Activity Report 2013

Project-Team MARELLE

Mathematical, Reasoning and Software

RESEARCH CENTER
Sophia Antipolis - Méditerranée

THEME
Proofs and Verification

Table of contents

Project-Team MARELLE

Keywords: Interactive Theorem Proving, Formal Methods, Security, Cryptography

Creation of the Project-Team: 2006 November 01.

1. Members

Research Scientists

Yves Bertot [Team leader, Inria, Senior Researcher, HdR]
José Grimm [Inria, Researcher]
Benjamin Grégoire [Inria, Researcher]
Laurence Rideau [Inria, Researcher]
Laurent Théry [Inria, Researcher]

External Collaborator

Loic Pottier [Min. de l'Education Nationale, Researcher, until Aug 2013, HdR]

PhD Students

Guillaume Cano [Inria, granted by the Microsoft Research-Inria joint center]
Maxime Dénès [Inria, granted by FP7 FORMATH project, until Sep 2013]

Post-Doctoral Fellows

Érik Martin-Dorel [Inria, granted by ANR project TAMADI, until Sep 2013]
Julianna Zsidó [Inria, granted by FP7 FORMATH project, until Aug 2013]

Visiting Scientists

Amy Felty [Professor at University of Ottawa, Canada, from Aug 2013]
Douglas Howe [Professor at Carleton University, Canada, from Aug 2013]

Administrative Assistant

Nathalie Bellesso [Inria]

Others

Konstantinos Lentzos [Inria, granted by FP7 FORMATH project, from Apr 2013 to Jul 2013]
Florent Bréhard [ENS Paris, Student, from Jun 2013 to Aug 2013]
Antoine Grospellier [ENS Lyon, Student, from Jun 2013 to Jul 2013]

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 automatics 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 is still being improved and part of our work concerns 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. For these algorithms, we generally base our work on the semantic description of a 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 participate in the verification that compilers for conventional programming languages are exempt from bugs.

4. Application Domains

4.1. Reliability of embedded software

Software embedded in physical devices performs computations where the inputs are provided by measures and the outputs are transformed into actions performed by actuators. to improve the quality of these devices, we expect that all the computations performed in this kind of software will need to be made more and more reliable. We claim that formal methods can serve this purpose and we develop the libraries and techniques to support this claim. This implies that we take a serious look at how mathematics can be included in formal methods, especially concerning geometry and calculus.

4.2. Security and Cryptography

The modern economy relies on the possibility for every actor to trust the communications they perform with their colleagues, customers, or providers. We claim that this trust can only be built by a careful scrutiny of the claims made by all public protocols and software that are reproduced in all portable devices, computers, and internet infrastructure systems. We advocate the use of formal methods in these domains and we provide easy-to-use tools for cryptographers so that the formal verification of cryptographic algorithms can become routine and amenable to public scrutiny.

4.3. Mathematics and Education

As librairies for theorem provers evolve, they tend to cover an ever increasing proportion of the mathematical background expected from engineers and scientists of all domains. Because the content of a formally verified library is extremely precise and explicit, we claim that this will provide a new kind of material for teaching mathematics, especially useful in remote education.

5. Software and Platforms

5.1. Tralics

Participant: José Grimm [correspondant].

Tralics is a Latex-to-XML translator available at http://www-sop.inria.fr/marelle/tralics. Version 2.15 has been released in 2012.

5.2. Semantics

Participant: Yves Bertot [correspondant].

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.
See also the web page http://coq.inria.fr/pylons/pylons/contribs/view/Semantics/v8.4.

- ACM: F3.2 F4.1
- AMS: 68N30
- Programming language: Coq

5.3. Easycrypt

Participants: Gilles Barthe [IMDEA Software Institute], François Dupressoir [IMDEA Software Institute], Benjamin Grégoire [correspondant], César Kunz [IMDEA Software Institute], Benedikt Schmid [IMDEA Software Institute], Pierre-Yves Strub [IMDEA Software Institute].

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.

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). ZooCrypt includes an experimental mechanism to generate EasyCrypt proofs of security of analyzed schemes.

5.4. CoqEAL

Participants: Maxime Dénès, Yves Bertot [correspondant].

