RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2012

Section Partnerships and Cooperations

Edition: 2013-04-24

ARIC Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR HPAC Project

Participants: Claude-Pierre Jeannerod, Nicolas Louvet, Nathalie Revol, Damien Stehlé, Philippe Théveny, Gilles Villard.

"High-performance Algebraic Computing" (HPAC) is a four year ANR project that started in January 2012. The Web page of the project is http://hpac.gforge.inria.fr/. HPAC is headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it involves AriC as well as the Inria project-team MOAIS (LIG, Grenoble), the Inria project-team PolSys (LIP6 lab., Paris), the ARITH group (LIRMM laboratory, Montpellier), and the HPC Project company.

The overall ambition of HPAC is to provide international reference high-performance libraries for exact linear algebra and algebraic systems on multi-processor architecture and to influence parallel programming approaches for algebraic computing. The central goal is to extend the efficiency of the LinBox and FGb libraries to new trend parallel architectures such as clusters of multi-processor systems and graphics processing units in order to tackle a broader class of problems in lattice cryptography and algebraic cryptanalysis. HPAC conducts researches along three axes:
- A domain specific parallel language (DSL) adapted to high-performance algebraic computations;
- Parallel linear algebra kernels and higher-level mathematical algorithms and library modules;
- Library composition and innovative high performance solutions for cryptology challenges.

8.1.2. ANR TaMaDi Project

Participants: Nicolas Brisebarre, Florent de Dinechin, Guillaume Hanrot, Vincent Lefèvre, Érik Martin-Dorel, Micaela Mayero, Jean-Michel Muller, Ioana Pasca, Damien Stehlé, Serge Torres.

The TaMaDi project (Table Maker's Dilemma, 2010-2013) is funded by the ANR and headed by Jean-Michel Muller. It was submitted in January 2010, accepted in June, and started in October 2010. The other French teams involved in the project are the MARELLE team-project of Inria Sophia Antipolis-Méditerranée, and the PEQUAN team of LIP6 lab., Paris.

The aim of the project is to find "hardest to round" (HR) cases for the most common functions and floating-point formats. In floating-point (FP) arithmetic having fully-specified "atomic" operations is a key-requirement for portable, predictable and provable numerical software. Since 1985, the four arithmetic operations and the square root are IEEE specified (it is required that they should be correctly rounded: the system must always return the floating-point number nearest the exact result of the operation). This is not fully the case for the basic mathematical functions (sine, cosine, exponential, etc.). Indeed, the same function, on the same argument value, with the same format, may return significantly different results depending on the environment. As a consequence, numerical programs using these functions suffer from various problems. The lack of specification is due to a problem called the Table Maker's Dilemma (TMD). To compute $f(x)$ in a given format, where x is a FP number, we must first compute an approximation to $f(x)$ with a given precision, which we round to the nearest FP number in the considered format. The problem is the following: finding what the accuracy of the approximation must be to ensure that the obtained result is always equal to the "exact" $f(x)$ rounded to the nearest FP number. In the last years, our team-project and the CACAO team-project of Inria Nancy-Grand Est designed algorithms for finding hardest-to-round cases. These algorithms do not allow to tackle with large formats. The TaMaDi project mainly focuses on three aspects:

- big precisions: we must get new algorithms for dealing with precisions larger than double precision. Such precisions will become more and more important (even if double precision may be thought as more than enough for a final result, it may not be sufficient for the intermediate results of long or critical calculations);
- formal proof: we must provide formal proofs of the critical parts of our methods. Another possibility is to have our programs generating certificates that show the validity of their results. We should then focus on proving the certificates;
- aggressive computing: the methods we have designed for generating HR points in double precision require weeks of computation on hundreds of PCs. Even if we design faster algorithms, we must massively parallelize our methods, and study various ways of doing that.

The various documents can be found at http://tamadiwiki.ens-lyon.fr/tamadiwiki/index.php/Main_Page.

8.2. International Initiatives

8.2.1. Inria Associate Teams

QOLAPS (Quantifier elimination, Optimization, Linear Algebra and Polynomial Systems) Associate Team between the Symbolic Computation Group at North Carolina State University (USA), the PolSys team at LIP6, Paris 6, and the AriC team. Participants: Nathalie Revol and Gilles Villard.

8.2.2. Participation in International Programs

Joint CNRS-Royal Society grant with Cong Ling (Imperial College, London). Participants: Guillaume Hanrot and Damien Stehlé.

CNRS Associate Team (PICS) with the Cryptography groups of Macquarie University (Christophe Doche and Igor Shparlinski) and Monash University (Ron Steinfeld). Participants: Nicolas Brisebarre, Guillaume Hanrot, Fabien Laguillaumie, Adeline Langlois and Damien Stehlé.

Merlion grant, co-funded by the French Embassy in Singapore and NTU (Nanyang Technological University), with the cryptography group of NTU (San Ling, Khoa Nguyen and Huaxiong Wang). Participants: Adeline Langlois and Damien Stehlé.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Prof. Peter Kornerup (Odense University, Denmark): September 5–19.

Dr. Benoît Libert (Université de Louvain-la Neuve, Belgium), Inria invited researcher: May 28–July 13.

Prof. San Ling (Nanyang Technological University, Singapore), ENS Lyon invited professor: August 20–October 11.

Prof. Dave Saunders (University of Delaware, U.S.A.), ENS Lyon invited professor: April 15–July 25.

CARAMEL Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Function field sieve: implementation and hardware acceleration

Participants: Jérémie Detrey [contact], Pierrick Gaudry, Hamza Jeljeli, Vlad-Cristian Miclea, Emmanuel Thomé.

The team has obtained for the years 2012 and 2013 a financial support from the Région Lorraine and Inria for a project focusing on the hardware implementation and acceleration of the function field sieve (FFS).

The FFS algorithm is currently the best known method to compute discrete logarithms in small-characteristic finite fields, such as may occur in pairing-based cryptosystems. Its study is therefore crucial to accurately assess the key-lengths which such cryptosystems should use. More precisely, this project aims at quantifying how much this algorithm can benefit from recent hardware technologies such as GPUs or CPU-embedded FPGAs, and how this might impact current key length recommendations.

The funding obtained was used to buy an FPGA ML-605 development board, on which Vlad-Cristian Miclea implemented operators for polynomial arithmetic in characteristic two and three during his internship; along with a GeForce GTX 580 graphics card, on which Hamza Jeljeli developed a GPU-based implementation of sparse linear algebra routines for solving discrete-logarithm problems [16].

8.2. National Initiatives

The team participates in the "Calcul formel, arithmétique, protection de l'information" research pole of the GDR-IM (CNRS Research Groupon Mathematical Computer Science). The team is a member of the "Arithmétique", "Calcul formel" and "Codage et Cryptographie" working groups.

8.2.1. ANR CATREL (Cribles: Améliorations Théoriques et Résolution Effective du Logarithme discret

Participants: Răzvan Bărbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact], Marion Videau, Paul Zimmermann.

The CATREL proposal has been accepted in ANR "programme Blanc" in 2012. This project involves CARAMEL as a leading team, in cooperation with two other partners which are Inria project-team GRACE (Inria Saclay, LIX, École polytechnique), and the Arith team of the LIRMM Laboratory (Montpellier). The project targets the algorithms for solving the discrete logarithm problem in finite fields, using the Number Field Sieve and the Function Field Sieve algorithms. Actual work on the CATREL project is scheduled to start in January 2013, but the kick-off meeting has already taken place in Nancy on Dec. 14th, 2012.

8.2.2. ANR CHIC (Courbes Hyperelliptiques, Isogénies, Comptage)

Participants: Pierrick Gaudry, Sorina Ionica, Emmanuel Thomé [contact].

The team has obtained a financial support from the ANR ("programme blanc") for a project, common with colleagues from IRMAR (Rennes) and IML (Marseille). The ANR CHIC grant covers the period 09/2009 to 08/2012, and has thus ended in 2012. The purpose of this ANR project is the study of several aspects of curves in genus 2, with a very strong focus on the computation of explicit isogenies between Jacobians.

In 2012, within the context of ANR CHIC, Ionica and Thomé worked on isogeny graphs in genus 2.

8.2.3. ANR DEMOTIS (Collaborative Analysis, Evaluation and Modelling of Health Information Technology)

Participant: Marion Videau.

The project from "programme ARPEGE" involved three Inria project-teams as a single partner (SMIS, SECRET and CARAMEL) together with colleagues from CECOJI (CNRS) and the company Sopinspace. It has been running from January 2009 and ended in March 2012.

The project experimented new methods for the multidisciplinary design of large information systems that have to take into account legal, social and technical constraints. Its main field of application is personal health information systems.

8.3. European Initiatives

8.3.1. PHC application with EPFL

The team obtained a PHC Germaine de Staël grant in collaboration with the LACAL team from EPFL (Lausanne, Switzerland), in 2011. The grant has been renewed for a second (and final) year 2012. This collaboration focuses on integer factorization and discrete logarithms.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Vlad-Cristian MICLEA (from Jun 2012 until Sep 2012)

Subject: Efficient FPGA implementation of finite-field multiplication algorithms

Institution: The Technical University of Cluj-Napoca (Romania)

CASCADE Project-Team

6. Partnerships and Cooperations

6.1. ANR Projects with Industrials

- **SAPHIR-II** *(Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes)*
  Security and analysis of innovating and recent hashing primitives.
  Participants: Patrick Derbez, Jérémy Jean.

  From April 2009 to March 2013.
  Partners: France Telecom R&D, Gemalto, EADS, SAGEM, DCSSI, Cryptolog, Inria/Secret, UVSQ, XLIM, CryptoExperts.
- **PACE: Pairings and Advances in Cryptology for E-cash.**
  Participants: Olivier Blazy, David Pointcheval, Damien Vergnaud.

  From December 2007 to February 2012.
  Partners: France Telecom R&D, NXP, Gemalto, CNRS/LIX (Inria/TANC), Univ. Caen, Cryptolog.
  This project aims at studying new properties of groups (similar to pairings, or variants), and then to exploit them in order to achieve more practical e-cash systems.
- **BEST: Broadcast Encryption for Secure Telecommunications.**
  Participants: Duong Hieu Phan, David Pointcheval, Elizabeth Quaglia, Mario Strefler.

  From December 2009 to November 2013.
  Partners: Thales, Nagra, CryptoExperts, Univ. Paris 8.
  This project aims at studying broadcast encryption and traitor tracing, with applications to the Pay-TV and geolocalisation services.
- **PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Fabrice Ben Hamouda, Michel Ferreira Abdalla, David Pointcheval.

  From December 2010 to November 2014.
  Partners: UVSQ, Oberthur Technologies, Ingenico, Gemalto, Tranef.
  We aim to undertake research in the field of leakage-resilient cryptography with a practical point of view. Our goal is to design efficient leakage-resilient cryptographic algorithms and invent new countermeasures for non-leakage-resilient cryptographic standards. These outcomes shall realize a provable level of security against side-channel attacks and come with a formally verified implementation. For this every practical aspect of the secure implementation of cryptographic schemes must be taken into account, ranging from the high-level security protocols to the cryptographic algorithms and from these algorithms to their implementation on specific devices which hardware design may feature different leakage models.

6.2. ANR Projects within Academics

- **ProSe: Security protocols : formal model, computational model, and implementations.**
  Participant: David Pointcheval.

  From December 2010 to November 2014.
  Partners: ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Inria/Prosecco, Verimag.
  The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.

- **ROMAnTIC: Randomness in Mathematical Cryptography.**
  Participant: Damien Vergnaud.

  From October 2012 to September 2016.
  Partners: ANSSI, Univ. Paris 7, Univ. Paris 8.
  The goal of this project is to get a better understanding of the interplay between randomness and cryptography and to study the security of various cryptographic protocols at different levels (information-theoretic and computational security, number-theoretic assumptions, design and provable security of new and existing constructions).

6.3. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to January 2013.
  There are three virtual labs that focus on the following core research areas: symmetric key algorithms (STVL), public key algorithms and protocols (MAYA), and secure and efficient implementations (VAMPIRE).
  ENS/Inria/CASCADE leads the MAYA virtual lab.
- **ERC Starting Grant: LATTICE.**
  From September 2010 to August 2012
- **SecFuNet: Security for Future Networks.**
  From July 2011 to December 2013

6.4. International Research Visitors

- Angelo De Caro (PhD student) – Univ. Salerno, Italy
- Karina M. Magalhães (PhD student) – University of Campinas, Brazil
- Daniel Masny (PhD student) – University of Bochum, Germany
- Nuttapong Attrapadung – The National Institute of Advanced Industrial Science and Technology, Japan
- Manuel Bernardo Barbosa – University of Minho, Portugal
- Yu Long – Shanghai Jiao Tong University, China
- Igor Shparlinski – Macquarie U., Australia
- Hoeteck Wee – George Washington University, USA
- Christian Schaffner – CWI, Amsterdam

GALAAD Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. GEOLMI

GEOLMI - Geometry and Algebra of Linear Matrix Inequalities with Systems Control Applications - is an ANR project working on topics related to the Geometry of determinantal varieties, positive polynomials, computational algebraic geometry, semidefinite programming and systems control applications.

The partners are LAAS-CNRS, Univ. de Toulouse (coordinator), LJK-CNRS, Univ. Joseph Fourier de Grenoble; Inria Sophia Antipolis Méditerranée; LIP6-CNRS Univ. Pierre et Marie Curie; Univ. de Pau et des Pays de l'Adour; IRMAR-CNRS, Univ. de Rennes.

More information available at http://homepages.laas.fr/henrion/geolmi.

7.1.2. ANEMOS

ANEMOS - Advanced Numeric for ELMs : Modeling and Optimized Schemes - is an ANR project devoted to the numerical modelling study of such ELM control methods as Resonant Magnetic Perturbations (RMPs) and pellet ELM pacing both foreseen in ITER. The goals of the project are to improve understanding of the related physics and propose possible new strategies to improve effectiveness of ELM control techniques. The study of spline spaces for isogemetric finite element methods is proposed in this context.

The partners are IRFM, CEA, Cadarache; JAD, University of Nice - Sophia Antipolis; Inria, Bacchus; Maison de la Simulation CEA-CNRS-Inria-University of Orsay- University of Versailles St Quentin .

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. TERRIFIC

Title: Towards Enhanced Integration of Design and Production in the Factory of the Future through Isogeometric Technologies

Type: COOPERATION (ICT)

Defi: PPP FoF: Digital factories: Manufactoring design and product lifecycle manage

Instrument: Specific Targeted Research Project (STREP)

Duration: September 2011 - August 2014

Coordinator: SINTEF, Oslo (Norway)

Others partners:

Alenia Aeronautica (Italy); Inria Méditerranée (France); Jozef Kepler universitet, Linz (Austria); JOTNE, Oslo (Norway); MAGNA, Steyr (Austria); Missler Software (France); Siemens AG (Germany); Technische Universität Kaiserslautern (Germany); University of Pavia (Italy).

See also: http://terrific-project.eu

Abstract: The project aims at significant improvement of the interoperability of computational tools for the design, analysis and optimization of functional products. An isogeometric approach is applied for selected manufacturing application areas (cars, trains, aircrafts) and for computer-aided machining. Computer Aided Design (CAD) and numerical simulation algorithms are vital technologies in modern product development, yet they are today far from being seamlessly integrated. Their interoperability is severely disturbed by inconsistencies in the mathematical approaches used. Efficient feedback from analysis to CAD and iterative refinement of the analysis model is a feature of isogeometric analysis, and would be an essential improvement for computer-based design optimization and virtual product development. Our vision is to provide and disseminate tangible evidence of the performance of the isogeometric approach in comparison to traditional ones in four important application areas as well as addressing interoperability and other issues that necessarily arise in a large-scale industrial introduction of isogeometry.

7.2.1.2. EXCITING

Title: Exact geometry simulation for optimized design of vehicles and vessels

Type: FP7-CP-SST-2007-RTD-1-218536, COOPERATION (TRANSPORTS)

Instrument: Specific Targeted Research Project (STREP)

Duration: October 2008 - April 2012

Coordinator: Jozef Kepler universitet, Linz (Austria)

Others partners:

SINTEF, Oslo (Norway); Siemens AG (Germany); National Technical University of Athens (Greece); Hellenic Register of Shipping (Greece); University of Technology, Munich (Germany); Inria Méditerranée (France); VA Tech Hydro (Austria); Det Norske Veritas AS (Norway).

See also: http://exciting-project.eu/

Abstract: This project focuses on computational tools for the optimized design of functional free-form surfaces. Specific applications are ship hulls and propellers in naval engineering and car components, frames, and turbochargers in the automotive and railway transportation industries. The objective is to base the corresponding computational tools on the same exact representation of the geometry. This should lead to huge benefits for the entire chain of design, simulation, optimization, and life cycle management, including a new class of computational tools for fluid dynamics and solid mechanics, simulations for vehicles and vessels based. This seamless integration of CAD and FEM will have direct applications in product design, simulation and optimization of core components of vehicles and vessels.

7.2.1.3. SAGA

Title: ShApe, Geometry and Algebra, 2008-2012

Type: FP7-PEOPLE-2007-1-1-ITN.

Instrument: Initial Training Network (ITN)

Duration: November 2008 - October 2012

Coordinator: SINTEF (Norway)

Others partners: University of Oslo (Norway); Johannes Kepler Universitaet Linz (Austria); Universidad de Cantabria, Santander (Spain); Vilniaus Universitetas (Lithuany); National and Kapodistrian University of Athens (Greece); Inria Méditerranée (France); GraphiTech (Italy); Kongsberg SIM GmbH (Austria); Missler Software (France);

See also: http://saga-network.eu/

Abstract: The project aims at promoting the interaction between Geometric Modeling and Real Algebraic Geometry and, in general, at strengthening interdisciplinary and inter-sectorial research and development concerning CAD/CAM. Its objective is also to train a new generation of researchers familiar with both academic and industry viewpoints, while supporting the cooperation among the partners and with other interested collaborators in Europe.

7.2.1.4. DECONSTRUCT

Title:Decomposition of Structured Tensors, Algorithms and Characterization.

Type: PEOPLE (FP7-PEOPLE-2009-IEF)

Instrument: Marie Curie Intra-European Fellowships for Career Development (IEF)

Duration: November 2010 - November 2012

Coordinator: Inria (France)

Others partners: No.

