Activity Report 2012

Project-Team MARELLE

Mathematical Reasoning and Software

RESEARCH CENTER
Sophia Antipolis - Méditerranée

THEME
Programs, Verification and Proofs

Table of contents

1. Members **1**
2. Overall Objectives **1**
2.1. Introduction 1
2.2. Highlights of the Year 2
3. Scientific Foundations **2**
3.1. Type theory and formalization of mathematics 2
3.2. Verification of scientific algorithms 2
3.3. Programming language semantics 2
4. Software **2**
4.1. Tralics 2
4.2. Semantics 3
4.3. Certicrypt and Easycrypt 3
5. New Results **3**
5.1. Coq and SMT provers 3
5.2. Formal proofs on Pi 3
5.3. Formal proofs on linear algebra 4
5.4. Formal proof of the Feit-Thompson theorem 4
5.5. Native execution for the Coq system 4
5.6. Provably correct approximations of elementary functions 4
5.7. Geometric algebras 5
5.8. Bourbaki in Coq 5
5.9. Reasoning on polynomial expressions 5
5.10. Higher-Order Abstract Syntax 5
5.11. Proofs in cryptography 5
6. Partnerships and Cooperations **6**
6.1. National Initiatives 6
6.2. European Initiatives 6
6.3. International Initiatives 7
6.4. International Research Visitors 7
7. Dissemination **7**
7.1. Scientific Animation 7
7.2. Teaching - Supervision - Juries 7
7.2.1. Teaching 7
7.2.2. Supervision 8
7.2.3. Juries 8
7.3. Popularization 8
8. Bibliography **8**

Project-Team MARELLE

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

Creation of the Project-Team: November 01, 2006 .

1. Members

Research Scientists

Yves Bertot [Team leader, Inria, HdR]
Benjamin Grégoire [Research scientist Inria]
José Grimm [Research scientist Inria]
Laurence Rideau [Research scientist Inria]
Loïc Pottier [Research scientist Inria, until August 2012, HdR]
Laurent Théry [Research scientist Inria]

PhD Students

Guillaume Cano [supervised by Y. Bertot]
Maxime Dénès [supervised by Y. Bertot]
Nicolas Julien [supervised by Y. Bertot]
Michaël Armand [supervised by L. Théry and B. Grégoire]

Post-Doctoral Fellows

Erik Martin-Dorel [starting in October]
Julianna Zsido [starting in September]

Administrative Assistant

Nathalie Bellesso [Administrative assistant]

2. Overall Objectives

2.1. Introduction

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.

Mathematical knowledge can also be made concrete in the form of decision procedures, often “satisfiability modulo theory” procedures, which can be connected to theorem proving tools in a way that preserves the trustability of the final results.

2.2. Highlights of the Year

This year, the Mathematical Components project of the Microsoft Research-Inria joint center under the direction of Georges Gonthier completed the major objective it had set six years ago: the complete formal verification of the Odd Order theorem, also known as the Feit Thompson theorem, which states that every odd order finite group is solvable. The Marelle project-team is a key participant in this project.

For more information : http://www.msr-inria.inria.fr/Projects/math-components/feit-thompson

3. Scientific Foundations

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. Second, 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). Thus, 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. Software

4.1. 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 this year. Some features have been added, and some bugs corrected.

4.2. 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/v8.3.

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

4.3. Certicrypt and Easycrypt

Participants: Gilles Barthe [IMDEA Software Institute], Juan Manuel Crespo [IMDEA Software Institute], Benjamin Grégoire [correspondant], Sylvain Heraud, César Kunz [IMDEA Software Institute], Federico Olmedo [IMDEA Software Institute], Santiago Zanella Béguelin [IMDEA Software Institute].

CertiCrypt takes a language-based approach to cryptography: the security of a cryptographic scheme and the cryptographic assumptions upon which its security relies are expressed by means of probabilistic programs, called games; in a similar way, adversarial models are specified in terms of complexity classes, e.g. probabilistic polynomial-time programs. This code-centric view leads to statements that are amenable to formalization and tool-assisted verification. CertiCrypt instruments a rich set of verification techniques for probabilistic programs, including equational theories of observational equivalence, relational Hoare logic, data-flow analysis-based program transformations, and game-based techniques such as eager/lazy sampling and failure events.