CoqEAL is a library of certified algorithms for linear algebra to be used in Coq. It provides a collection of algorithms to compute efficiently on matrices and polynomials. These algorithms are designed to run efficiently directly in the Coq system and take the best advantage of the internal execution capabilities of the this system (virtual machine execution of native code execution after compilation).

5.5. CoqApprox

Participants: Nicolas Brisebarre [CNRS], Mioara Joldes, Érik Martin-Dorel, Micaela Mayero [Iut de Villetaneuse], Jean-Michel Muller, Ioana Paşca [Iut de Nimes], Laurence Rideau, Laurent Théry.

We develop a formalization of rigorous polynomial approximation using Taylor models inside the Coq proof assistant, with a special focus on genericity and efficiency for the computations.

5.6. CoqHensel

Participants: Érik Martin-Dorel, Laurent Théry, Micaela Mayero [Iut de Villetaneuse], Guillaume Hanrot [ENS Lyon].

The CoqHensel library provides a Coq formalization of Hensel's lemma for both univariate and bivariate cases, with some effective and modular certificate checkers for the univariate small integral roots problem, the bivariate small integral roots problem, as well as the integer small value problem (ISValP), with the ultimate goal to provide a fully formally verified chain for solving the Table Maker's Dilemma.

6. New Results

6.1. Bourbaki, Sets and Ordinals

Participant: José Grimm [correspondant].

In previous years, we developped a formal library describing the part of the Bourbaki books on set theory, cardinals and ordinals, [18]. Here are ome additions to the library.

Since addition of ordinals is non-commutative, the sum of n ordinals x_1 to x_n depends on their ordering; the maximum number $f(n)$ is a priori bounded by $n!$, and we have shown that it satisfies a recurrence relation (R), Bourbaki asks, in an exercise, to show that $f(n) = 81f(n-5)$ for $n \geq 20$. This is an easy consequence of an explicit formula (F) for f. That (R) implies (F) can be expressed in pure Coq (with binary integers), but we have no idea how to prove it.

We proved some facts of the theory of models: the set V_ω of hereditarily finite sets satisfies ZF (but not the axiom of infinity); the von Neumann universe satisfies ZF and AF, there is a subset of the universe satisfiying ZF containing no inaccessible cardinal. We have also studied the set of formulas and show the theorem of Lövenheim-Skolem.

The main contribution this year is the study of some families of ordinals. If the family is internally closed and too big to be a set, then it is the image of a normal (continuous and strictly increasing) function, called the enumeration function of the family. The family of fix-points of a normal function satisfies this property, and the enumeration of this family is called the first derived function. There is a derivation at every order. For instance, the first derivation of $x \mapsto 1 + x$ is $x \mapsto \omega x$, and the derivation of order n is $x \mapsto \phi(n, x)$. The least x such that $x = \omega^x$ is known as ϵ_0; the least x such that $x = \phi(x, 0)$ is known as Γ_0.

We have shown that the inductive type T defined by zero and a constructor of type $T \to N \to T \to T$, without the terms that are not in "normal form" , is isomorphic to the set of ordinals less than ϵ_0; in the case of $T \to T \to N \to T \to T$, we get all ordinals less than Γ_0; we have also studied the case with one more T (the first two types were first implemented by Castéran, the last was suggested by Ackermann) [19]

6.2. Homotopy Type Theory

Participants: Yves Bertot [correspondant], Florent Bréhard.

Homotopy Type Theory is a domain born out of the conjuction of type theory, which serves as foundations for proof systems like Coq or Agda, and homotopy theory, and domain of mathematics which is concerned with equivalence classes of objects modulo continuous deformation. In particular, Homotopy Type Theory concentrates on paths (continuous substrate between various objects) and paths between paths: paths between points can be understood as lines, paths between lines can be understood as surfaces.

In particular, paths can be thought has having the same properties as the notion of equality that is usually defined inductively in type theory systems and homotopy type theory goes against the trend started in the 1990s where specialists thought an axiom should be added to express that all paths between paths should be equal. On the contrary, if all paths between paths are not equal, type theory can be used to model homotopy theory and that domain of mathematics because a new area of applications for type theory-based theorem provers.