See also: http://www-sop.inria.fr/teams/galaad/joomla/index.php/international-collaborations-147/172-deconstruct.html

Abstract: Tensors play a wide role in numerous application areas as Signal Processing for Telecommunications, Arithmetic Complexity or Data Analysis. In some applications tensors may be completely symmetric, or symmetric only in some modes, or may not be symmetric. In most of these applications, the decomposition of a tensor into a sum of rank-1 terms is relevant, since tensors of interest have a reduced rank. Most of them are structured, i.e., they are either symmetric or enjoy some index-invariance. Lastly, they are often real, which raises open problems concerning the existence and calculation of the decompositions. These issues build the basic bricks of the research program we propose. The classes of tensors described above have a geometric translation in terms of classical algebraic varieties: Segre, Veronese, Segre-Veronese varieties and Grassmannians and their secant varieties. A complete description of equations for those secant varieties and their dimensions is still not known (only dimensions of secant varieties to Veronsean are classified), although they have been studied by algebraic and differential geometers and algebraists for a long period up to now. The aim of this research project is:

- To attack both the description of the ideal of those secant varieties and their dimensions, starting from low dimensions and low degrees.
- To propose algorithms able to compute the rank of structured tensors.

7.2.2. Collaborations in European Programs, except FP7

7.2.2.1. PHC TOURNESOL FL

Program: Tournesol

Project acronym: PHC TOURNESOL FL 2012 - 26409SH

Project title: Extracting multidimensional shapes

Duration: January 2012 - December 2013

Coordinator: E. Hubert (Inria), A. Cuyt (Universiteit Antwerpen)

Other partners: Inria Sophia-Antipolis (France); Universiteit Antwerpen (Belgium)

Abstract: We are working on the shape-from-moments problem : from measurement-like data, reconstructing a desired object. Since many years, this problem has been solved and optimized in the 2D-case thanks to use of complex numbers. Thanks to a new formula, we want to stay in the real domain in order to generalize this problem to multidimensional shapes - in particular 3D-shapes. For more details about our project Tournesol : http://www-sop.inria.fr/teams/galaad/joomla/index.php/international-collaborations-147/173-tournesol.html. For more details about the program Tournesol : http://www.campusfrance.org/fr/tournesol-communaute-francaise.

7.3. International Initiatives

7.3.1. Participation In International Programs

7.3.1.1. CNRS-NSFC collaboration with Hangzhou Dianzi University

Contact in China: Xu Gang, College of computer - Hangzhou Dianzi University.

Participants in France: André Galligo, Bernard Mourrain, R. Duvigneau, B. Nkonga.

Abstract: CAD/CAE technology plays an important role in advanced manufacture, and the seamless integration of CAD/CAE is a difficult and important problem. The current CAD/CAE workflow can be classified into three steps: Computer-aided design, finite element analysis (FEA) and shape optimization. From the above workflow in CAD/CAE, the main gap of the geometric data is from the analysis step. Isogeometric analysis (IGA) can be employed to overcome the gap between CAD and finite element analysis by using the same geometric representation based on NURBS for the design and analysis tasks. In this collaboration, we studied the following problems: (1) Parameterization of computational domain for IGA methods, in particular generation of volume parameterization from CAD surface models. (2) IGA on complicated geometry and topology.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Wen-Shin Lee and Annie Cuyt (University of Antwerp, Belgium) visited on April 23-27 and December 10-22 in the context of the TOURNESOL project .

Nelly Villamizar (University of Oslo, Norway) visited us from March 28 to May 15, to collaborate with B. Mourrain on splines spaces, in the context of the ITN Marie-Curie SAGA.

Ibrahim Adamou (University of Cantabria, Spain) visited us from September 30 to October 8 to collaborate with B. Mourrain on Voronoï diagrams of half-lines and robust geometric computation, for his secondement in the context of the ITN Marie-Curie SAGA.

Gang Xu visited Inria and the university of Nice from November 1 to November 8 in the context of the CNRS-NSFC collaboration program.

Xiao-Shan Gao and Jingsan Chen (Chinese Academy of Science, Beijing) visited from July 18 to July 20.

George Labahn (University of Waterloo, Canada) visited from July 16 to July 22 to explore new collaboration topics with Evelyne Hubert.

GEOMETRICA Project-Team (section vide)

GRACE Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- CATREL (accepted June 2012, Kickoff December 14, 2012, Starting January 1st, 2013): "Cribles: Améliorations Théoriques et Résolution Effective du Logarithme" (Sieve Algorithms: Theoretical Advances and Effective Resolution of the Discrete Logarithm Problem). The aim of this project is to make effective "attacks" on reduced-size discrete logarithm problem (DLP) instances. It is a key ingredient for the assessment of the security of cryptosystems relying on the hardness of the DLP in finite fields, and for deciding on relevant key sizes.

7.1.2. DGA

- DIFMAT: this two-year project aims to find matrices with good diffusion, over small finite fields. These matrices are used in block ciphers and hash functions; coding theory helps to build and analyse them. G. Quintin has been hired as postdoctoral researcher using this funding.
- D. Augot is co-advising Gwezheneg Robert, with Pierre Loidreau (DGA, Rennes University).

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

Program: PHC Hubert Curien PROCOPE

Project acronym: PowerList

Project title: PowerList

Duration: 01/01/2011 to 31/12/2012.

Coordinator: Daniel Augot

Other partners: Ulm Universität, TAIT group, Germany.

Abstract: Building a less powerful but faster probabilistic list decoding algorithm. This funded Alexander Zeh's visits.

7.3. International Initiatives

7.3.1. Inria International Partners

- DTU Lyngby.
- Ulm Universität.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

7.4.1.1. Internships

- Johan Sebastian Nielsen, DTU Lyngby PhD student, visited us from September 1st to December 20th.

7.4.2. Visits to International Teams

- D. Augot, A. Couvreur, and B. Smith visited the University of Illinois at Urbana–Champaign. This visit included two talks given in the Number Theory seminar, and discussions with I. Duursma to prepare the second year of the DGA DIFMAT contract.
- A. Zeh visited the Institute of Information Transmission Problems (IITP), Moscow in December 2012. He gave a talk on low-rate small-minimum distance binary cyclic codes.

LFANT Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Projet Idex CPU

The LFANT team takes part in Work package 6 of the Idex project CPU (Numerical certification and reliability). The work package concerns "Codes, Cryptology and Arithmetic Algorithms" and involves researchers from the Institut de Mathématiques de Bordeaux (Codes and Lattices team, LFANT) and Laboratoire Bordelais de Recherche en Informatique (Combinatorics and Algorithmic team).

8.2. National Initiatives

8.2.1. ANR AlgoL: Algorithmics of L-functions

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge.

http://www.math.u-bordeaux1.fr/~belabas/algol/index.html

The ALGOL project comprises research teams in Bordeaux, Montpellier, Lyon, Toulouse and Besançon.

It studies the so-called L-functions in number theory from an algorithmic and experimental point of view. L-functions encode delicate arithmetic information, and crucial arithmetic conjectures revolve around them: Riemann Hypotheses, Birch and Swinnerton-Dyer conjecture, Stark conjectures, Bloch-Kato conjectures, etc.

Most of current number theory conjectures originate from (usually mechanised) computations, and have been thoroughly checked numerically. L-functions and their special values are no exception, but available tools and actual computations become increasingly scarce as one goes further away from Dirichlet L-functions. We develop theoretical algorithms and practical tools to study and experiment with (suitable classes of) complex or p-adic L-functions, their coefficients, special or general values, and zeroes. For instance, it is not known whether K-theoretic invariants conjecturally attached to special values are computable in any reasonable complexity model. On the other hand, special values are often readily computed and sometimes provide, albeit conjecturally, the only concrete handle on said invariants.

New theoretical results are translated into new or more efficient functions in the PARI/GP system.

The project lasted from 15/11/2007 to 15/02/2012, for 51 months it received an ANR funding of 200k€ for a global cost of 1M€.

8.2.2. ANR Peace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

http://chic2.gforge.inria.fr/

The PEACE project is joint between the research teams of Institut de Recherche en Mathématiques de Rennes (IRMAR), LFANT and Institut Mathématiques de Luminy (IML).

The project aims to constitute a comprehensive and coherent approach towards a better understanding of theoretical and algorithmic aspects of the discrete logarithm problem on algebraic curves of small genus. On the theorical side, this includes an effective description of moduli spaces of curves, of abelian varieties, the maps that link these spaces and the objects they classify. The effective manipulation of moduli objects will allow us to develop a better understanding of the algorithmic difficulty of the discrete logarithm problem on curves, which may have dramatic consequences on the security and efficiency of already deployed cryptographic devices.

One of the anticipated outcomes of this proposal is a new set of general criteria for selecting and validating cryptographically secure curves (or families of curves) suitable for use in cryptography. Instead of publishing fixed curves, as is done in most standards, we aim at proposing generating rationales along with explicit theoretical and algorithmic criteria for their validation.

8.2.3. ANR Simpatic – SIM and PAiring Theory for Information and Communications security

Participant: Damien Robert.

The SIMPATIC project is an industrial research project, formed by academic research teams and industrial partners: Orange Labs, École Normale Supérieure, INVIA, Oberthur Technologies, ST-Ericsson France, Université de Bordeaux 1, Université de Caen Basse-Normandie, University of Paris 8.

The aim of the SIMPATIC project is to provide the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card. This implementation will then be used to improve and develop new cryptographic efficient algorithms and protocols in the context of mobile phones and SIM cards. The project will more precisely focus on e-ticketing and e-cash, on cloud storage and on the security of contactless and of remote payment systems.

As a member, Damien Robert will aim to bridge the gap between the theoretical results described in the pairing module and the practical realisation of pairing-based SIM cards in an industrial setting.

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. ANTICS

Title: Algorithmic Number Theory in Cryptology

Type: IDEAS

Instrument: ERC Starting Grant

Duration: January 2012 - December 2016

Coordinator: Inria (France)

Abstract: Data security and privacy protection are major challenges in the digital world. Cryptology contributes to solutions, and one of the goals of ANTICS is to develop the next generation public key cryptosystem, based on algebraic curves and abelian varieties. Challenges to be tackled are the complexity of computations, certification of the computed results and parallelisation, addressed by introducing more informatics into algorithmic number theory.

8.3.2. Collaborations in European Programs, except FP7

Program: Erasmus Mundus

Project acronym: ALGANT

Project title: ALgebra, Geometry and Number Theory

Duration: 09/2004–

Coordinator: University Bordeaux 1

Other partners: University Leiden (Netherlands), University Milano (Italy), University Padova (Italy), University Paris-Sud (France), Chennai Mathematical Institute (India), Concordia University (Canada), Stellenbosch University (South Africa)

Abstract: Joint master and doctoral programme; the PhD theses of Athanasios Angelakis and Julio Brau are co-supervised by P. Stevenhagen (Leiden) and K. Belabas

8.4. Research Visitors

- Atelier PARI/GP (23–27/01)

  - Charles Boyd (Amherst)
  - Pierre Castel (Caen)
  - Jeroen Demeyer (Ghent)
  - Tony Ezome (Franceville)
  - Vincent Fleckinger (Besançon)
  - Jean-Pierre Flori (Télécom Paristech)
  - Eduardo Friedman (Santiago de Chile)
  - Loic Grenié (Bergamo)
  - Bernadette Perrin-Riou (Orsay)
  - Firmin Varescon (Besançon)
- Damien Stehlé, Lyon (06–09/03)
- Bernadette Perrin-Riou, Orsay (24–27/01, 09–23/03)
- Vasily Golyshev, Bonn and Moscow (12/03)
- Marco Streng, Warwick (27–30/03)
- Gaëtan Bisson, Sydney (10–13/04)
- David Lubicz, Rennes (10–13/04, 03–07/09, 17–21/12)
- Bruno Salvy, Inria Paris (14/06)
- Workshop MPFR/MPC (25–27/06)
  - Benjamin Dadoun (Nancy)
  - Mickaël Gastineau (Paris)
  - Vincent Lefèvre (Lyon)
  - Patrick Pélissier (Toulouse)
  - Philippe Théveny (Lyon)
  - Paul Zimmermann (Nancy)
- Bernhard Schmidt, Singapore (02/07)
- Fernando Mario, Berlin (09/10)
- Luca De Feo, Versailles (30/10)

8.4.1. Visits to International Teams

J.-M. Couveignes: Tsinghua University, Beijing, 02/04–08/05

A. Enge: Tsinghua University, Beijing, 20/04–02/06

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR Jeunes Chercheurs CAC Computer Algebra and Cryptography (2009-2013).** The contract CAC "Computer Algebra and Cryptography" started in October 2009 for a period of 4 years. This project investigates the areas of cryptography and computer algebra, and their influence on the security and integrity of digital data. In CAC, we plan to use basic tools of computer algebra to evaluate the security of cryptographic schemes. CAC will focus on three new challenging applications of algebraic techniques in cryptography; namely block ciphers, hash functions, and factorization with known bits. To this hand, we will use Gröbner bases techniques but also lattice tools. In this proposal, we will explore non-conventional approaches in the algebraic cryptanalysis of these problems (Participants: L. Perret [contact], J.-C. Faugère, G. Renault).
- **ANR Grant (international program) EXACTA (2010-2013): Exact/Certified Algorithms with Algebraic Systems.**
  The main objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with selected target applications using exact or certified computation. The project consists of one main task of basic research on the design and implementation of fundamental algorithms and four tasks of applied research on computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology. It will last for three years (2010–2013) with 300 person-months of workforce. Its consortium is composed of strong research teams from France and China (KLMM, SKLOIS, and LMIB) in the area of solving algebraic systems with applications.
- **ANR Grant HPAC: High Performance Algebraic Computing (2012-2016).** The pervasive ubiquity of parallel architectures and memory hierarchy has led to a new quest for parallel mathematical algorithms and software capable of exploiting the various levels of parallelism: from hardware acceleration technologies (multi-core and multi-processor system on chip, GPGPU, FPGA) to cluster and global computing platforms. For giving a greater scope to symbolic and algebraic computing, beyond the optimization of the application itself, the effective use of a large number of resources (memory and specialized computing units) is expected to enhance the performance multi-criteria objectives: time, resource usage, reliability, even energy consumption. The design and the implementation of mathematical algorithms with provable, adaptive and sustainable performance is a major challenge. In this context, this project is devoted to fundamental and practical research specifically in exact linear algebra and system solving that are two essential "dwarfs" (or "killer kernels") in scientific and algebraic computing. The project should lead to progress in matrix algorithms and challenge solving in cryptology, and should provide new insights into high performance programming and library design problems (J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din).
- **ANR Grant GeoLMI: Geometry of Linear Matrix Inequalities (2011-2015).** he GeoLMI project aims at developing an algebraic and geometric study of linear matrix inequalities (LMI) for systems control theory. It is an interdisciplinary project at the border between information sciences (systems control), pure mathematics (algebraic geometry) and applied mathematics (optimisation). The project focuses on the geometry of determinantal varieties, on decision problems involving positive polynomials, on computational algorithms for algebraic geometry, on computational algorithms for semi-definite programming, and on applications of algebraic geometry techniques in systems control theory, namely for robust control of linear systems and polynomial optimal control (Participants: J.-C. Faugère, M. Safey El Din [contact]).

8.2. European Initiatives

8.2.1. FP7 Projects

ECRYPT II - European Network of Excellence for Cryptology II is a 4 1/2 year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line Secure, dependable and trusted infrastructures. ECRYPT II started on 1 August 2008. Its objective is to continue intensifying the collaboration of European researchers in information security. The ECRYPT II research roadmap is motivated by the changing environment and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and by the requirements of new applications and cryptographic implementations. Its main objective is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players have integrated their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key algorithms and protocols (MAYA), and hardware and software implementations associate (VAMPIRE). They are joined by more than 20 adjoint members to the network who will closely collaborate with the core partners. The team joins the European Network of Excellence for Cryptology ECRYPT II this academic year as associate member (J.C. Faugère [contact], L. Perret, and G. Renault).

8.3. International Initiatives

8.3.1. Inria Associate Teams

The POLSYS Team and ARIC at ENS Lyon are part of the QOLAPS (Quantifier Elimination, Optimization, Linear Algebra and Polynomial Systems) Associate Team with the Symbolic Computation Group at North Carolina State University.

8.3.2. Participation In International Programs

The POLSYS Team is part of the ECCA (Exact/Certified Computations with Algebraic systems) project at LIAMA in Beijing; our Chinese collaborators are from Beihang University, Peking University, the Chinese Academy of Sciences (Key Laboratory of Mathematics Mechnanization and State Key Laboratory of Information Security).

We are also part of an International Royal Society Joint Project with the Crypto team Royal Holloway, University of London, UK (2010-2012). The Royal Society Joint Project Grant Programme is designed to enable international collaboration. The main goal of the project is to investigate the viability of a wide range of new algebraic techniques in the cryptanalysis of block ciphers, and potentially other symmetric cryptographic algorithms (such as hash functions).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

As part of its collaboration with Guénaël Renault, the Professor Kazuhiro Yokoyama from Rikkyo University (Japan) visited the team during December 2012.

Erich Kaltofen (Professor at North Carolina State University) visited the group in June-July 2012 in the frame of the QOLAPS Associate Team.

Xiao-Shan Gao, Lihong Zhi, Jinsan Cheng (Chinese Academy of Sciences, KLMM) visited the group in July 2012 in the frame of the ECCA project and the ANR EXACTA project.

8.4.1.1. Internships

- T. Verron (Internship M2 and ENS Paris): Computation of Gröbner bases for quasi-homogeneous systems.
- F. Martani (Internship M2): Dedicated Linear Algebra for Gröbner Bases.