See also the web page http://easycrypt.gforge.inria.fr/.

5. New Results

5.1. Coq and SMT provers

Participants: Michaël Armand, Benjamin Grégoire, Laurent Théry.

Continuing the work of previous years, we added an extra theory to the interface between Coq and Satisfiability Modulo Theory (SMT) provers: instantiation. It is the last really needed piece to make our tactic based on SMT provers really useful to Coq users. Part of the work was to make the proof work on statements existing in the Propositional type instead of the boolean type. This requires a change in the correctness proof.

5.2. Formal proofs on Pi

Participant: Yves Bertot.

We studied the chain of definitions and proofs necessary to show that

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \cdots$$

and removed the axiom that was left on this topic in Coq's standard library. This part re-used a past contribution of Guillaume Allais during an internship from Ecole Normale Supérieure de Lyon. We then added a study of Machin's formula to compute decimals of π.

5.3. Formal proofs on linear algebra

Participants: Guillaume Cano, Maxime Dénès, Anders Mörtberg [University of Chalmers, Sweden], Vincent Siles [University of Chalmers, Sweden], Yves Bertot.

This year we completed a work on matrix canonical forms, providing formal proofs for the following results:

- Smith normal forms of matrices on principal ideal domains are unique,
- Every matrix on a field is similar to its Frobenius normal form
- Every matrix on an algebraically closed field is similar to its Jordan normal form

We also studied techniques to combine high-level mathematical descriptions and proofs of algorithms with executable implementations. This work led to a publication at ITP'12 [10]. We are still working on extending this work to rational numbers and real algebraic numbers.

We then worked on tools to automate proofs. In the ring tactic, all elements considered must belong to the same type. We worked on extending this tactic to dependent families of types, like the type of matrices where each dimension gives rise to a different type in the family and multiplications typically concern matrices of different types, while remaining associative.

5.4. Formal proof of the Feit-Thompson theorem

Participants: Laurence Rideau, Laurent Théry.

The Feit-Thompson theorem, established in the beginning of the 1960s, states that every odd-order finite group is solvable. The proof of this result was initially published in an article with around 250 pages. This proof was cleaned by a team of mathematicians and re-published in the form of two books, totaling approximately the same number of pages. But these books also rested on some general knowledge about groups and various areas of algebras.

All this knowledge is now formally described in the Mathematical Components library. The proof of the theorem has been completed in September 2012. The team that achieved this result includes members of the Marelle project-team, along with members of the Typical project-team at Inria Saclay-Ile de France, members of the Microsoft Research Cambridge laboratory, and guests from other institutions.

This year, the members of the Marelle team concentrated on the following topics:

- General character theory: chapters 5 and 6 of the book by Isaacs,
- Character theory for the odd order theorem: chapters 1 to 4 of the book of the book by Peterfalvi.

More information at http://www.msr-inria.inria.fr/Projects/math-components/feit-thompson.

5.5. Native execution for the Coq system

Participants: Maxime Dénès, Benjamin Grégoire, Yves Bertot.

We have continued our work on the native execution of dependently typed terms, aiming at the integration of this work in the main branch of the Coq system.

5.6. Provably correct approximations of elementary functions

Participants: Erik Martin-Dorel, Laurence Rideau, Laurent Théry.

The elementary functions are general purpose mathematical functions that are often implemented in the hardware of modern micro-processors: exponential and trigonometric functions, and inverse functions like arctan or square-root. We participate in a nationally funded project (ANR-TaMaDi) where precise approximations of these functions and their combinations must be computed. A first approach is to use Taylor models. We implemented such an approach and proved its correctness in the Coq system. This led to the publication [9].

We are now working on applying Bernstein polynomials to the problem of approximating transcendental functions.

5.7. Geometric algebras

Participant: Laurent Théry.