V. Voevodsky organized a special year at Institute for Advanced Study in Princeton on this topic, and Yves Bertot participated to this special year, during which many experiments were performed, extensions to proof systems were designed, and a book was produced. In particular, Yves Bertot devised an extension of the Coq system with *private types* which makes it possible to simulate a new concept known as *higher inductive types*. On top of this extension, the members of the special year produced a collection of higher inductive types, describing circles, spheres, truncations.

During his internship in the Marelle project, Florent Bréhard studied the equivalence between several presentations of higher-dimension spheres using higher inductive types.

Work on higher inductive types was pursued more precisely by Bruno Barras from Saclay. We expect that the result of this work will supersede the experiments made possible by Yves Bertot's implementation of private types, but the concept of private type may retain applications in other domains.

6.3. Isolation of polynomial roots

Participants: Yves Bertot [correspondant], Julianna Zsidó.

Together with techniques to produce square-free polynomials (polynomials whose roots are all simple), Bernstein polynomials provide a way to decide whether a polynomial has roots in a given interval. Together with a dichotomy procedure, this makes it possible to isolate all the roots of a polynomial, or to show that no root of a given polynomial occur in a given interval. At the end of 2012, Julianna Zsidó started to study this procedure: she showed the properties of the procedure to obtain square-free polynomials and she then formalized a proof for a theorem known as the *theorem of three circles* which plays a rôle in proving that dichotomy will terminate. This work has been published as an article in the *Journal of Automated Reasoning*.

We expect to wrap up all this work by producing easy-to-use tactics to prove properties of polynomial formulas and generalizing it to polynomials in several variables.

During a summer internship, Konstantinos Lentzos worked on the representation of algebraic numbers (which can always be represented as roots of polynomials in a given interval) and the question of finding polynomials for algebraic numbers obtained through simple operations (like addition, multiplication, opposite, and inversion). However, this work was made extremely difficult by the problem of finding morphisms between various fields definable on top of a polynomial ring.

6.4. Properties of the π number

Participants: Yves Bertot [correspondant], Laurence Rideau, Laurent Théry.

As a testbed for the progress of formalized libraries in the domain of calculus, we studied an algorithm to compute π (the circle ratio) using arithmetic-geometric means. This study brought us to extend the libraries with improper integrals, studies of *arcsinh*, variable change in integrals, and error propagation proofs.

We also studied a formal proof of the spigot algorithm designed by Bailey, Borwein, and Plouffe, which is used to compute far digits in the hexadecimal representation of π as a fractional number. This relies on floating point computations and error control, for which we provided a formal proof.

6.5. Formal study of cryptography

Participants: Gilles Barthe [IMDEA Software Institute], François Dupressoir [IMDEA Software Institute], Benjamin Grégoire [correspondant], César Kunz [IMDEA Software Institute], Yassine Lakhnech [Univ. Grenoble 1], Benedikt Schmid [IMDEA Software Institute], Pierre-Yves Strub [IMDEA Software Institute], Santiago Zanella Béguelin [MSR].

The goal of this work is to provide a friendly tool easily usable by cryptographers without knowledge of formal proof assistants. The idea is to use the techniques formally proved in Certycrypt and to call SMT-provers. We provide two differents tools:

- Easycrypt (see http://www.easycrypt.info/) 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. This year, Easycrypt has been fully reimplemented, allowing more modularity in proofs and an interactive prover has been integrated.
- ZooCrypt (see http://www.easycrypt.info/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). ZooCrypt includes an experimental mechanism to generate EasyCrypt proofs of security of analyzed schemes.

This year we published papers concerning formal proofs for properties of elliptic curves, differential privacy, padding-based encryption, and probabilistic relational verification.

6.6. Approximation of Mathematical functions

Participants: Guillaume Hanrot, Érik Martin-Dorel, Micaela Mayero [Université de Paris 13], Ioana Paşca [Université de Nimes], Laurence Rideau, Laurent Théry [correspondant].

In a collaboration supported by ANR project Tamadi, we study the approximation of mathematical functions (exponential and trigonometric functions) using polynomial functions.

This year, we completed the formal verification of our library that computes Taylor Models for the usual mathematical functions of one variable within Coq. A presentation of this work has been done at SYNASC'2013.