SECRET Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **ANR DEMOTIS** ($02/09 \rightarrow 02/12$)
  Collaborative Analysis, Evaluation and Modelling of Health Information Technology
  http://www.demotis.org/
  ANR program: ARPEGE (Systèmes Embarques et Grandes Infrastructures)
  Partners: Sopinspace, Inria (project-teams SECRET and SMIS), CNRS/CECOJI
  55 kEuros.
  DEMOTIS brings together computer scientists and legal scholars. The project experiments new methods for the multidisciplinary design of large information systems that have to take in account legal, social and technical constraints. Its main field of application is personal health information systems. Most notably, work is conducted in priority on the infrastructure for the French personal medical file system (DMP) and secondarily on the data infrastructure for the research and public health networks associated with specific diseases (AIDS, cancer). The aim is to understand how the intrication between the legal and technical domains affects the design of such data infrastructures.
- **ANR SAPHIR-2** ($03/09 \rightarrow 03/13$)
  Security and Analysis of Primitives of Hashing Innovatory and Recent 2
  http://www.saphir2.fr/
  ANR program: VERSO (Reseaux du Futur et Services)
  Partners: France Telecom, Gemalto, Cryptolog international, EADS SN, Sagem Securite, ENS/LIENS, UVSQ/PRISM, Inria (project-team SECRET), ANSSI
  153 kEuros
  This industrial research project aims at participating to the NIST competition (cryptanalysis, implementations, optimizations, etc.), and in supporting the SHA-3 candidates proposed by its partners.
- **ANR COCQ** ($01/09 \rightarrow 07/12$)
  Codes correcteurs quantiques
  http://www-roc.inria.fr/secret/Jean-Pierre.Tillich/COCQ.html
  ANR program: Domaines emergents
  Partners: ENSEA, Inria (project-team SECRET), Université de Bordeaux, Telecom ParisTech
  117 kEuros
  This project deals with the development of fundamental research on error correcting codes for quantum channels. In particular, we aim to suggest suitable generalizations to the quantum setting of the best known families of quantum codes (such as LDPC or turbo-codes) and to analyze their performance.
- **ANR BLOC** ($10/11 \rightarrow 09/15$)
  Conception et analyse de chiffrements par blocs efficaces pour les environnements contraints
  ANR program: Ingénierie numérique et sécurité
  Partners: INSA Lyon, Inria (project-team SECRET), University of Limoges (XLIM), CryptoExperts
  446 kEuros
  The BLOC project aims at providing strong theoretical and practical results in the domain of cryptanalyses and design of block ciphers.

- **ANR KISS** ($12/11 \rightarrow 12/15$)
  Keep your personal Information Safe and Secure
  ANR program: Ingénierie numérique et sécurité
  Partners: Inria (project-teams SMIS and SECRET), LIRIS, Gemalto, UVSQ (Prism), Conseil Général des Yvelines
  64 kEuros
  The KISS project builds upon the emergence of new portable and secure devices known as Secure Portable Tokens (e.g., mass storage SIM cards, secure USB sticks, smart sensors) combining the security of smart cards and the storage capacity of NAND Flash chips. The idea promoted in KISS is to embed, in such devices, software components capable of acquiring, storing and managing securely personal data.

7.1.2. Others

- **French Ministry of Defense** ($01/11 \rightarrow 12/13$)
  Funding for the supervision of Marion Bellard's PhD.
  30 kEuros.
- **French Ministry of Defense** ($10/12 \rightarrow 09/15$)
  Funding for the supervision of Audrey Tixier's PhD.
  30 kEuros.
- **DGA-MI** ($12/11 \rightarrow 02/13$)
  Analysis of binary streams.
  20 kEuros.

7.2. European Initiatives

Associate member of the ECRYPT II European network of excellence ($08/08 \rightarrow 07/12$) http://www.ecrypt.eu.org/

7.2.1. Collaborations with Major European Organizations

Otto-von-Guericke Universität Magdeburg, Institut für Algebra und Geometrie (Germany)
Study of Boolean functions for cryptographic applications
DTU - Danmarks Tekniske Universitet, Department of Mathematics
Symmetric crytography and code-based cryptography

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Gohar Kyureghyan, Otto-von-Guericke Universität Magdeburg, Germany, from October 2011 to June 2012
- Davide Schipani, Universität Zurich, Switzerland, February 13-17
- Sergey Abrahamyan, Institute for Informatics and Automation Problems, Yerevan, Armenia, May 20-26
- Yves Edel, Gent University, Belgium, June 3-9
- Christiane Peters, DTU, Denmark, November 19-23
- Stefan Heyse, Ingo von Maurich and Ralf Zimmermann, Ruhr-Universität Bochum, Germany, November 19-23
- Grigory Kabatyanskiy, IPIT, Moscow, Russia, December 17-21 .

7.3.2. Visits to International Teams

- DTU-Mathematics, Denmark Technical University, Denmark, January-August, 8-month sabbatical stay funded by the DGA (A. Canteaut).
- School of Informatics, University of Edinburgh, Scotland, December 3-6, invitation to the *Quantum Security Meeting*, and visit of Elham Kashefi's group (A. Leverrier).

VEGAS Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR

The ANR blanc PRESAGE brings together computational geometers (from the VEGAS and GEOMETRICA projects of Inria) and probabilistic geometers (from Universities of Rouen, Orléans and Poitiers) to tackle new probabilistic geometry problems arising from the design and analysis of geometric algorithms and data structures. We focus on properties of discrete structures induced by or underlying random continuous geometric objects.

This is a four year project, with a total budget of 400kE, that started on Dec. 31st, 2011. It is coordinated by Xavier Goaoc (VEGAS).

6.2. International Research Visitors

6.2.1. Visits of International Scientists

William J. Lenhart, Williams College (USA), one year sabbatical until July 2012.

Boris Aronov, from NYU-Poly, visited the VEGAS project for 2 weeks in October.

Martin Tancer, Pavel Paták and Zuzana Safernová, from Charles Univ. in Prague, visited the VEGAS project for 1 week in August.

Hyo-Sil Kim (postdoc at POSTECH, South Korea) and Jae-Soon Ha (PhD student at KAIST, South Korea) visited the VEGAS project for 2 weeks in February.

ALF Project-Team

8. Partnerships and Cooperations

8.1. European Initiatives

8.1.1. DAL: ERC AdG 2010- 267175, 04-2011/03-2016

Participants: Pierre Michaud, Luis Germán García Morales, Nathanaël Prémillieu, Erven Rohou, André Seznec, Bharath Narasimha Swamy, Ricardo Andrés Velásquez, Arthur Pérais, Surya Narayanan, Arjun Suresh, Sajith Kalathingal, Kamil Kedzierski.

In the DAL, Defying Amdahl's Law project, we envision that, around 2020, the processor chips will feature a few complex cores and many (may be 1000s) simpler, more silicon and power effective cores. In the DAL research project, we will explore the microarchitecture techniques that will be needed to enable high performance on such heterogeneous processor chips. Very high performance will be required on both sequential sections —legacy sequential codes, sequential sections of parallel applications— and critical threads on parallel applications —e.g. the main thread controlling the application. Our research will focus on enhancing single process performance. On the microarchitecture side, we will explore both a radically new approach, the sequential accelerator, and more conventional processor architectures. We will also study how to exploit heterogeneous multicore architectures to enhance sequential thread performance.

For more information, see http://www.irisa.fr/alf/dal.

8.1.2. HiPEAC3 NoE

Participants: François Bodin, Pierre Michaud, Erven Rohou, André Seznec.

F. Bodin, P. Michaud, A. Seznec and E. Rohou are members of the European Network of Excellence HiPEAC3. HiPEAC3 addresses the design and implementation of high-performance commodity computing devices in the 10+ year horizon, covering both the processor design, the optimizing compiler infrastructure, and the evaluation of upcoming applications made possible by the increased computing power of future devices.

8.1.3. COST Action TACLe - Timing Analysis on Code-Level 10-2012/09-2015

Participants: Damien Hardy, Isabelle Puaut.

Embedded systems increasingly permeate our daily lives. Many of those systems are business- or safety-critical, with strict timing requirements. Code-level timing analysis is indispensable to ascertain whether these requirements are met. However, recent developments in hardware, especially multicore processors, and software organization make the analysis increasingly harder, thus challenging the evolution of timing analysis techniques. Principles for building "timing-composable" embedded systems are needed to make timing analysis tractable in the future. The furthering and consolidation of those principles require increased contacts within the timing analysis community as well as with the neighboring communities that deal with other forms of analysis, such as model checking and type inference, and with computer architectures and compilers. The goal of this COST Action (http://www.cost.eu/domains_actions/ict/Actions/IC1202) is to gather these forces in order to develop industrial strength code-level timing analysis techniques for future generation embedded systems.

Twelve countries are currently involved in this COST action.

8.2. Regional Initiative

8.2.1. Britanny region fellowship

Participants: Ricardo Andrés Velásquez, Pierre Michaud, André Seznec.

The Britanny region is funding a Ph.D. fellowship for Ricardo Velasquez on the topic "Fast hybrid multicore architecture simulation".

8.3. National Initiatives

8.3.1. ANR PetaQCD 01-2009/10-2012

Participants: Junjie Lai, André Seznec.

Simulation of Lattice QCD is a challenging computational problem that requires very high performance exceeding sustained Petaflops/s. The ANR PetaQCD project combines research groups from computer science, physics and two SMEs (CAPS Entreprise, Kerlabs) to address the challenges of the design of LQCD oriented supercomputer.

8.3.2. ANR W-SEPT

Participants: Hanbing Li, Isabelle Puaut, Erven Rohou.

Critical embedded systems are generally composed of repetitive tasks that must meet drastic timing constraints, such as termination deadlines. Providing an upper bound of the worst-case execution time (WCET) of such tasks at design time is thus necessary to prove the correctness of the system. Static WCET estimation methods, although safe, may produce largely over-estimated values. The objective of the project is to produce tighter WCET estimates by discovering and transforming flow information at all levels of the software design process, from high level-design models (e.g. Scade, Simulink) down to binary code. The ANR W-SEPT project partners are Verimag Grenoble, IRIT Toulouse, Inria Rennes. A case study is provided by Continental Toulouse.

8.3.3. Large Scale Initiative: Large scale multicore virtualization for performance scaling and portability

Participant: Erven Rohou.

An Inria Large Scale Initiative (Action d'Envergure) has been submitted and approved. It is entitled "Large scale multicore virtualization for performance scaling and portability". Partner project-teams include: ALF, ALGORILLE, CAMUS, REGAL, RUNTIME, as well as DALI.

This project aims to build collaborative virtualization mechanisms that achieve essential tasks related to parallel execution and data management. We want to unify the analysis and transformation processes of programs and accompanying data into one unique virtual machine.

8.3.4. ADT PADRONE 2012-2014

Participants: Erven Rohou, Emmanuel Riou.

Computer science is driven by two major trends: on the one hand, the lifetime of applications is much larger than the lifetime of the hardware for which they are initially designed; on the other hand the diversity of computing hardware keeps increasing. The net result is that many applications are not optimized for their current executing environment. The objective of PADRONE is to design and develop a platform for re-optimization of binary executables at run-time. There are many advantages: actual hardware is known, the whole application is visible (including libraries), profiling can be collected, and source code is not necessary (interesting in the case of proprietary applications).

8.4. International Initiative

8.4.1. PHC Imhotep (Egypt): Code obfuscation through JIT compilation, Jan 2012 – Dec 2013

Participant: Erven Rohou.

Collaboration with Pr Ahmed El-Mahdy, Egypt-Japan University for Science and Technology (Alexandria, Egypt)

This project proposes to leverage JIT compilation to make software tamper-proof. The idea is to constantly generate different versions of an application, even while it runs, to make reverse engineering hopeless. A strong random number generator will guarantee that generated code is not reproducible – though the functionality is the same. Performance will not be sacrificed thanks to multi-core architectures: the JIT runs on separate cores, overlapping with the execution of the application.

CAIRN Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. FP7 FLEXTILES

Participants: Olivier Sentieys, Emmanuel Casseau, Antoine Courtay, Daniel Chillet, Philippe Quémerais, Christophe Huriaux, Quang-Hoa Le.

Program: FP7-ICT-2011-7

Project acronym: Fmextiles

Duration: Oct. 2011 - Sep. 2014

Coordinator: Thales

Other partners: Thales (FR), UR1 (FR), KIT (GE), TU/e (NL), CSEM (SW), CEA LETI (FR), Sundance (UK)

Project title: Self Adaptive Heterogeneous Manycore Based on Flexible Tiles

A major challenge in computing is to leverage multi-core technology to develop energy-efficient high performance systems. This is critical for embedded systems with a very limited energy budget as well as for supercomputers in terms of sustainability. Moreover the efficient programming of multi-core architectures, as we move towards manycores with more than a thousand cores predicted by 2020, remains an unresolved issue. The FlexTiles project will define and develop an energy-efficient yet programmable heterogeneous manycore platform with self-adaptive capabilities. The manycore will be associated with an innovative virtualisation layer and a dedicated tool-flow to improve programming efficiency, reduce the impact on time to market and reduce the development cost by 20 to 50%. FlexTiles will raise the accessibility of the manycore technology to industry - from small SMEs to large companies - thanks to its programming efficiency and its ability to adapt to the targeted domain using embedded reconfigurable technologies.

7.1.2. FP7 ALMA

Participants: Steven Derrien, Romuald Rocher, Olivier Sentieys, Maxime Naullet, Ali Hassan El Moussawi.

Program: FP7-ICT-2011-7

Project acronym: Alma

Project title: Architecture oriented paraLlelization for high performance embedded Multicore systems using scilAb

Duration: Sep. 2011 - Aug. 2014

Coordinator: KIT

Other partners: KIT (GE), UR1 (FR), Recore Systems (NL), Univ. of Peloponnese (GR), TEI-MES (GR), Intracom SA (GR), Fraunhofer (GE)

The mapping process of high performance embedded applications to today's multiprocessor system on chip devices suffers from a complex toolchain and programming process. The problem here is the expression of parallelism with a pure imperative programming language which is commonly C. This traditional approach limits the mapping, partitioning and the generation of optimized parallel code, and consequently the achievable performance and power consumption of applications from different domains. The Architecture oriented paraLlelization for high performance embedded Multicore systems using scilAb (ALMA) project aims to bridge these hurdles through the introduction and exploitation of a Scilab-based toolchain which enables the efficient mapping of applications on multiprocessor platforms from high-level abstraction descriptions. This holistic solution of the toolchain allows the complexity of both the application and the architecture to be hidden, which leads to a better acceptance, reduced development cost and shorter time-to-market. Driven by the technology restrictions in chip design, the end of Moore's law and an unavoidable increasing request of computing performance, ALMA is a fundamental step forward in the necessary introduction of novel computing paradigms and methodologies. ALMA helps to strengthen the position of Europe in the world market of multiprocessor targeted software toolchains. The challenging research will be achieved by the unique ALMA consortium which brings together industry and academia. High class partners from industry such as Recore and Intracom, will contribute their expertise in reconfigurable hardware technology for multi-core systems-on-chip, software development tools and real world applications. The academic partners will contribute their outstanding expertise in reconfigurable computing and compilation tools development.

7.1.3. Collaborations with Major European Organizations

Imec (Belgium), Scenario-based fixed-point data format refinement to enable energy-scalable of Software Defined Radios (SDR)

Lund University (Sweden), Constraints programming approach application in the reconfigurable data-paths synthesis flow

Code and Cryptography group of University College Cork (Ireland), Arithmetic operators for cryptography and WSN for health monitoring

Ecole Polytechnique Fédérale de Lausanne - EPFL (Switzerland), Optimization of systems using fixed-point arithmetic

Technical University of Madrid - UPM (Spain), Optimization of systems using fixed-point arithmetic

Technical University of Tampere, University of Oulu (Finland), Reconfigurable Video Coding

Hervé Yviquel spent 4 months in the group of Jarmo Takala at Tampere University of Technology, Finland, from March.

7.2. National Initiatives

The CAIRN team has currently some collaboration with the following laboratories: CEA List, SATIE ENS Cachan, LEAT Nice, Lab-Sticc (Lorient, Brest), LIRMM (Montpellier, Perpignan), ETIS Cergy, LIP6 Paris, IETR Rennes, Ireena Nantes; and with the following Inria project-teams: Aric, Compsys, Swing, Symbiose, TexMex.
The team participates in the activities of the following research organization of CNRS (GdR for in French *"Groupe de Recherche"*):

- GdR SOC-SIP (*System On Chip & System In Package*), working groups on reconfigurable architectures, embedded software for SoC, low power issues. See http://www2.lirmm.fr/~w3mic/SOCSIP/index.php. CAIRN is the leader of the group on reconfigurable architectures.
- GdR ISIS (*Information Signal ImageS*), working group on *Algorithms Architectures Adequation*.
- GdR ASR (*Architectures Systèmes et Réseaux*)
- GdR IM (*Informatique Mathématiques*), C2 working group on Codes and Cryptography and ARITH working group on Computer Arithmetic

7.2.1. ANR Blanc - PAVOIS (2012–2016)

Participants: Arnaud Tisserand, Emmanuel Casseau, Romuald Rocher, Philippe Quémerais, Jérémie Métairie.

PAVOIS (in French: *Protections Arithmétiques Vis à vis des attaques physiques pour la cryptOgraphIe basée sur les courbeS elliptiques*) is a project on Arithmetic Protections Against Physical Attacks for Elliptic Curve based Cryptography. It involves IRISA-CAIRN (Lannion) and LIRMM (Perpignan and Montpellier). This project will provide novel implementations of curve based cryptographic algorithms on custom hardware platforms. A specific focus will be placed on trade-offs between efficiency and robustness against physical attacks. One of our goal is to theoretically study and practically measure the impact of various protection schemes on the performance (speed, silicon cost and power consumption). Theoretical aspects will include an investigation of how special number representations can be used to speed-up cryptographic algorithms, and protect cryptographic devices from physical attacks. On the practical side, we will design innovative cryptographic hardware architectures of a specific processor based on the theoretical advancements described above to implement curve based protocols. We will target efficient and secure implementations for both FPGA an ASIC circuits. For more details see http://pavois.irisa.fr.

7.2.2. ANR INFRA 2011 - FAON (2012-2015)

Participants: Raphaël Bardoux, Arnaud Carer, Matthieu Gautier, Pascal Scalart.

The FAON (Frequency based Access Optical Networks) project objectives are to demonstrate the technology and feasibility of a new type of Passive Optical Network (PON) for broadband access which uses a Frequency based shared access technique known as Frequency Division Multiplexing (FDM). These goals completely fall into the line of the expected capacity increase in PON which is today forecasted to go from 100 Mbps per user to 1 Gbps. For more details, see http://www.anr-faon.fr/. Faon involves Orange Labs, CEA-LETI, University of South Brittany (Lab-STICC laboratory) and University of Rennes 1 (Foton laboratory and CAIRNteam). CAIRNaims at developing a high-rate architecture at the receiver side. Specific receiver algorithms (synchronization and equalization) and FPGA implementation are the key issues that will be addressed.

7.2.3. Equipex FIT - Future Internet (of Things)

Participants: Vaibhav Bhatnagar, Arnaud Carer, Matthieu Gautier, Ganda-Stéphane Ouedraogo, Olivier Sentieys.