We translated our library to the ssreflect setting and provided a very concise certified implementation of geometric algebras based on binary trees.

5.8. Bourbaki in Coq

Participant: José Grimm.

In previous years, we developed a formal library describing the part of the Bourbaki books on set theory, cardinals, and ordinals. The whole development now runs under Coq 8.4, ssreflect 1.4. The main contribution this year is the study of some families of numbers (Stirling numbers of the second kind, Euler numbers, Bell numbers), and their relations to cardinalities (number of partitions of a set, number of partition with p parts, number of surjections $I_n \to I_p$). We have some explicit formulas for $\sum_{i<n} i^k$ as sums of binomial coefficients.

5.9. Reasoning on polynomial expressions

Participants: José Grimm, Julianna Zsido, Yves Bertot.

Continuing previous work by Bertot, we showed that if p is a polynomial on any ordered ring, that has n positive roots, the list of its coefficients has at least n sign changes. If there is exactly one sign change, and the ring is an Archimedian field, there is a number a such that the polynomial is negative on $[0, a]$ and strictly increasing after a; thus it has at most one positive root, and there is a Cauchy sequence x_i such that $p(x_i) < 0$ but $p(x_i + c/2^n) > 0$.

The publication by Bertot, Mahboubi, and Guilhot in 2011 on Bernstein polynomials describes a procedure that works only for polynomials with simple roots. We added the proofs that describe how to obtain such polynomials, starting from arbitrary ones. In other words, we proved the following statement: *for every polynomial p, p divided by the greatest common divisor of p and its derivative has the same roots as p and all the roots are simple.*

We started working on a proof that the dichotomy process based on Bernstein polynomials is bound to terminate, concentrating on a theorem known as *the theorem of three circles*.

5.10. Higher-Order Abstract Syntax

Participant: Julianna Zsido.

With Martin Hyland from the University of Cambridge, we worked on an approach to reconcile the points of view of Fiore, Plotkin, and Turi on the one hand and Hirschowitz and Maggesi on the other hand. This approach relies on a large monad that abstracts over the two approaches.

5.11. Proofs in cryptography

Participants: Gilles Barthe [IMDEA Software Institute], Juan Manuel Crespo [IMDEA Software Institute], Benjamin Grégoire, Sylvain Heraud [Prove&Run], César Kunz [IMDEA Software Institute], Yassine Lakhnech [University of Grenoble], Pierre-Yves Strub [IMDEA Software Institute], Santiago Zanella Béguelin [IMDEA Software Institute].

We are continuing our work on providing a user-friendly tool for cryptographers who want to develop formal proofs of correctness, based on Certicrypt and SMT provers. There were invited talks at ITP, CPP, MPP, SAS, and JFLA. There was also an article in ERCIM news, whose contents is more oriented towards the open public. See also the web page http://easycrypt.gforge.inria.fr/.

As an illustrative example, we proposed a machine-checked proof of a construction of a hash function based on elliptic curves, where the correctness proof uses the Random Oracle Model. The proof is based on an extension of CertiCrypt for reasoning about approximate forms of observational equivalence and uses mathematical results from group theory and elliptic curves.

Thanks to our language-based approach to describing cryptographic constructions and our automatic approach to proving them correct, we can now explore systematically the space of possible designs. Using this approach, we have been able to explore over 1.3 million schemes, including more than 100 variants of OAEP studied in the literature and to prove the correctness of 250,000 schemes for one kind of model and 17,000 for another kind.

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR

- We participated in the ANR project DeCert, which started on January 2009. Other participants are CEA List (Paris), LORIA-Inria (Nancy), Celtique (IRISA Rennes), Proval (LRI Orsay), Typical (Inria Saclay), Systerel (Aix-en-provence). The objective of the DeCert project was to design an architecture for cooperating decision procedures. To ensure trust in the architecture, the decision procedures will either be proved correct inside a proof assistant or produce proof witnesses allowing external checkers to verify the validity of their answers.
- We participate 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.