The SLZ algorithm checks that there is no hard-to-round floating numbers for a given range in a given floating-point format. It usually consists of a very long computation returning a yes/no answer. Formally proving the implementation of the algorithm is current outside reach since it requires very sophisticated numerical libraries that are currently impossible to verify formally. We have defined a notion of certificate for these computations based on Hensel's lemma and derived an executable checker within Coq that is capable to verify such computations. A publication has been submitted.

6.7. Formal verification in Geometry

Participants: Laurent Fuchs, Laurent Théry [correspondant].

Grassmann-Cayley Algebras are a convenient algebraic way of talking about geometrical concepts. We have further improved our certified Grassmann-Cayley Algebra library to accommodate unbalanced binary trees. A publication has been accepted and will be published in 2014.

6.8. SMT automation for Ssreflect

Participants: Antoine Grospellier, Laurent Théry [correspondant].

The proof of the Feit-Thompson theorem (also known as the odd-order theorem) has been carried on with little use of automation. We have customised the existing connection between Coq and SMT solvers using Why to accomodate Ssreflect specificities. The preliminary results are encouraging.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- We participated in the ANR project TAMADI, which started in October 2010. Other participants are ARENAIRE-Inria Rhone-Alpes and the PEQUAN team from University of Paris VI Pierre and Marie Curie. The objective of the TAMADI project is to study the question of precision in floating-point arithmetic and to provide formal proofs on this topic. This project was completed in October 2013.

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. FORMATH

Type: COOPERATION

Defi: Future and Emerging Technologies

Instrument: Specific Targeted Research Project

Objectif: FET-Open: Challenging Current Thinking

Duration: March 2010 - August 2013

Coordinator: University of Göteborg (Sweden)

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

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

Inria contact: Y. Bertot

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.

7.3. International Initiatives

7.3.1. Informal International Partners

We interact regularly with the team of Prof. Thierry Coquand at University of Göteborg and Chalmers University in Sweden and the team of Prof. Julio Rubio at Universidad de La Rioja in spain.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Amy Felty, professor at the University of Ottawa, Doug Howe, professor at Carleton University in Canada, are visiting from September 2013 to Summer 2014.

7.4.1.1. Internships

- Florent Bréhard, student at École Normale Supérieure, worked from June to August 2013 on *homotopy type theory*. In particular, he produced a proof of equivalence between various presentations of spheres, at all dimensions.
- Antoine Grospellier, student at École Normale Supérieure, worked from June to August 2013 on integrating automatic proof tools for first order logic in the Coq system.

7.4.2. Visits to International Teams

- Yves Bertot spent three months From January 15th to April 15th, 2013 at Institute for Advanced Study, Princeton, where he was invited to participate to the special year on *Homotopy Type Theory*.

8. Dissemination

8.1. Scientific Animation

Members of the project refereed papers for the journals MSCS (Mathematical Structures of Computer Science), JFR (Journal of Formalized Reasoning), they participated to the program committee of ITP (Interactive Theorem Provers),ACL2 (A Computational Logic for Applicative Common Lisp), PxTP (Proof Exchange for Theorem Provers), and refereed papers for the conferences ITP and ESOP (European Symposium on Programming),ISSAC (International Symposium on Symbolic and Algebraic Computation).

Benjamin Grégoire gave lectures at the first EasyCrypt summer school in Philadelphia in July.

Members of the project participated to the conferences “Journées Francophones des Langages Applicatifs” (Aussois, France, January) “workshop on Foundation of Mathematics for Computer-Aided Formalization” (Padova, Italy, January), “Journées Nationales de l’Informatique Mathématique” (Lyon, January),“Conferences on Inteligent Computer Mathematics” (London, July), “Conference on Interactive Theorem Proving” (Rennes, France), “Conference on Symbolic and Numerical Algorithms for Scientific Computing” (Timisoara, Romania, September).