FIT is one of 52 winning projects from the first wave of the French Ministry of Higher Education and Research's "Équipements d'Excellence" (Equipex) research grant programme. FIT involves UPMC, Inria, LSIIT and the Institut Mines-Telecom and runs over a nine-year period. FIT offers a federation of several independent experimental testbeds to provide a larger-scale, more diverse and higher performance platform for accomplishing advanced experiments. For more details, see http://fit-equipex.fr/. Inria (CAIRNand Socrate teams) develops the cognitive radio testbed that will provide a full experimental environment for evaluating the coexistence and the cooperation between heterogeneous multistandard nodes. To this aim, a fully open architecture based on software defined radio nodes is developed. CAIRNaims at proposing an FPGA based software defined radio with high level specifications. Cognitive radio testbed development is supported by an ADT funding of Inria.

7.2.4. ANR Ingénérie Numérique et Sécurité - ARDyT (2011-2015)

Participants: Sébastien Pillement, Arnaud Tisserand, Philippe Quémerais.

ARDyT (in French: *Architecture Reconfigurable Dynamiquement Tolérante aux fautes*) is a project on a Reliable and Reconfigurable Dynamic Architecture. It involves IRISA-CAIRN (Lannion), Lab-STICC (Lorient), LIEN (Nancy) and ATMEL. The purpose of the ARDyT project is to provide a complete environment for the design of a fault tolerant and self-adaptable platform. Then, a platform architecture, its programming environment and management methodologies for diagnosis, testability and reliability have to be defined and implemented. The considered techniques are exempt from the use of hardened components for terrestrial and

aeronautics applications for the design of low-cost solutions. The ARDyT platform will provide a European alternative to import ITAR constraints for fault-tolerant reconfigurable architectures. For more details see http://ardyt.irisa.fr.

7.2.5. ANR Ingénérie Numérique et Sécurité - COMPA (2011-2015)

Participants: Emmanuel Casseau, Steven Derrien, Sébastien Pillement.

COMPA (model oriented design of embedded and adaptive multiprocessor) is a project which involves CAIRN, IETR (Institut d'Electronique et de Télécommunications de Rennes), Lab-STICC (University of Bretagne Sud), CAPS Entreprise, Modae Technologies and Texas Instruments. The goal of the project is to design adaptive multiprocessor embedded systems from dataflow models. Reconfigurable video coding (RVC) standard will be targeted as application use case. We will then more specifically focus on the use of the portable and platform-independent RVC-CAL language to describe the applications. We will propose transformations in order to refine, optimize and translate the application model into software and hardware components. Task mapping, instructions and processor allocation, and constrained scheduling will also be investigated for runtime execution and reconfiguration.

7.2.6. ANR Ingénérie Numérique et Sécurité - DEFIS (2011-2015)

Participants: Olivier Sentieys, Daniel Menard, Romuald Rocher, Nicolas Simon.

DEFIS (Design of fixed-point embedded systems) is a project which involves CAIRN, LIP6 (University of Paris VI), LIRMM (University of Perpignan), CEA LIST, Thales, Inpixal. The main objectives of the project are to propose new approaches to improve the efficiency of the floating-point to fixed-point conversion process and to provide a complete design flow for fixed-point refinement of complex applications. This infrastructure will reduce the time-to-market by automating the fixed-point conversion and by mastering the trade-off between application quality and implementation cost. Moreover, this flow will guarantee and validate the numerical behavior of the resulting implementation. The proposed infrastructure will be validated on two real applications provided by the industrial partners. For more details see http://defis.lip6.fr.

7.2.7. ANR ARPEGE - GRECO (2010-2013)

Participants: Olivier Sentieys, Olivier Berder, Arnaud Carer, Trong-Nhan Le.

Sensor network technologies and the increase efficiency of photovoltaic cells show that it is possible to reach communicating objects solutions with low enough power consumption to foresee the possibility of developing autonomous objects. Greco (GREen wireless Communicating Objects) is a project on the design of autonomous communicating object platforms (i.e. self-powered sensor networks). The aim is to optimize the power consumption based on (i) a modeling of the performance and power of the required blocks (RF front-end, converters, modem, peripherals, digital architecture, OS, software, power generator, battery, etc.) (ii) heterogeneous simulation models and tools, and (iii) the use of a real-time global "Power Manager". The final validation will be performed on various case studies: a monitoring system and an audio communication between firemen. A HW/SW prototyping (based on an CAIRN's PowWow platform with energy harvesting) and a simulation associating a precise modeling (virtual platform) of an object inserted in a network simulator-like environment will be developed as demonstrators. Greco involves Thales, Irisa-CAIRN, CEA List, CEA Leti, Im2nP, LEAT, Insight-SiP. For more details see http://greco.irisa.fr.

7.2.8. S2S4HLS

Participants: Emmanuel Casseau, Steven Derrien, Daniel Menard, Olivier Sentieys, Antoine Morvan, Chenglong Xiao, Jean-Charles Naud.

NANO2012 Program - S2S4HLS (2008-2012)

High-level synthesis (HLS) tools start to be used for industrial designs. HLS is analogous to software compilation transposed to the hardware domain. From an algorithmic behavior of the specification, HLS tools automate the design process and generate a register transfer level RTL architecture taking account of user-specified constraints. However, design performance still depends on designer's skill to write the appropriate source code. The S2S4HLS (Source-to-Source for High-Level Synthesis) project intends to process source code transformations to guide synthesis hence leading to more efficient designs, and aims at providing a toolbox for automatic C code source-to-source transformations. The project is focused on three complementary goals to push the limits of existing HLS tools: loop transformations for performance optimization and a better resource usage, automatic floating-point to fixed-point conversion and synthesis of multi-mode architectures. S2S4HLS is organized into three sub-projects targeting these three objectives. The project is in close collaboration with STMicroelectronics and Compsys team at Inria Rhône-Alpes, within the overall Inria-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program. CAIRNis responsible of the project and involved in the three workpackages.

7.2.9. NANO2012 Program - RecMotifs (2008-2012)

Participants: François Charot, Antoine Floc'h, Christophe Wolinski.

The RecMotifs project aims at the generation of application specific extensions targeting the STxP70 processor from STMicroelectronics. CAIRNwill study advanced technologies algorithms for graph matching and graph merging together with constraints programming methods. The project is in close collaboration with STMicroelectronics within the overall Inria-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program.

7.2.10. ANR Architectures du Futur Open-People (2009-2012)

Participants: Daniel Chillet, Robin Bonamy, Olivier Sentieys.

The Open-People (Open Power and Energy Optimization PLatform and Estimator) project aims at defining a complete platform for power estimation and optimization. The platform will be composed of hardware boards to support measurements for the applications. End-users will be able to upload their applications through a web portal, and to control the power measurements of the execution of their applications on a specific electronic board. The Open-People project will also propose a complete power component model library which allows end-users to estimate the power consumption of some parts of the applications without making measurements. This will allow to quickly evaluate the different design choices regarding the power consumption. Finally, through the web portal http://www.open-people.fr, Open-People will propose software tools to apply power optimizations. In this project, CAIRN team will develop power model for FPGA components using dynamic reconfiguration. Open-People involves LabSticc (Lorient), Trio (Nancy), CAIRN (Rennes/Lannion) and Dart (Lille/Valenciennes) teams from Inria, Leat at Nice, Thales (Colombes) and InPixal (Rennes). CAIRNis in charge of power models and optimization for reconfigurable architectures.

7.2.11. Images and Networks competitiveness cluster - 100GFlex project (2010-2013)

Participants: Olivier Sentieys, Arnaud Carer, Remi Pallas, Pascal Scalart.

Speed and flexibility are quickly increasing in the metropolitan networks. In this context, 100GFLEX studies the relevance of a new transmission scheme: the multiband optical OFDM at very-high rates (up to 100 Gbits/s). In this project we will study efficient algorithms (e.g. synchronization) and high-speed architectures for the digital signal processing of the optical transceivers. Due to the high rate of analog signals (sampling at more than 10Gsample/s), synchronizing and processing is real challenge. 100Gflex involves Mitsubishi-Electric R&D Center Europe, Institut Télécom, Ekinops, France Télécom, Yenista Optics, Foton and CAIRN.

7.3. International Initiatives

7.3.1. Inria Associate Team LRS

Title: Loop unRolling Stones: compiling in the polyhedral model

Inria principal investigator: Steven Derrien

International Partner (Institution - Laboratory - Researcher):

Colorado State University (United States) - Mélange Group

Duration: 2010 - 2012

See also: http://www.irisa.fr/cosi/HOMEPAGE/Derrien/EA-2010/LRS.htm

The goal of the team is twofold: i) Propose new methodologies and algorithms to tackle some of the open problems in automatic parallelization and high level hardware synthesis from nested loop specifications. In particular, we would like to address the problem of parallelization of complex bioinformatics algorithms based of sophisticated dynamic programming algorithms, for which we would like to propose efficient parallelization schemes for both FPGAs (Field Programmable Gate Arrays) and GPUs (Graphical Processing Units). ii) Provide a common open software infrastructure based on (modern/cutting edge) software engineering techniques (Model Driven Software Development) so as to help researchers prototyping new ideas and concept in the domain of optimizing compilers. Our goal being to be able to make our in-house software completely interoperable.

7.3.2. Inria International Partners

LRTS laboratory, Laval University in Québec (Canada), Architectures for MIMO systems, Wireless Sensor Networks, Inria Associate Team (2006-2008)

LSSI laboratory, Québec University in Trois-Rivières (Canada), Design of architectures for digital filters and mobile communications

Computer Science Department, Colorado State University in Fort-Collins (USA), Loop parallelization, development of high-level synthesis tools, Inria Associate Team (2010-2012)

University of Adelaide (Australia), Arithmetic operators

VLSI CAD lab, Electrical and Computer Engineering Department, University of Massachusetts at Amherst (USA), CAD tools for arithmetic datapath synthesis and optimization

7.3.3. CNRS PICS - SPiNaCH (2012 - 2014)

Title: Secure and low-Power sensor Networks Circuits for Healthcare embedded applications

Principal investigator: Arnaud Tisserand, Olivier Berder, Olivier Sentieys

International Partner (Institution - Laboratory - Researcher):

Code&Crypto group in University College Cork (Ireland)

Duration: 2012 - 2014

Biomedical sensor networks may be used more and more in the future. For instance, they allow patient's health-care parameters to be remotely monitored at home. In this project, we plan to address two important challenges in the design of biomedical sensors networks: i) design of low-power sensor devices for embedded autonomous systems (health monitoring, pace-maker...) with long battery life; ii) confidentiality and security aspects and especially with public key cryptography processor that are robust against side channel attacks (measure of the computation time, the power consumption or the electromagnetic radiations of the circuit) and with limited power-energy resources.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Prof. Gabriel Caffarena (University CEU-San Pablo, Madrid) for one month in August-September.

Prof. Maciej Ciesielski (University of Massachusetts, VLSI CAD Laboratory, USA) for one month in June-July.

Dr Muhammad Adeel Ahmed Pasha, Assistant Professor at LUMS for a two-month stay in July-August.

PhD Student Nabil Ghanmy (University of Sfax, Tunisia) for one month in November-December.

PhD Student Tomofumi Yuki (Colorado State University, USA) for two months in November and December.

Prof. Sanjay Rajopadhye (Colorado State University, USA) for one week in December.

7.4.2. Internships

Simara Pérez Zurita (from Oct 2012 until Aug 2013)

Subject: Optimizing Computational Precision in High-level Synthesis of Signal Processing Systems: Theory and Implementation using TDS and GECOS

Institution: *Technical University of Kaiserslautern* (Kaiserslautern, Germany)

CAMUS Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. Action d'Envergure Nationale

Philippe Clauss, Alain Ketterlin and Vincent Loechner are involved in the proposition of an Inria Large Scale Initiative (*Action d'Envergure Nationale*) entitled "Large scale multicore virtualization for performance scaling and portability" and regrouping several french researchers in compilers, parallel computing and program optimization. Philippe Clauss shares the head of the project with Gilles Muller of the Inria REGAL team. The project should start officially early 2013. Philippe Clauss and Erven Rohou (ALF team) will co-advise a PhD thesis on dynamic binary code analysis, parallelization and optimization in the frame of this project.

7.2. International Initiatives

7.2.1. Inria Associate Teams

7.2.1.1. ANCOME

Title: Memory and applications memory behavior

Inria principal investigator: Philippe Clauss

International Partner (Institution - Laboratory - Researcher):

University of Buenos Aires (Argentina) - Departamento de Computación, Facultad de Ciencias Exactas y Naturales - Sergio Yovine

Duration: 2011 - 2013

See also: http://lafhis.dc.uba.ar/wiki/index.php/EA-Ancome

This associate team focuses on developing original methods for the analysis of programs memory behavior, in particular in the context of applications using dynamic memory allocation. The proposed approaches consist in analyzing and modeling the runtime behavior, where extracted properties are then verified thanks to static analysis processes. Thus pure static approaches limits will be overpassed. Further, the case of multi-threaded applications run on multi-core architectures will be studied in order to elaborate and extend our analysis techniques and to extract properties specific to this context. The issues are mainly concerned with the conception of real-time applications using dynamic memory allocation.

7.2.2. Participation In International Programs

The collaboration between the LaFhis team of the University of Buenos Aires and the CAMUS team has also been supported by the CNRS-MINCyt project QUATRIX since 2011.

The CAMUS team is associated to the CNRS-CONICET Associated International Laboratory France-Argentina INFINIS (INformatique Fondamentale, logIque, laNgages, vérIfication et Systèmes) inaugurated in December 2011.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Rachid Seghir, assistant professor at University of Batna (Algeria), was invited in our team from May 10 to 26, 2012. We worked on improving `ZPolyTrans`, our library for computing integer affine images of $\mathbb{Z}$-polyhedra. More precisely, we have implemented non-regression tests and we improved the performance of the library by reducing the complexity of some algorithms. Our major publication on this topic was published in 2012 in ACM TACO [15].

Diego Garbervetsky, University of Buenos Aires, Argentina, has spent two weeks of October 2012 in the CAMUS team.

7.3.1.1. Internships

Juan Manuel Martinez Caamaño, who is Master student at the University of Buenos Aires, is doing his Master thesis internship in the CAMUS team from August 2012 to January 2013.

Gervasio Perez, PhD student at the University of Buenos Aires, Argentina, has spent one month in the CAMUS team in November 2012.

7.3.2. Visits to International Teams

Philippe Clauss visited the parallel computing research team of the University of Tunis, Tunisia, from November the 26th to the 30th. The main goal of the visit was to meet the student Imèn Fassi and her co-advisor Yosr Slama to work for the starting co-advised PhD thesis.

Alain Ketterlin has spent three weeks in the LAFHIS team in January 2012.

Philippe Clauss has spent one week in the LAFHIS team in December 2012.

COMPSYS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. CNRS PEPS

Christophe Alias and Laure Gonnord initiated with the DART/Emeraude team at LIFL Laboratory (University of Lille) a CNRS PEPS ("Projets Exploratoire Premier Soutien") called "HLS and real time" (8kEuros/year, during two years). The goal of this project is to investigate how to introduce real-time constraints in the high-level synthesis workflow.

8.1.2. Inria AEN

Compsys is part of an Inria Large Scale Initiative (AEN: action d'envergure nationale) that regroups eight teams: Camus, Regal, Alf, Runtime, Algorille, Parkas, Dali on "Large scale multicore virtualization for performance scaling and portability".

8.1.3. French compiler community

The french compiler community is now well identified and is visible through its web-page http://compilation.gforge.inria.fr/. The "journées françaises de la compilation" were initiated in 2010 and are still animated by Fabrice Rastello and Laure Gonnord as a biannual event. Their local organization is handled alternately by the different research teams (Lyon in Summer 2010, Aussois in Winter 2010, Dinard in Spring 2011, St Hippolyte in Autumn 2011, Rennes in Summer 2012, Lyon/Annecy in Spring 2013).

8.2. International Research Visitors

8.2.1. Visits to International Teams (at least one month)

Paul Feautrier has been invited to spend the month of June 2012 at Colorado State University (CSU), Fort Collins, CO, USA, in prof. Sanjay Rajopadhye's team. The work reported in Section 6.2 and accepted at PPoPP'13 [13] was initiated during this stay. Sanjay Rajopadhye and Tomofumi Yuki, both from CSU, have spent a few days in Paris and Lyon in December 2012. During this visit, we have initiated a sequel to this work, which will handle other parallel features of X10.

8.2.2. Informal Collaborations and Short-Term Visitors

Shorter visits (but at least a week) include exchanges (in both directions) with the groups of S. Rajopadhye (Colorado State University), of P. Sadayappan (Ohio State University), of J. Ramanujam (Louisiana State University), of L.-N. Pouchet (UCLA), all related directly or indirectly to polyhedral code optimizations.

Compsys has also regular contacts with Sebastian Hack (Saarland University, Saarbrücken, Germany), Benoît Dupont de Dinechin (Kalray, Grenoble), Christophe Guillon (STMicroelectronics), Fernando M. Q. Pereira (Federal University of Mina Gerais, Brazil) on back-end code optimizations.

Among french academic researchers, Compsys is particularly linked with people such as Albert Cohen (Inria Parkas team), Steven Derrien (Inria Cairn team), Alain Ketterlin (Inria Camus team), François Irigoin (Ecole des Mines de Paris).

Finally, taking the opportunity of the HdR defense of Fabrice Rastello [2] and the PhD defense of Quentin Colombet [1] on December 7, 2012, a "compilation day" was organized in Lyon on December 6, including talks by K. Pingali (University of Texas, Austin), E. Altman (IBM Yorktown), and V. Sarkar (Rice University).

AOSTE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. CIM PACA

Participants: Robert de Simone, Ameni Khecharem, Carlos Gomez Cardenas.

This ambitious regional initiative is intended to foster collaborations between local PACA industry and academia partners on the topics of microelectronic design, though mutualization of equipments, resources and R&D concerns. We are so far actively participating in the Design Platform (one of the three platforms launched in this context), of which Inria is a founding member.

This year our ANR proposal HOPE was labeled by the regional SCS Cluster, through its ARCSIS/CIM PACA branch for microelectronics design. The project was consequently accepted, and will benefit from support from CIM PACA Design platform to host prototype and commercial software from project members (Synopsys, Docea Power, and Magillem, see 8.2.1.3).

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. RT-Simex

Participants: Julien deAntoni, Frédéric Mallet.

The RT-Simex project is dedicated to the reverse engineering of analysis traces of simulation and execution back up to the source code, or in our case most likely into the original models in a MARTE profile representation. The prime contractor is OBEO, a software publishing company based in Nantes. The project ended in April 2012.

