proofs for transcendance", started October 2016, supervised by Yves Bertot and Laurence Rideau,

PhD in progress : Boris Djalal, "Formal verification of cylindrical algebraic decomposition", supervised by Cyril Cohen and Yves Bertot,

PhD in progress : Mohammad El Laz, "Formal study of Security", started December 2017, supervised by Benjamin Grégoire and Tamara Rezk (Indes Inria project team),

PhD in progress, : Damien Rouhling, "Formal proofs for control and robotics", started in October 2016, supervised by Yves Bertot and Cyril Cohen.

8.2.3. Juries

- Laurent Théry attended the middle thesis review for David Braun, in Strasbourg,
- Enrico Tassi was a member of the Jury for the defence of Roberto Blanco Martinez (Ecole Polytechnique),
- Laurent Théry was a member of the Jury for the defence of Thomas Sibut-Pinote (Ecole Polytechnique).

8.3. Popularization

Laurent Théry gave a talk in high-school (Centre International de Valbonne) in the context of the annual "Fête de la Science".

Damien Rouhling and Cécile Baritel-Ruet participated to the event "My thesis in 180 seconds" at the regional level.

9. 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] Y. BERTOT, L. RIDEAU, L. THÉRY. *Distant decimals of π: Formal proofs of some algorithms computing them and guarantees of exact computation*, in "Journal of Automated Reasoning", 2017, pp. 1-45, https://arxiv.org/abs/1709.01743 , forthcoming, https://hal.inria.fr/hal-01582524

[6] A. FAITHFULL, J. BENGTSON, E. TASSI, C. TANKINK. *Coqoon*, in "International Journal on Software Tools for Technology Transfer", May 2017, https://hal.inria.fr/hal-01410450

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] J. B. ALMEIDA, M. BARBOSA, G. BARTHE, A. BLOT, B. GRÉGOIRE, V. LAPORTE, T. OLIVEIRA, H. PACHECO, B. SCHMIDT, P.-Y. STRUB. *Jasmin: High-Assurance and High-Speed Cryptography*, in "CCS 2017 - Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security", Dallas, United States, October 2017, pp. 1-17, https://hal.archives-ouvertes.fr/hal-01649140

[9] J. B. ALMEIDA, M. BARBOSA, G. BARTHE, F. DUPRESSOIR, B. GRÉGOIRE, V. LAPORTE, V. PEREIRA. *A Fast and Verified Software Stack for Secure Function Evaluation*, in "CCS 2017 - ACM SIGSAC Conference on Computer and Communications Security", Dallas, United States, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017, ACM, October 2017, pp. 1-18, https://hal.archives-ouvertes.fr/hal-01649104

[10] 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*, in "Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Paris, France, Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, April 2017, vol. 10210, pp. 535–566, https://hal.inria.fr/hal-01414009

[11] G. BARTHE, T. ESPITAU, B. GRÉGOIRE, J. HSU, P.-Y. STRUB. *Proving uniformity and independence by self-composition and coupling*, in "LPAR 2017 - International Conferences on Logic for Programming, Artificial Intelligence and Reasoning", Maun, Botswana, LPAR 2017 - International Conferences on Logic for Programming, Artificial Intelligence and Reasoning, May 2017, 19 p. , http://hal.upmc.fr/hal-01541198

[12] G. BARTHE, B. GRÉGOIRE, J. HSU, P.-Y. STRUB. *Coupling proofs are probabilistic product programs*, in "POPL 2017 - Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages", Paris, France, ACM, January 2017, vol. 52, n^{o} 1, pp. 161-174 [*DOI :* 10.1145/3009837.3009896], https://hal.archives-ouvertes.fr/hal-01649028

[13] S. BERNARD. *Formalization of the Lindemann-Weierstrass Theorem*, in "Interactive Theorem Proving", Brasilia, Brazil, September 2017, https://hal.inria.fr/hal-01647563

[14] A. BLOT, J.-M. MULLER, L. THÉRY. *Formal correctness of comparison algorithms between binary64 and decimal64 floating-point numbers*, in "Numerical Software Verification", Heidelberg, Germany, Lecture Notes in Computer Science (LNCS), Springer, July 2017, n^{o} 10381, https://hal.archives-ouvertes.fr/hal-01512294

[15] C. COHEN, D. ROUHLING. *A Formal Proof in Coq of LaSalle's Invariance Principle*, in "Interactive Theorem Proving", Brasilia, Brazil, September 2017 [*DOI :* 10.1007/978-3-319-66107-0_10], https://hal.inria.fr/hal-01612293

National Conferences with Proceedings

[16] 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

[17] J. GRIMM. *Implementation of Bourbaki's Elements of Mathematics in Coq: Part Two; Ordered Sets, Cardinals, Integers*, Inria Sophia Antipolis ; Inria, 2017, n^{o} RR-7150, pp. 1-764, https://hal.inria.fr/inria-00440786

Other Publications

[18] B. DJALAL. *A Constructive Formalisation of Semi-Algebraic Sets and Functions*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01643919

[19] F. GUIDI, C. SACERDOTI COEN, E. TASSI. *Implementing Type Theory in Higher Order Constraint Logic Programming*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01410567

[20] D. ROUHLING. *A Formal Proof in Coq of a Control Function for the Inverted Pendulum*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01639819

[21] E. TASSI. *Elpi: an extension language for Coq Metaprogramming Coq in the Elpi λProlog dialect*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01637063

[22] L. THÉRY. *A Formalisation of the Generalised Towers of Hanoi*, January 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01446070

References in notes

[23] R. CHEN, J.-J. LÉVY. *A Semi-automatic Proof of Strong connectivity*, in "9th Working Conference on Verified Software: Theories, Tools and Experiments (VSTTE)", Heidelberg, Germany, July 2017, https://hal.inria.fr/hal-01632947

[24] 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