Yves Bertot was invited to give a joint seminar on homotopy type theory at Harvard in Boston, USA, and MIT on March 25th, 2013, Benjamin Grégoire made 8 visits to IMDEA in Madrid, Spain, to work on formally verified proofs in cryptography and automatic tools for formal verification for cryptographers, L. Rideau, L. Théry, E. Martin-Dorel were invited to meetings in Lyon, in July and October, Y. Bertot, L. Rideau participated to the Spring Day of Microsoft Research-Inria joint centre.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Laurence Rideau, “Introduction to programming” classe préparatoire MP*, teaching assistant, 48 hours, Lycée Masséna, Nice, France

Master : Laurent Théry: “Formalization of floating point arithmetic”, 8 hours, ENS Lyon, France

Master : Laurent Théry: “Introduction to Coq”, 3 hours, École des Mines de Paris, Sophia Antipolis, France

Master : Laurent Théry: Examiner for the exam “agrégation de mathématiques, option informatique”

Master : Julianna Zsidó: “Logic”, 48 hours, École Polytechnique Universitaire, Sophia Antipolis, France

8.2.2. Supervision

PhD : Maxime Dénès, “Étude formelle d’algorithmes efficaces en algèbre linéaire”, Université de Nice, defended on November, 20th, 2013, supervised by Yves Bertot.

PhD in progress: Maxime Cano, “Interaction entre algèbre linéaire et analyse en formalisation des mathématiques”, thèse commencée en octobre 2010, supervised par Yves Bertot.

8.2.3. Juries

- Yves Bertot was an examiner for the thesis defense of Shi Xiaomu (University of Grenoble, France and Tsinghua University, Beijing, China), María Poza (Universidad de la Rioja, Spain–with written report duty), Pierre Néron (Ecole Polytechnique, France–as chairman for the Jury), Victor Magron (Ecole Polytechnique, France–with written report duty).
- Benjamin Grégoire was an examiner for the thesis of Chantal Keller (Ecole Polytechnique, France).

8.2.4. Community Service

- José Grimm is a member of the *comité de centre*, the committee where representatives of personnel and management discuss questions of daily life at the level of the Sophia-Antipolis Méditerranée center, he also participates in a commision on continued training and a commission on hygiene, safety, and working conditions. This activity involves around 12 meetings per year.
- Benjamin Grégoire was a member of the *comité de développement technologique* (in English, technological development committee), the committe that overseas the allocation of software engineers on experimental software and platform development, until June 2013. Laurent Théry is a member of the same committee since June 2013.
- Benjamin Grégoire and Yves Bertot are members of the Coq steering committee. Yves Bertot has been appointed chairman of this committee since October 2013. As such, Yves Bertot attended a Coq users meeting at ICFP in 2013.
- Yves Bertot is deputy scientific director for the Sophia Antipolis méditerranée research center. This task implies meetings approximately every fortnight with the center director, the scientific director, and the director of admnistrative services for the center, together with frequent meetings with researchers from any domain in the center and monthly meetings at the national level as part of the evaluation committee.

8.3. Popularization

Yves Bertot participated to two articles published in popular science magazines (*Science et Vie* and *Science et Avenir*) and Laurence Rideau to one of these articles.

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, P. Castéran. , *Interactive Theorem Proving and Program Development, Coq'Art:the Calculus of Inductive Constructions*, Springer-Verlag, 2004

[3] 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/

[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

Doctoral Dissertations and Habilitation Theses

[5] M. Dénès. , *Étude formelle d'algorithmes efficaces en algèbre linéaire*, Université Nice Sophia Antipolis, November 2013, http://hal.inria.fr/tel-00945775

Articles in International Peer-Reviewed Journals

[6] G. Barthe, B. Grégoire, S. Heraud, F. Olmedo, S. Zanella Beguelin. *Verified indifferentiable hashing into elliptic curves*, in "Journal of Computer Security", November 2013, http://hal.inria.fr/hal-00935747

[7] É. Martin-Dorel, G. Melquiond, J.-M. Muller. *Some issues related to double roundings*, in "BIT Numerical Mathematics", December 2013, vol. 53, n^{o} 4, pp. 897-924 [*DOI :* 10.1007/s10543-013-0436-2], http://hal.inria.fr/ensl-00644408

[8] J. Zsidó. *Theorem of three circles in Coq*, in "Journal of Automated Reasoning", December 2013, 25 p. [*DOI :* 10.1007/s10817-013-9299-0], http://hal.inria.fr/hal-00864827

International Conferences with Proceedings

[9] G. Barthe, J. M. Crespo, B. Gregoire, C. Kunz, Y. Lakhnech, B. Schmidt, S. Zanella Beguelin. *Fully automated analysis of padding-based encryption in the computational model*, in "2013 ACM SIGSAC Conference on Computer and Communications Security", Berlin, Germany, ACM, November 2013, pp. 1247-1260 [*DOI :* 10.1145/2508859.2516663], http://hal.inria.fr/hal-00935737