8.2.1.2. HeLP

Participants: Carlos Gomez Cardenas, Ameni Khecharem, Robert de Simone, Jean-Vivien Millo.

The ANR HeLP project deals with joint modeling of functional behavior and energy consumption for the design of low-power heterogeneous SoCs. Partners are ST Microelectronics and Docea Power (SME) as industrial; Inria, UNS (UMR LEAT), and VERIMAG (coordinator) as academics. Our goal in this project is twofold: first, combine SoC modeling with temporal behavior and logical time with energy/power modeling as extra annotations on MARTE models; second, compare the capacities of high-level SystemC TLM abstraction with that of Esterel seen as a multiclock formalism based on logical abstract time.

The PhD thesis of Carlos Gomez, while not formerly funded by this project, is closely linked to its results (by providing a MDE metamodel with non-functional multiview aspects, such as performance, power and temperature. Several transformation links were realized, towards AcePlorer tool by DOCEA POWER, partner of the project, or also (as part of Ameni Khecharem internship) towards Scilab for simulation execution. Some of this work will be continued in the forthcoming ANR HOPE project.

8.2.1.3. HOPE

Participants: Carlos Gomez Cardenas, Ameni Khecharem, Robert de Simone.

This project was only recently started, with a kick-off meeting in November. Original proponents were UMR LEAT, Texas Instruments, Synopsys, Docea Power, Magillem, and ourselves. It seems that, due to internal reorganisation, TI might withdraw from the project. Other major semiconductor industrial partners in PACA are being approched for replacement (mainly Intel). The purpose of the HOPE project is to focus on high-level modeling and early estimation of hierarchical power management techniques, with potential synthesis in the end if feasible.

8.2.1.4. GeMoC

Participants: Matias Vara Larsen, Julien deAntoni, Frédéric Mallet.

This project was only recently started, with a kick-off meeting in December. It is admistratively handled by CNRS for our joint team, on the UMR I3S side. Partners are Inria (Triskell EPI), ENSTA-Bretagne, IRIT, Obeo, Thales TRT.
The project focuses on the modeling of heterogeneous systems using Models of Computation and Communication for embedded and real-time systems, described using generic means of MDE techniques (and in our case the MARTE profile, and most specifically its Time Model, which allows to specify precise timely constraints for operational semantic definition).

8.2.2. FUI

8.2.2.1. FUI P

Participants: Abderraouf Benyahia, Dumitru Potop Butucaru, Yves Sorel.

The goal of project P is to support the model-driven engineering of high-integrity embedded real-time systems by providing an open code generation framework able to verify the semantic consistency of systems described using safe subsets of heterogeneous modeling languages, then to generate optimized source code for multiple programming (Ada, C/C++) and synthesis (VHDL, SystemC) languages, and finally to support a multi-domain (avionics, space, and automotive) certification process by providing open qualification material. Modeling languages range from behavioural to architectural languages and present a synchronous and asynchronous semantics (Simulink/Matlab, Scicos, Xcos, SysML, MARTE, UML),
See also: http://www.open-do.org/projects/p/
Partners of the project are: industrial partners (Airbus, Astrium, Continental, Rockwell Collins, Safran, Thales), SMEs (AdaCore, Altair, Scilab Enterprise, STI), service companies (ACG, Aboard Engineering, Atos Origins) and research centers (CNRS, ENPC, Inria, ONERA).

8.2.2.2. FUI PARSEC

Participants: Dumitru Potop Butucaru, Thomas Carle, Zhen Zhang, Yves Sorel.

The PARSEC Project aims at providing development tools for critical real-time distributed systems requiring certification according to the most stringent standards such as DO-178B (avionics), IEC 61508 (transportation) or Common Criteria for Information Technology Security Evaluation. The approach proposed by PARSEC provides an integrated toolset that helps software engineers to meet the requirements associated to the certification of critical embedded software. Partners of the project are: Alstom, Thales, Ellidiss, OpenWide, Systerel, CEA, InriaS, Telecom ParisTech.
See also: http://www.systematic-paris-region.org/sites/default/files/exports/projets/fichiers/ProjetPARSEC_BookSystematic2012.pdf.

8.3. European Initiatives

8.3.1. ARTEMIS Projects

8.3.1.1. CESAR

Participant: Robert de Simone.

Title: CESAR

Duration: February 2009 - June 2012

Coordinator: AVL - GmbH (Austria)

Others partners: AIRBUS Operations GbmH (Germany), AIRBUS Operations SAS (France), ABB AS (Norway), ABB AB (Sweden), AbsInt Angewandte Informatik GmbH (Germany), ACCIONA Infraestructuras S.A. (Spain), Ansaldo STS S.p.A. (Italy), ASTRIUM SAS (France), AIRBUS Operations Limited (United Kingdom), Aristotle University of Thessaloniki (Greece), Commissariat à l´Energie Atomique et aux Energies Alternatives (France), CNRS (France), Centro Ricerche Fiat S.C.p.A. (Italy), Critical Software S.A. (Poland), Danieli Automation S.p.A. (Italy), Delphi France SAS (France), Deutsches Zentrum für Luft- und Raumfahrt e.V. (Germany), Dassault Systemes (France), EADS Deutschland GmbH (Germany), Fondacion Tecnalia Research & Innovation (Italy), ESTEREL Technologies SA (France), Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V. (Germany)

See also: http://www.cesarproject.eu/

Abstract: CESAR stands for Cost-efficient methods and processes for safety relevant embedded systems and is a European funded project from ARTEMIS JOINT UNDERTAKING (JU). The three transportation domains automotive, aerospace, and rail, as well as the automation domain share the need to develop ultra-reliable embedded systems to meet societal demands for increased mobility and ensuring safety in a highly competitive global market. To maintain the European leading edge position in the transportation as well as automation market, CESAR aims to boost cost efficiency of embedded systems development and safety and certification processes by an order of magnitude. CESAR pursuits a multi-domain approach integrating large enterprises, suppliers, SME's and vendors of cross sectoral domains and cooperating with leading research organizations and innovative SME's.
Upon completion, CESAR was awarded an ARTEMIS honorary mention for achievement.

8.3.1.2. PRESTO

Participants: Frédéric Mallet, Arda Goknil, Julien Deantoni, Marie-Agnès Peraldi Frati, Robert de Simone.

Title: PRESTO

Duration: April 2011 - March 2014

Coordinator: Miltech (Greece)

Others partners: TELETEL S.A. (Greece), THALES Communications (France), Rapita Systems Ltd. (United Kingdom), VTT (Finland), Softeam (France), THALES (Italy), MetaCase (Finland), Inria (France), University of LâAquila (Italy), MILTECH HELLAS S.A (Greece), PragmaDev (France), Prismtech (United Kingdom), Sarokal Solutions (Finland).

See also: http://www.cesarproject.eu/

Abstract: The PRESTO project aims at improving test-based embedded systems development and validation, while considering the constraints of industrial development processes. This project is based on the integration of test traces exploitation, along with platform models and design space exploration techniques. Such traces are obtained by execution of test patterns, during the software integration design phase, meant to validate system requirements. The expected result of the project is to establish functional and performance analysis and platform optimisation at early stage of the design development. The approach of PRESTO is to model the software/hardware allocation, by the use of modelling frameworks, such as the UML profile for model-driven development of Real Time and Embedded Systems (MARTE). The analysis tools, among them timing analysis including Worst Case Execution Time (WCET) analysis, scheduling analysis and possibly more abstract system-level timing analysis techniques will receive as inputs on the one hand information from the performance modelling of the HW/SW-platform, and on the other hand behavioural information of the software design from tests results of the integration test execution.

8.3.2. Collaborations in European Programs, except FP7

8.3.2.1. ITEA2 Timmo2Use

Participants: Marie-Agnès Peraldi Frati, Julien DeAntoni, Arda Goknil, Jean-Vivien Millo, Yves Sorel.

Program: ITEA2

Project acronym: Timmo2Use

Project title: TIMing MOdel, TOols, algorithms, languages, methodology, and USE cases

Duration: October 2010 - October 2012

Coordinator: Volvo Technology AB (Sweden)

Other partners: AbsInt Angewandte Informatik GmbH (Germany), Arcticus Systems AB (Sweden), Chalmers University of Technology (Sweden), Continental Automotive GmbH (Germany), Delphi France SAS (France), dSPACE GmbH (Germany), INCHRON GmbH (Germany), Institut National de Recherche en Informatique et Automatique (France), Mälardalen University (Sweden), Rapita Systems Ltd. (United Kingdom), RealTime-at-Work (France), Robert Bosch GmbH (Germany), Symtavision GmbH (Germany), Technische Universität Braunschweig (Germany), Time Critical Networks (Sweden), Universität Paderborn (Germany).

See also: http://timmo-2-use.org/

Abstract: TIMMO develops different types of timing constraints and dynamic behaviour formalisms, to be used inside the supply chain and the complex development process in distributed real-time automotive system design. TIMMO-2-USE stands for TIMing MOdel - TOols, algorithms, languages, methodology, and USE cases which summarizes the main objectives of the project, i.e., the development of novel tools, algorithms, languages, and a methodology validated by use cases.

The project provides partial funding for the postdoctoral positions of Jean-Vivien Millo and Arda Goknil.

8.3.2.2. ITEA2 OPENPROD

Participants: Simon Nivault, Yves Sorel.

Program: ITEA2

Project acronym: OpenProd

Project title: Open Model-Driven Whole-Product Development and Simulation Environment

Duration: June 2009 - May 2012

Coordinator: Siemens Industrial TurboMachinery AB (Sweden)

Other partners: Appedge (France), Bosch Rexroth AG (Sweden), CEA LIST (France), EADS Innovation Works (France), Electricité De France (France), Equa Simulation AB (Sweden), ETH Zürich (Switzerland), Fachhochschule Bielefeld (Germany), Fraunhofer FIRST (Germany), IFP (France), Inria Rocquencourt (France), INSA Lyon (France), Linköping University (Sweden), LMS Imagine (France), MathCore Engineering AB (Sweden), Metso Automation (France), Nokia (Finland), Plexim GmbH (Germany), Pöyry Forest Industry (Finland), PSA Peugeot Citroen (France), Siemens AG, Sector Energy (Germany), SKF Sverige AB (Sweden), Technische Universität Braunschweig (Germany), TLK Thermo GmbH (Germany), VTT Technical Research Centre (Finland), XRG Simulation GmbH (Germany).

See also: http://www.ida.liu.se/~pelab/OpenProd/

Abstract: The OPENPROD project is developing an open whole-product, model-driven systems development, modelling and simulation (M&S) environment that integrates the leading open industrial software development platform Eclipse with open-source modelling and simulation tools such as OpenModelica and industrial M&S tools and applications. The project will enable a more formalised validation of production to cut time to market and ensure higher quality, using open solutions which will have a high impact, based on easy uptake and wide dissemination.

8.4. International Initiatives

8.4.1. Inria Associated Teams

8.4.1.1. DAESD

Title: Distributed/Asynchronous and Embedded/synchronous Systems Development

Inria principal investigator: Robert de Simone

International Partner (Institution - Laboratory - Researcher):

East China Normal University (China) - SEI-Shone - Yixiang Chen

Duration: 2012 - 2014

See also: https://team.inria.fr/DAESD/

The development of concurrent and parallel systems has traditionally been clearly split in two different families: distributed and asynchronous systems on one hand, now growing very fast with the recent progress of the Internet towards large scale services and clouds; embedded, reactive, or hybrid systems on the other hand, mostly of synchronous behaviour. The frontier between these families has attracted less attention, but recent trends, e.g. in industrial systems, in *Cyber-Physical systems*, or in the emerging *Internet of Things*, give a new importance to research combining them. The aim of the DAESD associate team is to combine the expertise of the Oasis and Aoste teams at Inria, the SEI-Shone team at ECNU-Shanghai, and to build models, methods, and prototype software tools inheriting from synchronous and asynchronous models. We plan to address modelling formalisms and tools, for this combined model; to establish a method to analyze temporal and spatial consistency of embedded distributed real-time systems; to develop scheduling strategies for multiple tasks in embedded and distributed systems with mixed constraints. In parallel with our research collaboration this Associate Team, the SEI-Shone lab is organizing a workshop in Shanghai, with a first edition in Nov. 2011, on "Distributed - Asynchronous and Embedded - synchronous Systems Development".

8.4.2. Participation In International Programs

8.4.2.1. LIAMA

Following the DAESD associated-team, a proposal for a LIAMA project with ECNU Shanghai, named HADES, has been presented recently at the LIAMA steering committee in December 2012. It is a joint proposal with the OASIS EPI.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Jagadish Suryadevara (IDT, Mälardalen University, Sweden) visited us for two months in May/June 2012.

8.5.1.1. Internships

Matias Ezequiel VARA LARSEN (from Mar 2012 until Jun 2012)

Subject: Study of the influence of Linux operating system on OpenMP applications performances on multicore processors

Institution: National University of La Plata (Argentina)

CONVECS Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FSN (Fonds National pour la Société Numérique)

8.1.1.1. OpenCloudware

Participants: Rim Abid, Hugues Evrard, Frédéric Lang, Gwen Salaün [correspondent], Lina Ye.

OpenCloudware (see http://www.opencloudware.org) is a project funded by the FSN. The project is led by France Telecom / Orange Labs (Meylan, France) and involves 18 partners, among which Bull, OW2, Thalès, Inria, etc. OpenCloudware aims at providing an open software platform enabling the development, deployment and administration of cloud applications. The objective is to provide a set of integrated software components for (i) modeling distributed applications to be executed on cloud computing infrastructures, (ii) developing and constructing multi-tier virtualized applications, and (iii) deploying and administrating these applications (PaaS platform) possibly on multi-IaaS infrastructures.

OpenCloudware started in January 2012 for three years and nine months. The main contributions of CONVECS to OpenCloudware are the formal specification of the models, architectures, and protocols (self-deployment, self-management, etc.) underlying the OpenCloudware platform, the automated generation of code from these specifications for rapid prototyping purposes, and the formal verification of the aforementioned protocols.

8.1.1.2. Connexion

Participants: Hubert Garavel [correspondent], Frédéric Lang, Raquel Oliveira.

Connexion (*COntrôle commande Nucléaire Numérique pour l'EXport et la rénovatION*) is a project funded by the FSN within the second call for projects "*Investissements d'Avenir — Briques génériques du logiciel embarqué*". The project (see http://www.cluster-connexion.fr), led by EDF and supported by the *Pôles de compétitivité* Minalogic, Systematic, and *Pôle Nucléaire Bourgogne*, involves many industrial and academic partners, namely All4Tech, Alstom Power, ArevA, Atos Worldgrid, CEA, CNRS/CRAN, Corys Tess, ENS Cachan, Esterel Technologies, Inria, LIG, Predict, and Rolls-Royce. Connexion aims at proposing and validating an innovative architecture dedicated to the design and implementation of control systems for new nuclear power plants in France and abroad.

Connexion started in April 2012 for four years. CONVECS will participate, in cooperation with the IIHM team of LIG, to study the application of CADP to specify and validate human-machine interfaces formally.

8.1.2. Competitivity Clusters

8.1.2.1. Bluesky for I-Automation

Participants: Hubert Garavel, Fatma Jebali, Jingyan Jourdan-Lu, Frédéric Lang, Eric Léo, Radu Mateescu [correspondent].

Bluesky for I-Automation is a project funded by the FUI (*Fonds Unique Interministériel*) within the *Pôle de Compétitivité* Minalogic. The project, led by Crouzet Automatismes (Valence), involves the SMEs (*Small and Medium Enterprises*) Mootwin and VerticalM2M, the LCIS laboratory of Grenoble INP, and CONVECS. Bluesky aims at bringing closer the design of automation applications and the Internet of things by providing an integrated solution consisting of hardware, software, and services enabling a distributed, Internet-based design and development of automation systems. The automation systems targeted by the project are networks of programmable logic controllers, which belong to the class of GALS (*Globally Asynchronous, Locally Synchronous*) systems.

Bluesky started in September 2012 for three years. The main contributions of CONVECS to Bluesky are the definition of the formal pivot language for describing the asynchronous behaviour of logic controller networks and the automated verification of the behaviour using compositional model checking and equivalence checking techniques.

8.1.3. Other National Collaborations

Additionally, we collaborated in 2012 with the following Inria project-teams:

- CONTRAINTES (Inria Paris-Rocquencourt): Grégory Batt,
- OASIS (Inria Sophia-Antipolis – Méditerranée): Eric Madelaine and Ludovic Henrio.

Beyond Inria, we had sustained scientific relations with the following researchers:

- Gaëlle Calvary and Sophie Dupuy-Chessa (LIG, Grenoble),
- Pascal Poizat (LIP6, Paris),
- Meriem Ouederni (IRIT, Toulouse),
- Dimitris Vekris (LACL, Paris-Est Créteil).

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. Sensation

Participants: Hubert Garavel, Radu Mateescu, Wendelin Serwe.

Sensation (*Self ENergy-Supporting Autonomous computaTION*) is the European project no. 318490 funded by the FP7-ICT-11-8 programme. The project (see http://people.cs.aau.dk/~rrh/SENSATION) gathers 9 participants: Inria (Triskell and Convecs teams), Aalborg University (Denmark), RWTH Aachen and Saarland University (Germany), University of Twente and Embedded System Institute (The Netherlands), STMicroelectronics (France), GomSpace (Denmark), and Recore Systems (The Netherlands). The main goal of Sensation is to increase the scale of systems that are self-supporting by balancing energy harvesting and consumption up to the level of complete products. In order to build such Energy Centric Systems, embedded system designers face the quest for optimal performance within acceptable reliability and tight energy bounds. Programming systems that reconfigure themselves in view of changing tasks, resources, errors and available energy is a demanding challenge.

Sensation started on October 1st, 2012 for three years. CONVECS contributes to the project regarding the extension of formal languages with quantitative aspects, studying common semantic models for quantitative analysis, and applying formal modeling and analysis to the case studies provided by the industrial partners.

8.2.2. Collaborations with Major European Organizations

The CONVECS team is member of the FMICS (*Formal Methods for Industrial Critical Systems*) working group of ERCIM (see http://fmics.inria.fr). R. Mateescu is currently the chairman of the FMICS working group and H. Garavel is member of the FMICS board, in charge of dissemination actions.