6.2. European Initiatives

6.2.1. FP7 Projects

6.2.1.1. FORMATH

Title: Formath

Type: COOPERATION (ICT)

Defi: FET Open

Instrument: Specific Targeted Research Project (STREP)

Duration: March 2010 - July 2013

Coordinator: Univ Gӧtegorg (Sweden)

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

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

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

6.3. International Initiatives

6.3.1. Inria International Partners

We are in close contact with the University of Chalmers in Göteborg, Sweden and with the IMDEA Software Institute in Madrid, Spain.

6.4. International Research Visitors

6.4.1. Visits to International Teams

- Benjamin Grégoire visited IMDEA in Madrid, spain in April (23-27), October (1-5), and November (26-30).

7. Dissemination

7.1. Scientific Animation

- We organized the MAP spring school on the formalization of mathematics, March 12-16, 2012, at Inria Sophia Antipolis. This school had 65 attendants and 5 invited speakers: G. Gonthier (Microsoft Research, Prize the EADS foundation), T. Hales (University of Pittsburgh), J. Rubio (Universidad de la Rioja), B. Spitters (Radboud University), and V. Voevodsky (Institute for Advanced Study, Fields Medal). The local organization was supervised by Yves Bertot and included a strong investment by Nathalie Bellesso and Agnès Cortell, from Inria's service for scientific events. Yves Bertot, Laurence Rideau, and Laurent Théry also taught at this school.
- Yves Bertot participated as a lecturer in the asian-pacific summer school on formal methods, July 16-20, at East China Normal University in Shanghai. He gave 6 lectures and supervised laboratory sessions.
- Yves Bertot and Patrick Rambert released a multi-media course on the Coq system, consisting in more than 8 hours of recorded courses available at http://fuscia.inrialpes.fr/cours/coq/.
- members of the project participated in the program committees of PXTP (Proof Exchange for Theorem Proving), PAAR (Practical Aspects of Automated Reasoning), ITP (Interactive Theorem Proving).

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence : Laurence Rideau, introduction to programming in CAML, Classe préparatoire MP* (L2 level), Lycée Masséna, Nice

Master : Benjamin Grégoire, “Verification and Security”, 18 ETD, M2, University of Nice, France

Master : Yves Bertot, “Verification of proofs and programs”, 27 ETD, University of Nice, France

Master : Laurent Théry, “Introduction to Coq”, 3 ETD, Ecole des Mines, Sophia Antipolis, France

Master : Laurent Théry, “Formalization of floating point arithmetic”, Ecole Normale Supérieure de Lyon, France

Doctorate : Yves Bertot, “Introduction to formalized mathematics”, 30ETD, Inria Sophia Antipolis, France

Doctorate : Laurence Rideau, “Introduction to formalized mathematics”, 30ETD, Inria Sophia Antipolis, France

Doctorate : Laurent Théry, “Introduction to formalized mathematics”, 30ETD, Inria Sophia Antipolis, France

Doctorate : Yves Bertot, “Formal verification with Coq”, 50 ETD, East China Normal University, Shanghai, China.

7.2.2. *Supervision*

PhD & HdR :

PhD : Sylvain Heraud, “Verification Semi-automatique de primitives cryptographiques”, University of Nice Sophia Antipolis, March 12, 2012 (thesis started in October 2008), supervisor : Benjamin Grégoire.

PhD in progress : Michaël Armand, “Application de la certification de résultats à l’automatisation de preuves interactives”, started in October 2009, supervisors: Laurent Théry and Benjamin Grégoire.

PhD in progress : Guillaume Cano, “Une formalisation adaptable de l’algèbre linéaire”, started in October 2010, supervised by Yves Bertot.

PhD in progress : Maxime Dénès, “Description formelle d’algèbre linéaire pour l’algorithmique rapide”, started in September 2010, supervised by Yves Bertot.

7.2.3. *Juries*

+ Yves Bertot was a reviewer for the PhD theses of Celia Picard (U. Toulouse) and Erik Martin-Dorel (ENS Lyon) and an examiner for the thesis of Francesco Bongiovanni (U. Nice).
+ Laurent Théry was an examiner for the thesis of Thomas Braibant (U. Grenoble) and for the Licenciate degree of Anders Mörtberg (U. Göteborg, Sweden).