[10] G. Barthe, G. Danezis, B. Grégoire, C. Kunz, S. Zanella Beguelin. *Verified Computational Differential Privacy with Applications to Smart Metering*, in "2013 IEEE 26th Computer Security

Foundations Symposium", New Orleans, United States, IEEE Computer Society, June 2013, pp. 287-301 [*DOI :* 10.1109/CSF.2013.26], http://hal.inria.fr/hal-00935736

[11] G. BARTHE, C. FOURNET, B. GREGOIRE, P.-Y. STRUB, N. SWAMY, S. ZANELLA BEGUELIN. *Probabilistic relational verification for cryptographic implementations*, in "The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages", San Diego, United States, January 2014, http://hal.inria.fr/hal-00935743

[12] G. CANO, M. DÉNÈS. *Matrices à blocs et en forme canonique*, in "JFLA - Journées francophones des langages applicatifs", Aussois, France, D. POUS, C. TASSON (editors), Damien Pous and Christine Tasson, February 2013, http://hal.inria.fr/hal-00779376

[13] 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

[14] É. MARTIN-DOREL, M. MAYERO, I. PASCA, L. RIDEAU, L. THÉRY. *Certified, Efficient and Sharp Univariate Taylor Models in COQ*, in "SYNASC 2013 - 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing", Timisoara, Romania, 2013, http://hal.inria.fr/hal-00845791

[15] Q. WANG, B. BARRAS. *Semantics of Intensional Type Theory extended with Decidable Equational Theories*, in "Computer Science Logic 2013", Dagstuhl, Germany, S. R. D. ROCCA (editor), Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, August 2013, vol. 23, pp. 653–667 [*DOI :* 10.4230/LIPICS.CSL.2013.653], http://hal.inria.fr/hal-00937197

Scientific Books (or Scientific Book chapters)

[16] P. ACZEL, B. AHRENS, T. ALTENKIRCH, S. AWODEY, B. BARRAS, A. BAUER, Y. BERTOT, M. BEZEM, T. COQUAND, E. FINSTER, D. GRAYSON, H. HERBELIN, A. JOYAL, D. LICATA, P. LUMSDAINE, A. MAHBOUBI, P. MARTIN-LÖF, S. MELIKHOV, A. PELAYO, A. POLONSKY, M. SHULMAN, M. SOZEAU, B. SPITTERS, B. VAN DEN BERG, V. VOEVODSKY, M. WARREN, C. ANGIULI, A. BORDG, G. BRUNERIE, C. KAPULKIN, E. RIJKE, K. SOJAKOVA, J. AVIGAD, C. COHEN, R. CONSTABLE, P.-L. CURIEN, P. DYBJER, M. ESCARDÓ, K.-B. HOU, N. GAMBINO, R. GARNER, G. GONTHIER, T. HALES, R. HARPER, M. HOFMANN, P. HOFSTRA, J. KOCH, N. KRAUS, N. LI, Z. LUO, M. NAHAS, E. PALMGREN, E. RIEHL, D. SCOTT, P. SCOTT, S. SOLOVIEV. , *Homotopy Type Theory: Univalent Foundations of Mathematics*, Aucun, 2013, 448 p. , http://hal.inria.fr/hal-00935057

Research Reports

[17] J. GRIMM. , *Implementation of Bourbaki's Elements of Mathematics in Coq: Part One, Theory of Sets*, Inria, 2013, n^{o} RR-6999, 205 p. , http://hal.inria.fr/inria-00408143

[18] J. GRIMM. , *Implementation of Bourbaki's Elements of Mathematics in Coq: Part Two; Ordered Sets, Cardinals, Integers*, Inria, 2013, n^{o} RR-7150, 604 p. , http://hal.inria.fr/inria-00440786

[19] J. GRIMM. , *Implementation of three types of ordinals in Coq*, Inria, 2013, n^{o} RR-8407, 74 p. , http://hal.inria.fr/hal-00911710

Other Publications

[20] É. Martin-Dorel, G. Hanrot, M. Mayero, L. Théry. , *Formally verified certificate checkers for hardest-to-round computation*, December 2013, http://hal.inria.fr/hal-00919498