Hubert Garavel was appointed to a new Working Group within Informatics Europe: “Parallel Computing (Supercomputing) Education in Europe: State-of-Art”. This is a relatively small working group (about 10 people) with the following missions: to show the need for urgent changes in higher education in the area of computational sciences, to compose a survey of the current landscape of parallel computing and supercomputing education in Europe with respect to different universities and countries, and to prepare a set of recommendations on how to bring ideas of parallel computing and supercomputing into higher educational systems of European countries.

8.2.3. Other European Collaborations

In addition to our partners in aforementioned contractual collaborations, in 2012 we had scientific relations with several European universities and research centers, including:

- Saarland University (Alexander Graf-Brill, Ernst-Moritz Hahn, Arnd Hartmanns, Holger Hermanns, and Andrea Turrini),
- Oxford University (Ernst-Moritz Hahn, Marta Kwiatkowska, and Dave Parker),
- RWTH Aachen (Joost-Pieter Katoen and Viet Yen Nguyen),
- University of Twente (Freark van der Berg and Marielle Stoelinga),
- Technical University of Eindhoven (Anton Wijs).

H. Garavel participates in the DFG (*Deutsche Forschungsgemeinshaft*) transregional project AVACS (*Automatic Verification and Analysis of Complex Systems*, see http://www.avacs.org) and he attended two meetings held at Freiburg (Germany) in February 2012 and at Mannheim (Germany) in November 2012.

8.3. International Initiatives

H. Garavel is a member of IFIP (*International Federation for Information Processing*) Technical Committee 1 (*Foundations of Computer Science*) Working Group 1.8 on Concurrency Theory chaired successively by Luca Aceto and Jos Baeten.

8.3.1. Other International Collaborations

We had sustained scientific relations with Tevfik Bultan (University of California at Santa Barbara, USA).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Pascal Poizat (LIP6, University Pierre et Marie Curie, Paris) visited us on March 26–27, 2012.
- Dimitris Vekris (LACL, University Paris-Est Créteil) visited us from April 23 to May 11, 2012.
- Meriem Ouederni (IRIT, Toulouse) visited us on June 4–15, 2012.
- The annual CONVECS seminar was held in Pont-en-Royans (France) on November 5–7, 2012. The following invited scientists attended the seminar:
  - Jérémy Buisson (University of Bretagne-Sud / VALORIA and Ecoles de St-Cyr Coëtquidan) gave on November 5, 2012 a talk entitled "*Vers un futur pi-ADL reconfigurable*".
  - Sophie Dupuy-Chessa (LIG, Grenoble) gave on November 6, 2012 a talk entitled "*Qualité des interfaces homme-machine plastiques*".
  - Massimo Zendri (STMicroelectronics) gave on November 6, 2012 a talk entitled "*Circuit Level Formal Verification in Industrial Environment*".

DART Project-Team

8. Partnerships and Cooperations

8.1. European Initiatives

8.1.1. Collaboration with Romania

We collaborate with the University of Laşi (Romania) on formal techniques for general and domain specific languages.

8.1.2. Collaboration with the Netherlands

We collaborate with the Eindhoven University of Technology (The Netherlands) on formal techniques for general and domain specific languages.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

Tim Willemse

Subject: visit to explore future collaborations.

Institution: Eindhoven University of Technology, NL

Duration: 1 week

Frank Stappers

Subject: formal verification for reconfigurable languages

Institution: Eindhoven University of Technology, NL

Duration: 6 weeks

8.2.1.1. Internships

Bram Gerron

Subject: formal verification of compilation

Institution: Eindhoven University of Technology, NL

Duration: 3 months

ESPRESSO Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

Program: ANR

Project acronym: VeriSync

Project title: Vérification formelle d'un générateur de code pour un langage synchrone

Duration: Nov. 2010 - Oct. 2013

Coordinator: IRIT

Other partners: IRIT

URL: http://www.irit.fr/Verisync/

Abstract:

The VeriSync project aims at improving the safety and reliability assessment of code produced for embedded software using synchronous programming environments developed under the paradigm of Model Driven Engineering. This is achieved by formally proving the correctness of essential transformations that a source model undergoes during its compilation into executable code.

Our contribution to VeriSync consists of revisiting the seminal work of Pnueli et al. on translation validation and equip the Polychrony environment with updated verification techniques to scale it to possibly large, sequential or distributed, C programs generated from the Signal compiler. Our study covers the definition of simulation and bisimulation equivalence relations capable of assessing the correspondence between a source Signal specification and the sequential or concurrent code generated from it, as well as both specific abstract model-checking techniques allowing to accelerate verification and counter-example search techniques, to filter spurious verification failures obtained from excessive abstracted exploration.

7.1.2. Competitivity Clusters

Program: FUI

Project acronym: P

Project title: Project P

Duration: March 2011 - Feb. 2014

Coordinator: Continental Automotive France

Other partners: 19 partners (Airbus, Astrium, Rockwell Collins, Safran, Thales Alenia Space, Thales Avionics...)

URL: http://www.open-do.org/projects/p/

Abstract:

The aim of project P is 1/ to aid industrials to deploy model-driven engineering technology for the development of safety-critical embedded applications, 2/ to contribute on initiatives such as OPEES and CESAR to develop support for tools inter-operability and 3/ to provide state-of-the-art automated code generation techniques from multiple, heterogeneous, system-levels models. The focus of project P is the development of a code generation toolchain starting from domain-specific modeling languages for embedded software design and to deliver the outcome of this development

as an open-source distribution, in the aim of gaining an impact similar to GCC for general-purpose programming, as well as a kit to aid with the qualification of that code generation toolchain.

The contribution of project-team ESPRESSO in project P is to bring the necessary open-source technology of the Polychrony environment to allow for the synthesis of symbolic schedulers for software architectures modeled with P in a manner ensuring global asynchronous deterministic execution.

The current activities in the project consist in gathering and writing detailed documentation about the project context, requirements and constraints. We are now familiar with the technologies involved in the project and started refining high-level requirements so as to to express technical objectives and solutions. The P formalism is still in the process of being defined and some aspects of the language are unknown (namely the sofwtare architecture formalism). For the subset of P that is sufficiently known and stable, we are investigating the semantical mapping between P and Signal with respect to controller synthesis.

7.1.3. CORAC

Program: CORAC

Project acronym: CORAIL

Project title: Composants pour l'Avionique Modulaire Étendue

Duration: Sep. 2011 - Dec. 2016

Coordinator: Thales Avionics

Other partners: Airbus, Dassault Aviation, Eurocopter, Sagem...

URL: http://www.corac-ame.com/

Abstract:

The CORAIL project aims at defining components for Extended Modular Avionics. The contribution of project-team ESPRESSO is to define a specification method and to provide a generator of multi-task applications.

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

Program: ARTEMIS

Project acronym: CESAR

Project title: Cost-efficient methods and processes for safety relevant embedded systems

Duration: March 2009 - June 2012

Coordinator: AVL List GmbH

Other partners: 59 project partners (main partners for us: AIRBUS, IRIT (CNRS)...)

URL: http://www.cesarproject.eu/

Abstract:

In the context of CESAR, we have participated to the sub-project 3 demonstrator in order to demonstrate the usability of Polychrony as a co-simulation tool within the reference technology platform of the project, to which its open-source release has been integrated. The case-study, implemented in collaborateion with Airbus and IRIT, consists of co-modeling the doors management system of an Airbus A350 by merging its architecture description, specified with AADL, with its behavioral description, specified with Simulink.

In this case-study, we demonstrate that the Polychrony toolset can effectively serve as a modeling infrastructure to compositionally assemble, compile and verify heterogeneous specifications (AADL and Simulink). Our case study covers code generation for real-time simulation and test as well as

formal verification both at system-level and in a GALS framework. Based on that case study, we are developing further modular code-generation services, real-time simulation, test and performance evaluation, formal verification as well as the validation of the generated concurrent and distributed code.

Program: ITEA2

Project acronym: OPEES

Project title: Open Platform for the Engineering of Embedded Systems

Duration: Feb. 2009 - Dec. 2012

Coordinator: Obeo

Other partners: 30 partners (main partners for us: Airbus, CS Communication & Systèmes, INDRA (Spain), INPT/IRIT...)

URL: http://www.opees.org/

Abstract: The ITEA2 project OPEES is the continuation of the ANR project OPENEMBEDD to provide an open-source platform for embedded software design. Its outcome will outlive the duration of the project as it has given rise to an Industrial Working Group of the Eclipse consortium, Polarsys, whose goal is to host and maintain the proposed open-source platform and guarantee its long-term availability.

The mission of OPEES is to build a community able to ensure durability of innovative engineering technologies in the domain of critical software-intensive embedded systems. Its main objectives are to secure the industrial strategy, improve their competitiveness and develop the European software industry.

Our goal in the OPEES project was to deliver the Polychrony toolset on the Polarsys platform as an infrastructure for the co-simulation and co-verification of embedded architectures. To this end, Polychrony has been under a quality assessment process performed in collaboration with CS.

7.3. International Initiatives

7.3.1. Inria Associate Teams

7.3.1.1. POLYCORE

Title: Polychronous models

Inria principal investigator: Jean-Pierre Talpin

International Partner (Institution - Laboratory - Researcher):

Virginia Tech (United States) - Fermat Laboratory - Sandeep Shukla

Duration: 2011 - 2013

See also: http://www.irisa.fr/espresso/Polycore

Inria Associate Project POLYCORE starts from an observation that can be shared with anyone how experienced with multi-threaded programming, to acknowledge the difficulty of designing and implementing such software. Resolving concurrency, synchronization, and coordination issues, and tackling the non-determinism germane in multi-threaded software is extremely difficult. Ensuring correctness with respect to the specification and deterministic behavior is however necessary for safe execution of such code on embedded architectures. It is therefore desirable to synthesize multi-threaded code from formal specifications using a provably ‘correct-by-construction’ approach.

While time-triggered programming model simplifies code generation, our shared intuition is that multi-rate event driven execution models are much more efficiently adapted to tackle embedded software design challenges posed by forthcoming heterogeneous multi-core embedded architectures. To this aim, we develop formal models, methods, algorithms and techniques for generating provably correct multi-threaded reactive real-time embedded software for mission-critical applications. For

scalable modeling of larger embedded software systems, the specification formalism has to be compositional and hierarchical.

Our proposed formalism entails a model of computation (MoC) based on a multi-rate synchronous data-flow paradigm: Polychrony. It aims at combining the capabilities of Esterel/Quartz (ESG/TUKL) for correctly programming synchronous modules, with the capabilities of Polychrony (Inria), to give high-level abstractions of complex multi-clocked networks and yet provide powerful communication and scheduling code synthesis, all combined in an application-specific modeling and programming environment, design in collaboration with Virginia Tech and the AFRL [12], [11]. This year, we laid novel semantical foundations to designing our envisioned environment by defining a constructive semantic encompassing the polychronous data-flow model of Signal and the reactive synchronous imperative model of Quartz, and allowing to formulate the very first executable, small-step, structured operational semantics of Signal [17].

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Pr. John Koo (SIAT, Shenzhen) visited ESPRESSO in summer 2012 with the support of the University of Rennes 1. During his stay, we elaborated a collaboration plan and project proposal on integrated discrete/continuous/hardware simulation with LIAMA.

In the context of the associate project Polycore, Jens Brandt (TU Kaiserslautern) visited ESPRESSO in June to share code generation techniques in Quartz and Signal. Loïc Besnard visited Virginia Tech in June to present the open-source release of Polychrony and explore possibles uses of Polychrony in the MRCDIF environment developed at the FLVT. Jean-Pierre Talpin visited Virginia Tech in May and October to prepare our work on Quartz and Signal and jointly draft a project proposal for the USAFRL.

7.4.2. Visits to International Teams

Jean-Pierre Talpin received a grant as invited scientist by the Chinese Academy of Science to visit the Shenzhen Institute for Advanced Technology in December 2012 and further ongoing collaborations with Pr. Koo and LIAMA.

MUTANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. INEDIT

Title: Interactivity in the Authoring of Time and Interactions

Project acronym: INEDIT

Type: ANR Contenu et Interaction 2012 (CONTINT)

Instrument: ANR Grant

Duration: September 2012 - September 2015

Coordinator: IRCAM (France)

Other partners: Grame (Lyon, France), LaBRI (Bordeaux, France).

Abstract: The INEDIT project aims to provide a scientific view of the interoperability between common tools for music and audio productions, in order to open new creative dimensions coupling *authoring of time* and *authoring of interaction*. This coupling allows the development of novel dimensions in interacting with new media. Our approach lies within a formal language paradigm: An interactive piece can be seen as a virtual interpreter articulating locally synchronous temporal flows (audio signals) within globally asynchronous event sequence (discrete timed actions in interactive composition). Process evaluation is then to respond reactively to signals and events from an environment with heterogeneous actions coordinated in time and space by the interpreter. This coordination is specified by the composer who should be able to express and visualize time constraints and complex interactive scenarios between mediums. To achieve this, the project focuses on the development of novel technologies: dedicated multimedia schedulers, runtime compilation, innovative visualization and tangible interfaces based on augmented paper, allowing the specification and realtime control of authored processes. Among posed scientific challenges within the INEDIT project is the formalization of temporal relations within a musical context, and in particular the development of a GALS (Globally Asynchronous, Locally Synchronous) approach to computing that would bridge in the gap between synchronous and asynchronous constraints with multiple scales of time, a common challenge to existing multimedia frameworks.

7.1.2. Other National Initiatives

The team participated to the CLASYCO network on DSL for simulation, supported by the RNSC (réseau national des systèmes complexes).

Jean-Louis Giavitto participates to the SynBioTIC ANR Blanc project (with IBISC, University of Evry, LAC University of Paris-Est, ISC - Ecole Polytechnique).

7.2. International Research Visitors

7.2.1. Visits of International Scientists

Miller S. Puckette is a professor of computer music in University of California San Diego (UCSD) and author of *Max* and *PureData* real-time programming environments for interactive arts. He participated in May 2012 in the MuTant Real-time Multimedia Computing Seminars (available on the web) and contributed to the team's knowledge of multimedia real-time scheduling challenges and paradigms.

James McCartney is a senior researcher in Apple Core Audio project and author of the audio synthesis and algorithmic composition programming environment *SuperCollider*. He visited *MUTANT* in November 2012 and participated in the MuTant Real-time Multimedia Computing Seminars (available on the web). He is interested in robust scheduling of heterogeneous computing for real-time multimedia applications.

David Rizo is lecturer at the University of Alicante, Spain. He is interested in music information retrieval and classification of musical genres by combining audio and symbolic descriptors. He visited *MuTant* in March 2012 and participated in a session of the MaMux seminar dedicated to trees and hierarchical structures in computer music.

Masahiko Sakai is a professor at the University of Nagoya and director of the Sakabe/Sakai computer science laboratory of the department of computer science and mathematical informatics of Nagoya University. He visited *MuTant* in April 2012.

Yoshiharu Kojima is an research fellow of the Japan society for the promotion of science. He has made a two months post-doctoral visit in *MuTant* in October and November 2012 on the application of term rewriting techniques to the formalization of musical processes, under the institutional program for young researchers overseas visits of the graduate school of information science at Nagoya University.

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

ANR WMC project (program “jeunes chercheuses, jeunes chercheurs”), 2012–2016, 200 Keuros. F. Zappa Nardelli is the main investigator.

ANR Boole project (program “action blanche”), 2009-2014.

ANR Partout (program “defis”), 2009-2012.

ANR CAFEIN, 2013-2015.

Action d’envergure Synchronics, 2008-2012. The action was driven by Alain Girault (Inria, PopArt, Grenoble) and Marc Pouzet (Inria, Parkas, Paris-Rocquencourt), to focus on “langages for embedded systems”. This has been instrumental in driving our new research on hybrid system modelers.

8.1.2. Competitivity Clusters

FUI project OpenGPU, 2008–2012.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

September, 27 - October, 3, Peter Sewell (U. Cambridge) visited the Parkas team for collaboration with F. Zappa Nardelli and R. Morisset.

October, 6-13, Mike Hicks (U. Maryland) visited the Département d’informatique of the ENS.

January, 18-20, P. Sadayappan (Ohio State U.) visited the team to work with Tobias Grosser and Sven Verdoolaege. Similar visits took place in July and December.

June-July 2013. Stephen Edwards (Columbia U.) was invited by ENS to spend a month in the team.

8.2.1.1. Internships

January-July, Pankaj Pawan (IIT Kanpur) was intern student (M2) under the supervision of F. Zappa Nardelli.

May-September, Robin Morisset (ENS Ulm) was intern student (M2) under the supervision of F. Zappa Nardelli.

May-September, Fran cois Gindraud (ENS Ulm) was intern student (M2) under the supervision of A. Cohen.

December 2011-November 2012, Mehdi Dogguy was post-doc funded by the ANR Partout grant. Mehdi Dogguy worked on the static analysis of ReactiveML programs and was supervised by L. Mandel.

April-July 2012, Cyprien Lecourt (École Polytechnique) was intern student (M1) under the supervision of M. Pouzet.

April-September 2012, Guillaume Baudart (École normale supérieure de Cachan) was intern student (M2) under the supervision of M. Pouzet. Guillaume was a student from IRCAM and the supervision was joint with Florent Jacquemart (Inria Paris-Rocquencourt and IRCAM).

8.2.2. Visits to International Teams

Louis Mandel spent 7 weeks in the team of Vijay Saraswat at IBM T.J. Watson. He worked on the type system of the X10 language.

Albert Cohen and Tobias Grosser visited Prof. Uday Bondhugula at the Indian Institute of Science (IISc), CSA department, for 4 days and 2 weeks, respectively. Tobias Grosser gave a lecture/tutorial on optimizing compilation in LLVM to IISc students and AMD engineers.

POP ART Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Inria Large Scale Actions

8.1.1.1. Inria Large Scale Action Synchronics: Language Platform for Embedded System Design

Participants: Gwenaël Delaval, Alain Girault [contact person, co-coordinator], Bertrand Jeannet, Xavier Nicollin, Peter Schrammel.

The SYNCHRONICS (Language Platform for Embedded System Design) project [mid-2008 to mid-2012] gathers 9 permanent researchers on the topic of embedded systems design: B. Caillaud (INRIA Rennes – Bretagne Atlantique), A. Cohen, L. Mandel, and M. Pouzet (Inria-Saclay and ENS Paris), G. Delaval, A. Girault, and B. Jeannet (INRIA Grenoble – Rhône-Alpes), E. Jahier and P. Raymond (VERIMAG).