7.3. Popularization

- Laurence Rideau took part in a presentation of research topics for students from “classes préparatoires” at Inria Sophia Antipolis Méditerranée.

8. Bibliography

Major publications by the team in recent years

[1] G. Barthe, B. Grégoire, S. Zanella Béguelin. *Formal Certification of Code-Based Cryptographic Proofs*, in "36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2009", ACM, 2009, p. 90–101, http://dx.doi.org/10.1145/1480881.1480894.

[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, p. 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, p. 86-101, http://hal.inria.fr/inria-00139131.

Publications of the year

Articles in International Peer-Reviewed Journals

[5] B. GRÉGOIRE. *Recent Advances in the Formal Verification of Cryptographic Systems: Turing's Legacy*, in "ERCIM News", 2012, vol. 2012, n° 91, http://hal.inria.fr/hal-00765897.

Invited Conferences

[6] G. BARTHE, B. GRÉGOIRE, S. ZANELLA BÉGUELIN. *Probabilistic relational Hoare logics for computer-aided security proofs*, in "Mathematics of Program Construction - 11th International Conference, MPC 2012", Madrid, Spain, 2012 [*DOI :* 10.1007/978-3-642-31113-0_1], http://hal.inria.fr/hal-00765864.

International Conferences with Proceedings

[7] M. BACKES, G. BARTHE, M. BERG, B. GRÉGOIRE, C. KUNZ, M. SKORUPPA, S. ZANELLA BÉGUELIN. *Verified Security of Merkle-Damgaard*, in "25th IEEE Computer Security Foundations Symposium, CSF 2012", Cambridge, MA, United States, 2012 [*DOI :* 10.1109/CSF.2012.14], http://hal.inria.fr/hal-00765883.

[8] G. BARTHE, B. GRÉGOIRE, S. HERAUD, F. OLMEDO, S. ZANELLA BÉGUELIN. *Verified Indifferentiable Hashing into Elliptic Curves*, in "Principles of Security and Trust - First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012", Tallinn, Estonia, 2012 [*DOI :* 10.1007/978-3-642-28641-4_12], http://hal.inria.fr/hal-00765874.

[9] N. BRISEBARRE, M. JOLDES, É. MARTIN-DOREL, M. MAYERO, J.-M. MULLER, I. PAŞCA, L. RIDEAU, L. THÉRY. *Rigorous Polynomial Approximation using Taylor Models in Coq*, in "Fourth NASA Formal Methods Symposium", Norfolk, Virginia, United States, A. GOODLOE, S. PERSON (editors), Lecture Notes in Computer Science, Springer, April 2012, 15, http://hal.inria.fr/ensl-00653460.

[10] M. DÉNÈS, A. MÖRTBERG, V. SILES. *A refinement-based approach to computational algebra in COQ*, in "ITP - 3rd International Conference on Interactive Theorem Proving - 2012", Princeton, United States, L. BERINGER, A. FELTY (editors), Lecture Notes In Computer Science, Springer, 2012, vol. 7406, p. 83-98 [*DOI :* 10.1007/978-3-642-32347-8_7], http://hal.inria.fr/hal-00734505.

[11] J. HERAS, M. DÉNÈS, G. MATA, A. MÖRTBERG, M. POZA, V. SILES. *Towards a certified computation of homology groups for digital images*, in "CTIC - Computational Topology in Image Context - 2012", Bertinoro, Italy, Lecture Notes In Computer Science, Springer, 2012, vol. 7309, p. 49-57 [*DOI :* 10.1007/978-3-642-30238-1_6], http://hal.inria.fr/hal-00711385.

Research Reports

[12] L. RIDEAU, B. SERPETTE, C. TEDESCHI. *Formalization and Concretization of Ordered Networks*, Inria, December 2012, n° RR-8172, 22, http://hal.inria.fr/hal-00762627.