SYNCHRONICS capitalizes on recent extensions of data-flow synchronous languages, as well as relaxed forms of synchronous composition or compilation techniques for various platform, to address two main challenges with a language-centered approach: (i) the co-simulation of mixed discrete-continuous specifications, and more generally the co-simulation of programs and properties (either discrete or continuous); (ii) the ability, inside the programming model, to account for the architecture constraints (execution time, memory footprint, energy, power, reliability, etc.).

8.1.2. ANR

8.1.2.1. ANR Asopt: Analyse Statique et OPTimisation

Participants: Bertrand Jeannet [contact person, coordinator], Peter Schrammel.

The ASOPT (Analyse Statique et OPTimisation) project [january 2009-july 2012] [35] brings together static analysis (Inria-POP ART, VERIMAG, CEA LMeASI), optimisation, and control/game theory experts (CEA LMeASI, Inria-MAXPLUS) around some program verification problems. POP ART is the project coordinator.

Many abstract interpretations attempt to find "good" geometric shapes verifying certain constraints; this not only applies to purely numerical abstractions (for numerical program variables), but also to abstractions of data structures (arrays and more complex shapes). This problem can often be addressed by optimisation techniques, opening the possibility of exploiting advanced techniques from mathematical programming.

The purpose of ASOPT is to develop new abstract domains and new resolution techniques for embedded control programs, and in the longer run, for numerical simulation programs.

The main results are 1. improved *numerical abstract domains* (in particular the MaxPLus polyhedra and zonotopes-based abstract domains), and their combination with finite-types domains (using BDDs); 2. new *symbolic domains*, in particular for the accurate analysis of aliased expressions in data-structures and for precise interprocedural analysis in the presence of pointers to the call-stack; 3. improved *equation solving techniques*, with the generalization of the *policy iteration* approach and the widening of its applicability; 4. precise abstractions of full blocks of code, based either on quantifier elimination or on abstract acceleration.

Most of these contributions have been integrated into either the FIXPOINT library or the APRON/BDDAPRON libraries and they can be experimented on-line or off-line with the INTERPROC analyzer (see Section 5.5.5), which was the common experimental platform of the project.

8.1.2.2. ANR Vedecy: Verification and Design of Cyber-physical Systems

Participants: Gregor Goessler [contact person], Bertrand Jeannet, Sebti Mouelhi.

[35] http://asopt.inrialpes.fr/index.php

The VEDECY project brings together hybrid systems and formal methods experts. Three partners are involved: Laboratoire Jean Kuntzmann (LJK), Inria POP ART, and VERIMAG.

VEDECY aims at pursuing fundamental research towards the development of algorithmic approaches to the verification and design of cyber-physical systems. Cyber-physical systems result from the integration of computations with physical processes: embedded computers control physical processes which in return affect computations through feedback loops. They are ubiquitous in current technology and their impact on lives of citizens is meant to grow in the future (autonomous vehicles, robotic surgery, energy efficient buildings, ...).

Cyber-physical systems applications are often safety critical and therefore reliability is a major requirement. To provide assurance of reliability, model based approaches and formal methods are appealing. Models of cyber-physical systems are heterogeneous by nature: discrete dynamic systems for computations and continuous differential equations for physical processes. The theory of hybrid systems offers a sound modeling framework for cyber-physical systems. The purpose of VEDECY is to develop hybrid systems techniques for the verification and the design of cyber-physical systems.

8.2. International Initiatives

8.2.1. Inria Associate Teams

8.2.1.1. AFMES

Title: Advanced Formal Methods for Embedded Systems

Inria principal investigator: Alain Girault

International Partner (Institution - Laboratory - Researcher):

University of Auckland (New Zealand) - Department of Electrical and Computer Engineering

Duration: 2010 - 2012

See also: http://pop-art.inrialpes.fr/~girault/Projets/Afmes/

Embedded systems are characterized by several constraints, such as determinism and bounded reaction time. Accordingly, design methods for embedded systems should, when possible, guarantee these properties by construction. This allows the shifting of the burden of checking these constraints from the programmer to the design method and the associated compilers and code generation tools. In order to achieve this, our goal is to improve the existing design methods in several key directions: (1) Incremental converter synthesis. (2) Programming language for adaptive computing (SystemJ and beyond) [15]. (3) Time predictable programming language and execution architectures [10], [12]. Together, these advanced methods will provide a higher level of safety in the design of embedded systems.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- Aditya Zutshi, PhD student at the University of Colorado Boulder (USA), visited POP ART from July to August 2012 and worked on the abstract acceleration of general linear loops with inputs.
- Partha Roop, Senior Lecturer at the University of Auckland (New Zealand) visited POP ART in March 2012 to work on the AFMES associated team.
- Eugene Yip, PhD student at the University of Auckland (New Zealand) visited POP ART from October to December 2012 to work on the AFMES associated team.

8.3.2. Visits to International Teams

- Bertrand Jeannet and Peter Schrammel visited the University of Colorado Boulder (USA) in February 2012 from the 3th to the 21th.
- Alain Girault visited the University of Auckland (New Zealand) to work on the AFMES Associated Team.
- Alain Girault visited the University of California Berkeley (USA) in August 2012 to work on time predictable programming languages and on parametric dataflow models of computation.

S4 Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. Synchronics: Language Platform for Embedded System Design

Participants: Albert Benveniste, Benoît Caillaud.

Large scale initiative funded by INRIA. *http://synchronics.inria.fr/*

This project, started Jan 1st 2008, is supported by INRIA. It capitalizes on recent extensions of data-flow synchronous languages (mode automata, Lucid Synchrone, Signal, Lustre, ReactiveML, relaxed forms of synchronous composition or compilation techniques for various platforms). We aim to address the main challenges of embedded system design, starting from a single, semantically well founded programming language.

Our contributions to Synchronics in 2012 are:

- A journal paper [10] presenting the non-standard semantics for hybrid systems and its applications to the semantics and compilation of hybrid modeling languages. Details can be found in Section 6.2 .
- Inputs to the latest evolution of the Modelica language, related to state machines and a clock calculus.
- A study of modular code generation techniques for reactive synchronous programming languages, based on an interface theoretic approach [15], [26]. See 6.3 for further details.

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

Program: ITEA 2
Project acronym: MODRIO
Project title: Model driven Physical Systems Operation
Duration: Sep 2012 - Aug 2015
Coordinator: EDF (France)
Other partners:ABB (Sweden and Germany), AIT (Austria), Ampère - INSA Lyon and CNRS (France), Bielefeld university (Germany), Dassault Aviation (France), DLR (Germany), DPS (France), Dassault Systèmes (France), EADS (France), Enicon (Austria), Equa Simulation (Sweden), IFPEN (France), Ilmenau university (Germany), ITI (Germany), KUL (Belgium), Knorr-Bremse (Germany), Linköping university (Sweden), LMS Imagine (France and Belgium), MathCore Engineering (Sweden), Modelon AB (Sweden), Pöyry Finland Oy (Finland), QTronic (Germany), Scania (Sweden), Semantum Oy (Finland), Sherpa Engineering (France), Siemens AG (Germany), Siemens Industrial Turbomachinery AB (Sweden), Simpack AG (Germany), Supméca (France), Triphase (Belgium), University of Calabria (Italy), Vattenfall (Sweden), VTT (Finland), Wapice Ltd. (Finland).
Abstract: MODRIO seeks solutions to support adoption of model-based systems engineering in the design of mechatronic systems. The project covers all phases of the development cycle - from early concept design, over detailed system design, to verification and validation - and operational use including diagnostics during the entire system's life cycle.

7.3. International Initiatives

7.3.1. Participation In International Programs

Eric Badouel is contributing to the ALOCO research project of the LIRIMA, on component-based software architectures (http://www.lirima.uninet.cm/index.php/component/content/article?id=2).

7.4. International Research Visitors

7.4.1. Internships

Hela GOMRI (from Mar 2012 until Sep 2012)

Subject: Systèmes collaboratifs à l'aide de documents actifs.

Institution: Ecole Nationale d'Ingénieurs de Tunis (Tunisia)

TRIO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Open-PEOPLE - Open Power and Energy Optimization PLatform and Estimator

Participants: Fabrice Vergnaud, Jérôme Vatrinet, Kévin Roussel, Olivier Zendra.

Open-PEOPLE initially gathers 5 partners from academia and 2 from industry. This project aims at providing a federative and open platform for the estimation and optimization of power and energy consumption in computer systems. The platform users will be able to evaluate application consumption on a hardware architecture chosen among a set of provided typical, parametric architectures. In the considered system, the components will be picked from a library of hardware and software components, be they parametric or not. It will be possible to perform the estimation at various stages of the specification refinement, thanks to a methodology based on multi-level, interoperable and exchangeable consumption models allowing an easy exploration of the design space. Thus, estimations results may be used to check the energy behaviour of a system developed with simulation platforms. Feedback about the application functional properties will allow further refining of the estimation results in Open-PEOPLE. A standardisation of consumption models will be proposed in order to allow interoperability and have easier exchanges with other platforms. The Open-PEOPLE library of consumption models will be extensible: new component models will be added as the user applicative requirements evolve and as implementation techniques progress. To do so, the software estimation platform that will be accessible via an Internet portal shall be linked to a hardware platform made of an automated measurement testbench, which will be controllable from the software platform. A standalone version will also be provided to meet the confidentiality requirements of industry. A library of applications benchmarks will be proposed to characterize new components and new architectures. In addition to the research work required to build methods for multi-level estimation in heterogeneous complex systems, research work shall be carried on in order to offer new methods and techniques making it possible to optimize consumption thanks to the results provided by Open-PEOPLE. Open-PEOPLE is hence geared towards academia to support research work pertaining to consumption estimation and optimization methods, as well as towards industry to estimate or optimize the consumption of future products.

This project ended in late 2012, and we hope to continue work in this direction through other subsequent projects.

8.1.2. BGLE DEPARTS

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo.

The project DEPARTS started on October 1st for five next years. This project is funded by the national funding program BGLE. TRIO team will propose solutions for probabilistic component-based models.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. PROARTIS

Title: ___PROARTIS___
Type: COOPERATION (ICT)
Defi: Embedded Systems Design
Instrument: Specific Targeted Research Project (STREP)
Duration: February 2010 - July 2013
Coordinator: Barcelona Supercomputong Center (Spain)
See also: ___http://www.proartis-project.eu/___

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Luca Santinelli, Codé Lo, Dorin Maxim.

TRIO team participates to PROARTIS which is a STREP project within the FP7 call and it started on February 2010. It has six partners: Barcelona Supercomputing, University of York, University of Padova, Inria and Airbus. The overarching objective of the PROARTIS project is to facilitate a probabilistic approach to timing analysis. The proposed approach will concentrate on proving that pathological timing cases can only arise with negligible probability, instead of struggling to eradicate them, which is arguably not possible and could severely degrade performance. This will be a major turn from previous approaches that seek analyzability by trying to predict with cycle accuracy the state of hardware and software through analysis.

The PROARTIS project will facilitate the production of analysable CRTE systems on advanced hardware platforms with features such as memory hierarchies and multi core processors.

8.2.1.2. TIMMO-2-USE

Participants: Liliana Cucu-Grosjean, Aurélien Monot, Nicolas Navet, Françoise Simonot-Lion, Ammar Oulamara, Luca Santinelli, Dominique Bertrand, Cristian Maxim.

TRIO team participated to TIMMO-2-USE (http://timmo-2-use.org/) is an ITEA 2 European project. It started in November 2010 and ended in September 2012. TIMMO-2-USE addresses the specification, transition and exchange of different types of timing information throughout different steps of the development process. The general goal is to evaluate and enhance standards for different applications in the development by different technical use cases covering multiple abstraction levels and tools. For this, TIMMO-2-USE will bring the AUTOSAR standard, TADL and EAST-ADL2 into different applications like WCET analysis and in-the-loop scenarios. This will bring new algorithms and tools for the transition and conversion of timing information between different tools and abstraction level based on a new advanced methodology which, in turn, will be based on a combination of the TIMMO and the ATESST2 methodologies.

8.2.2. Collaborations in European Programs, except FP7

8.2.2.1. European Network of Excellence (NOE) High Performance Embedded Architectures and Compilation (HiPEAC)

Participant: Olivier Zendra.

The TRIO team is involved in the HiPEAC (High Performance Embedded Architecture and Compilation) European Network of Excellence (NoE). Olivier Zendra was initiator and leader in this context of a cluster of European Researchers “Architecture-aware compiler solutions for energy issues in embedded systems” from mid-2007 to mid-2009. A STREP proposal tentatively titled "RuSH2LEAP: Runtime Software-Hardware interactions to Lower Energy And Power"is currently being written, mostly in the context of this network of excellence, for submission in Call ICT 2013.10, challenge 3.4 Advanced computing, embedded and control systems.

8.2.3. Collaborations with Major European Organizations

Partner 1: University of York (U.K.)

Sujet 1: probabilistic and statistical analysis of real-time systems

Partner 2: Malardelan University (Sweden)

Sujet 2: statistical analysis of real-time systems

Partner 3: University of Edinburgh (U.K.)

Sujet 3: energy modeling and optimisation of computing systems

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- Rob Davis, University of York
- Marko Bertogna, University of Modena

8.3.2. Visits to International Teams

Luca Santinelli visited University of York and Rapita, York for one month in April 2012.

VERTECS Project-Team

7. Partnerships and Cooperations

7.1. National initiatives

7.1.1. ANR VACSIM: Validation of critical control-command systems by coupling simulation and formal analysis

Participants: Nathalie Bertrand, Thierry Jéron, Hervé Marchand.

The Vacsim project (2011-2014) is a 3-year project with EDF R&D, Dassault Systèmes, LURPA Cachan, I3S Nice and Labri Bordeaux. The project aims at developping both methodological and formal contributions for the simulation and validation of control-command systems. The role of the Vertecs team will be to contribute to the advance of validation techniques for timed systems, including quantitative analysis and its application to testing, monitoring of timed systems, and verification of communicating timed automata. The VACSIM project funds the PhD thesis of Srinivas Pinisetty.

7.1.2. ANR Ctrl-Green (Autonomic management of green data centers)

Participant: Hervé Marchand.

The project Ctrl-Green (2011-2014) is a 3-year project with UJF/LIG, INPT/IRIT, Inria, EOLAS, Scalagent. This project aims at developing techniques for the automatic optimal management of reconfigurable systems in the context of data centers using discrete controller synthesis methodology applied in the synchronous paradigm. The role of the Vertecs team will be to contribute to the development of new controller synthesis methodology for symbolic synchronous systems handling variables and to its application to the autonomic management of data centers.

7.2. European Initiatives

7.2.1. Artist design network of excellence

Participants: Nathalie Bertrand, Thierry Jéron, Hervé Marchand.

Program: FP7

Project acronym: Artist Design

Project title: Artist - European Network of Excellence on Embedded System Design

Duration: 01/08 - 03/12

Coordinator: VERIMAG

Abstract: The central objective for ArtistDesign is to build on existing structures and links forged in Artist2, to become a virtual Center of Excellence in Embedded Systems Design. This will be mainly achieved through tight integration between the central players of the European research community. Also, the consortium is smaller, and integrates several new partners. These teams have already established a long-term vision for embedded systems in Europe, which advances the emergence of Embedded Systems as a mature discipline.
The research effort aims at integrating topics, teams, and competencies, grouped into 4 Thematic Clusters: “Modelling and Validation”, “Software Synthesis, Code Generation, and Timing Analysis”, “Operating Systems and Networks”, “Platforms and MPSoC”. “Transversal Integration” covering both industrial applications and design issues aims for integration between clusters.
The Vertecs EPI is a partner of the “Validation” activity of the “Modeling and Validation” cluster. This year, the Vertecs EPI has contributed to quantitative verification of timed automata [20], test generation from nondeterministic timed automata [7], and control sysnthesis using abstract interpretation for infinite state systems [12].

7.2.2. Major European Organizations with which the Team has followed Collaborations

Université Libre Bruxelles (Belgium), Prof. Thierry Massart, Testing and control of symbolic transitions systems.

University of Kaiserslautern (Germany), Roland Meyer, Petri nets.

University of Dresden (Germany), Prof. Christel Baier, Probabilistic automata over infinite words.

University of Mons (Belgium), Prof. Thomas Brihaye, Stochastic timed automata.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Laurie Ricker, associate professor at the Mathematics & Computer Science department of Mount Allison University (Canada) has visited Vertecs for 6 months, from January 2012 to June 2012. We collaborate on control of discrete event systems for distributed and decentralized systems.

7.3.2. Visits to International Teams

Nathalie Bertrand spent 9 months at University of Liverpool, from November 1st 2011 to July 31st 2012. Her visit was supported by the Leverhulme Trust and the Sabbatical program of Inria, which also permitted Paulin Fournier to spend 5 months at University of Liverpool for his Master thesis.

ABSTRACTION Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. AbstractCell

Title: Formal abstraction of quantitative semantics for protein-protein interaction cellular network models

Instrument: ANR-Chair of Excellence (Junior, long term)

Duration: December 2009 - December 2013

Coordinator: Inria (France)

Others partners: None

See also: http://www.di.ens.fr/ feret/abstractcell

Abstract: The overall goal of this project is to investigate formal foundations and computational aspects of both the stochastic and differential approximate semantics for rule-based models. We want to relate these semantics formally, then we want to design sound approximations for each of these semantics (by abstract interpretation) and investigate scalable algorithms to compute the properties of both the stochastic and the differential semantics. Jérôme Feret is the principal investigator for this project.

8.1.1.2. AstréeA

Title: Static Analysis of Embedded Asynchronous Real-Time Software

Type: ANR Ingénierie Numérique Sécurité 2011

Instrument: ANR grant

Duration: January 2012 - December 2015

Coordinator: Airbus France (France)

Others partners: École normale supérieure (France)

See also: http://www.astreea.ens.fr

Abstract: The focus of the ASTRÉEA project is on the development of static analysis by abstract interpretation to check the safety of large-scale asynchronous embedded software. During the THÉSÉE ANR project (2006–2010), we developed a concrete and abstract models of the ARINC 653 operating system and its scheduler, and a first analyzer prototype. The gist of the ASTRÉEA project is the continuation of this effort, following the recipe that made the success of ASTRÉE: an incremental refinement of the analyzer until reaching the zero false alarm goal. The refinement concerns: the abstraction of process interactions (relational and history-sensitive abstractions), the scheduler model (supporting more synchronisation primitives and taking priorities into account), the memory model (supporting volatile variables), and the abstraction of dynamical data-structures (linked lists). Patrick Cousot is the principal investigator for this project.

8.1.1.3. Verasco

Title: Formally-verified static analyzers and compilers

Type: ANR Ingénierie Numérique Sécurité 2011

Instrument: ANR grant

Duration: Septembre 2011 - September 2015

Coordinator: Inria (France)

Others partners: Airbus France (France), IRISA (France), Inria Saclay (France)

See also: http://www.systematic-paris-region.org/fr/projets/verasco

Abstract: The usefulness of verification tools in the development and certification of critical software is limited by the amount of trust one can have in their results. A first potential issue is *unsoundness* of a verification tool: if a verification tool fails (by mistake or by design) to account for all possible executions of the program under verification, it can conclude that the program is correct while it actually misbehaves when executed. A second, more insidious, issue is *miscompilation*: verification tools generally operate at the level of source code or executable model; a bug in the compilers and code generators that produce the executable code that actually runs can lead to a wrong executable being generated from a correct program.

The project VERASCO advocates a mathematically-grounded solution to the issues of formal verifying compilers and verification tools. been mechanically proved to be free of any miscompilation will be continued. Finally, the tool qualification issues that must be addressed before formally-verified tools can be used in the aircraft industry, will be investigated.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. MBAT

Title: Combined Model-based Analysis & Testing of Embedded Systems

Type: Artemis Call 10

Instrument: FP7 project

Duration: November 2011 - October 2014

Coordinator: Daimler (Germany)

Others partners: 38 partners in Austria, Denmark, Estonia, France, Germany, Italy, Sweden, and United Kingdom

See also: http://www.artemis-ia.eu/project/index/view/?project=29

Abstract: MBAT will mainly focus on providing a technology platform for effective and cost-reducing validation and verification of embedded systems, focusing primarily on transportation domain, but also to be used in further domains. The project involves thirty three European industrial (large companies and SMEs) and five academic partners. Radhia Cousot is the principal investigator for this project.

8.2.1.2. MemCad

Title: Memory Compositional Abstract Domains

Type: IDEAS ()

Instrument: ERC Starting Grant (Starting)

Duration: October 2011 - September 2016

Coordinator: Inria (France)

Others partners: none

See also: http://www.di.ens.fr/~rival/memcad.html

Abstract: The MemCAD project aims at setting up a library of abstract domains in order to express and infer complex memory properties. It is based on the abstract interpretation frameworks, which allows to combine simple abstract domains into complex, composite abstract domains and static analyzers. While other families of abstract domains (such as numeric abstract domains) can be easily combined (making the design of very powerful static analyses for numeric intensive applications possible), current tools for the analysis of programs manipulating complex abstract domains usually rely on a monolithic design, which makes their design harder, and limits their efficiency. The purpose of the MemCAD project is to overcome this limitation. Our proposal is based on the observation that the complex memory

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Yanjun Wen is associate professor at the Department of Computer Science and Technology, College of Computer, National University of Defense Technology, Changsha, P. R. China. He has visited the team from June 2011 to May 2012 and is interested in the static analysis of parallel software by abstract interpretation.

Roberto Giacobazzi, professor at the University of Verona, Italy, visited the Team in May 2012.

Michael Hicks is associate professor at the Department of Computer Science, University of Maryland, USA. He has visited the team in October 2012 and is interested in abstract interpretation, software security, and differential privacy.

Tatjana Petrov is a PhD student at ETH Zürich. She has visited the team in February 2012 and is interested in the model reduction of stochastic systems.

8.3.1.1. Internships

David Delmas is an engineer at Airbus France on educational leave to pursue the 2nd year of the Parisian Master of Research in Computer Science (MPRI). He has visited the team from September 2011 to August 2012.

ATEAMS Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. Master Software Engineering

ATEAMS is the core partner in the Master Software Engineering at Universiteit van Amsterdam. This master is a collaboration between SWAT/ATEAMS, Universiteit van Amsterdam, Vrije Universiteit and Hogeschool van Amsterdam.

6.1.2. Early Quality Assurance in Software Production

The EQUA project is a collaboration among Hogeschool van Amsterdam (main partner) Centrum Wiskunde & Informatica (CWI), Technisch Universiteit Delft, Laboratory for Quality of Software (LaQuSo), Info Support, Software Improvement Group (SIG), and Fontys Hogeschool Eindhoven.

6.1.3. Model-Driven Engineering in Digital Forensics

In this project ATEAMS works with the Dutch National Forensics Institute on next generation carving software for recovering evidence from damaged or erased data storage media.

6.1.4. Next Generation Auditing: Data-assurance as a service

This collaboration between Centrum Wiskunde & Informatic (CWI) PriceWaterhouseCoopers (PWC), Belastingdienst (National Tax Office), and Computational Auditing, is to enable research in the field of computational auditing.

6.2. European Initiatives

6.2.1. FP7 Projects

OSSMETER aims to extend the state-of-the-art in the field of automated analysis and measurement of open-source software (OSS), and develop a platform that will support decision makers in the process of discovering, comparing, assessing and monitoring the health, quality, impact and activity of open-source software. The project started in October 2012. ATEAMS contributes to this project by focusing on software analysis and related areas.

6.3. International Research Visitors

6.3.1. Visits of International Scientists

- Michael W. Godfrey, PhD, Associate professor - David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada. (full year visit)
- Alex Loh - University of Texas, Austin, U.S.A. (three month internship for excellent PhD students)
- William Cook - University of Texas, Austin, U.S.A.
- Erik Meijer - Microsoft Research, Seattle, U.S.A.
- Oege de Moor - Semmle & Oxford University
- Krzystof Czarnecki - University of Waterloo, Canada
- Stéphane Ducasse - Inria Lille, France
- Ralf Lämmel - University of Koblenz-Landau, Germany
- Magne Haveraaen - University of Bergen, Norway

- Anya Helene Bagge, PhD - University of Bergen, Norway
- Vlad Rusu - Inria Lille, France
- Ted Kaminsky - University of Minnesota, U.S.A.
- Anthony Cleve - FUNDP, Namur, Belgium
- Anthony Sloane - Macquarie University, Australia
- Elizabeth Scott - RHUL, London, England
- Peter Mosses - University of Swansea, Wales
- Adrian Johnstone - RHUL, London, England

6.3.1.1. Internships

- Douwe Kasemier
- Arnoud Roo
- Jasper Timmer
- Wietse Venema
- Ashim Shahi
- Jouke Stoel
- Dennis van Leeuwen
- Jeroen Lappenschaar
- Luuk Stevens
- Floris Looijesteijn
- Pieter Brantwijk

6.3.2. Visits to International Teams

- Tijs van der Storm visited University of Texas Austin for two weeks in November.
- Paul Klint visited University of London and University of Swansea
- Paul Klint visited University of Swansea
- Paul Klint visited FUNDP in Namur
- Jurgen Vinju and Tijs van der Storm visited RMOD at Inria Lille
- Jurgen Vinju visited VUB, Brussels, Belgium
- Vadim Zaytsev visited Universität Koblenz-Landau, Germany

CARTE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Emmanuel Jeandel is a member of ANR Blanche ANR-09-BLAN-0164 (EMC: *Emerging Phenomena in Computation Models*).
- We obtained an ANR project called Binsec which will start in 2013. The aim of the BINSEC project is to fill part of the gap between formal methods over executable code on one side, and binary-level security analyses currently used in the security industry. We target two main applicative domains: vulnerability analysis and virus detection. Two other closely related applications will also be investigated: crash analysis and program deobfuscation.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. FI-WARE

Title: Morphus

Type: COOPERATION (ICT)

Defi: PPP FI: Technology Foundation: Future Internet Core Platform

Instrument: Integrated Project (IP)

Duration: September 2011 - May 2014

Coordinator: Telefonica (Spain)

Others partners:Thales, SAP, Inria

See also: http://www.fi-ware.eu/

Abstract: FI-WARE will deliver a novel service infrastructure, building upon elements (called Generic Enablers) which offer reusable and commonly shared functions making it easier to develop Future Internet Applications in multiple sectors. This infrastructure will bring significant and quantifiable improvements in the performance, reliability and production costs linked to Internet Applications for building a true foundation for the Future Internet.

8.3. International Initiatives

8.3.1. Inria Associate Teams

8.3.1.1. CRISTAL

Title: Resource Control by Semantic Interpretations and Linear Proof Theory

Inria principal investigator: Romain Péchoux

International Partner (Institution - Laboratory - Researcher):

Universita degli Studi di Torino (Italy) - Dipartimento di informatica

Duration: 2010 - 2012

See also: http://carte.loria.fr/index.php?option=com_content&view=article&id=61&Itemid=75

Topic: resource control using semantics interpretations and linear proof theory.

8.3.2. Participation In International Programs

Mathieu Hoyrup is the principal investigator of a Partenariat Hubert Curien Imhotep 2011-2012 together with Walid Gooma, University of Alexandria, Egypt.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Daniel Leivant: October 25th to November 5th, 2012, Indiana University, USA.

Walid Gooma: December, 2012, University of Alexandria, Egypt.

8.4.2. Visits to International Teams

Guillaume Bonfante: July 7th to 15th, 2012, invited by Stanislas Leibler from the 'Institute of Advanced Studies', Princeton, USA. He gave a course on computer virology at the summer school "PiTP", Prospects in Theoretical Physics http://www.sns.ias.edu/pitp2/index.html

Jean-Yves Marion: October 25th to November 5th, 2012, Indiana University, USA, work with Daniel Leivant.

Romain Péchoux: February and August 2012, University of Pennsylvania, USA, invited talk to the PLclub seminar.

CASSIS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Franche-Comté Region project SyVAD (SysML Verification and Validation), coordinated by Fabrice Bouquet, duration: 3 years, started in September 2011. This project focuses on the SysML models for the validation and verification of the micro-systems, in particular for distributed micro airduct. The project associates several team of FEMTO-ST institute.

8.2. National Initiatives

8.2.1. ANR

- ANR DECERT — *Deduction and Certification*, coordinated by Thomas Jensen (IRISA). This project focuses on the design of decision procedures, in particular for fragments of arithmetic, and their integration into larger verification systems, including skeptical proof assistants. Partners are: IRISA Rennes, LRI Orsay, Inria Sophia, Systerel and CEA. From Inria Nancy, the teams Veridis and Cassis are involved. This project started in January 2009 for three years.
- ANR TASCCC *Test Automatique basé sur des Scenarios et Critères Communs – Automated Testing based on Scenarios and Common Criteria*, duration: 3 years, starting in December 2009. The project aims at completing the model-based testing process initiated in the POSE project, using scenarios to specify the test cases that have to be generated by model animation. The goal is here to provide an automated means for generating the scenarios from a given set of properties. The overall objective is to ease the Common Criteria evaluation of secure softwares. Partners: Trusted Labs (leader), Gemalto, LIG, LIFC, Supelec, Smartesting, and Serma Technologies. The local coordinator is Frédéric Dadeau.
- ANR PROSE *Protocoles de sécurité : modèle formel, modèle calculatoire, and implémentations — Security protocols : formal model, computational model, and implementations*, duration: 4 years, started in December 2010. The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: *(i)* the symbolic level, in which messages are terms, *(ii)* the computational level, in which messages are bitstrings, and *(iii)* the implementation level: the program itself. Partners are Cascade Paris (leader), LSV Cachan, Cassis and Verimag Grenoble.
- ANR STREAMS *Solution for Peer-to-peer Real-Time Social Web*, duration: 3 years, starting in October 2010. This project proposes to design peer-to-peer solutions that offer underlying services required by real-time social web applications and that eliminate the disadvantages of centralised architectures. There exists a tension between sharing data with friends in a social network deployed in an open peer-to-peer network and ensuring privacy. One of the most challenging issues in social applications is how to balance collaboration with access control to shared objects. This project aims at providing theoretical solutions to these challenges as well as practical experimentations. Partners are: LORIA Score team (leader), Inria project-teams Regal, Asap, Cassis, and XWiki.
- ANR FREC *Frontiers of recognizability*, duration: 4 years, starting in October 2010. The goal of this project is to be a driving force behind the extension of the algebraic theory of regular languages made possible by recent advances. Four directions will be investigated: tree languages, λ-terms, automata with counters, algebraic and topological tools. Partners are LABRI (leader), LIAFA (University Paris 7). Pierre-Cyrille Héam is a member of this project, attached to Paris 7 for administrative facilities.

- ANR OSEP *Online and offline model-based testing of SEcurity Properties*, duration: 2 years, starting in December 2011. The goal of this project is to test the security with online and offline model-based testing approach. The main element of project is to capitalize or to reuse a test model with different testing method. So, we develop new algorithms to allow online testing. This approach must be compatible with our previous offline approach to increase the number of artefacts that can be shared. This approach can be applied to the components of security and the Software Radio. Partners are DGA and Smartesting.

8.2.2. Competitivity Clusters

- FUI SQUASH *Software QUality ASsurance enHancement*, duration: 2 years, starting in April 2011. This project aims to industrialize and to structure software testing activities. The project will provide a methodology and tools based on open source components.
- Project "Investissement d'Avenir - Développement de l'Econimie Numérique" DAST (Dynamic Application Security Testing), duration: 2 years, starting in September 2012. The goal of this project is to generate automatically the tests to prevent vulnerabilities. Partners are NBSystem, Smartesting (coordinator), Thales, Trusted-Labs and Inria Cassis.

8.3. European Initiatives

8.3.1. FP7 Projects

- Nessos is a Network of Excellence on Engineering Secure Future Internet Software Services and Systems in FP7-ICT (starting in October 2010 for a period of 42 months). Nessos has 12 partners and aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. Partner Inria is involved through project-teams Arles, Triskell and Cassis. Cassis will focus on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [4]— ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. This long-term project aims at developing provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, we foresee three main tasks. First, we plan to develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second, we will consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we aim at proposing modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.
- SecureChange[5] is funded under the 7th FP (Seventh Framework Program) Research area: ICT-2007.8.6: ICT forever yours. The project will develop processes and tools that support design techniques for evolution, testing, verification, re-configuration and local analysis of evolving software. Our focus is on mobile devices and homes, which offer both great research challenges and long-term business opportunities. The project is lead by Fabio Massacci (University of Trento, Italy) and it has started in February 2009 for a period of 36 months. Cassis is leader of the 7th workpackage (Testing). The local coordinator is Fabrice Bouquet.

8.4. International Initiatives

8.4.1. Inria Associate Teams

BANANAS[6]*Automated design and autonomous control of hybrid solver cooperations*. In order to tackle large scale instances and intricate problem structures, sophisticated solving techniques have been developed,

[4] http://www.loria.fr/~cortier/ProSecure.html
[5] http://www.securechange.eu
[6] http://www.loria.fr/~ringeiss/CHILI/bananas

combined, and hybridized to provide efficient solvers. A common idea to get more efficient and robust algorithms consists in combining several resolution paradigms in order to take advantage of their respective assets. Autonomous Search is a very attractive approach for designing adaptive systems with the capability of improving its solving performance by selecting and adapting its search strategies to the problem at hand. The main goal of the project is to apply the Autonomous Search approach to hybrid solver cooperations, by automating the selection and the cooperation of solvers, by tuning the cooperation parameters, and by adapting the cooperation during solving. The international partners are Technical University Federico Santa Maria, Valparaíso (Chile) — Department of Computer Science — Carlos Castro and Eric Monfroy; University of Chile (Chile) — Center for Mathematical Modeling — Jorge Amaya. The Inria principal investigator is Christophe Ringeissen.

8.4.2. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on soundness of symbolic models w.r.t. cryptographic ones.
- Collaboration with Mark Ryan's group (University of Birmingham) on the formal analysis of e-voting protocols.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.

8.4.3. Participation In International Programs

French-Tunisian project on *Security Policies and Configurations of Firewalls: Compilation and Automated Verification*. We collaborate with SupCom Tunis and the Inria project-team Dahu in the context of STIC-Tunisia.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Jan Otop (Wroclaw University), one month in March 2012
- Markulf Kohlweiss (Microsoft Cambridge), one week in April 2012
- Bogdan Warinshi (Bristol University), one week in May 2012
- Myrto Arapinis (University of Birmingham), three weeks in July 2012
- Mark Ryan (University of Birmingham), one week in July 2012
- Serdar Erbatur (SUNY Albany), two months in October–November 2012
- John Mullins (Ecole Polytechnique de Montréal), one week, February 2012.
- Hanifa Boucheneb, (Ecole Polytechnique de Montréal), one month in March 2012

8.5.1.1. Internships

- Aurel Josias Randolph (from Apr 2012 until May 2012)
  - Subject: Specifying and verifying access control policies for collaborative editors
  - Institution: Polytechnic School of Montreal (Canada)
- Ghazi Maatoug (from Mar 2012 until Jul 2012)
  - Subject: Verification of protocols, analysis of symbolic trace and simulated execution
  - Institution: Ecole Supérieure des Communications de Tunis (Tunisia)
- Apoorva Desphande (from Jul 2012 until Nov 2012)
  - Subject: Verification of equivalence properties in security protocols
  - Institution: BITS Pilani University (India)
- Anshul Malhotra (from Dec 2012 until Jan 2013)

  - Subject: Efficient implementation of a procedure for the verification of equivalence properties
  - Institution: IIT Delhi (India)

8.5.2. Visits to International Teams

- Véronique Cortier, February 2012 (one week), Bristol University (collaboration with Bogdan Warinschi)
- Christophe Ringeissen and Laurent Vigneron, December 2012 (two weeks), UTFSM Valparaíso (Inria Associate Team BANANAS)

CELTIQUE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. The PiCoq ANR project

Participant: Alan Schmitt.

Process calculi, Verification, Proof Assistants

The goal of the (PiCoq project) is to develop an environment for the formal verification of properties of distributed, component-based programs. The project's approach approach lies at the interface between two research areas: concurrency theory and proof assistants. Achieving this goal relies on three scientific advances, which the project intends to address:

- Finding mathematical frameworks that ease modular reasoning about concurrent and distributed systems: due to their large size and complex interactions, distributed systems cannot be analysed in a global way. They have to be decomposed into modular components, whose individual behaviour can be understood.
- Improving existing proof techniques for distributed/modular systems: while behavioural theories of first-order concurrent languages are well understood, this is not the case for higher-order ones. We also need to generalise well-known modular techniques that have been developed for first-order languages to facilitate formalization in a proof assistant, where source code redundancies should be avoided.
- Defining core calculi that both reflect concrete practice in distributed component programming and enjoy nice properties w.r.t. behavioural equivalences.

The project partners include Inria, LIP, and Université de Savoie. The project runs from November 2010 to October 2014.

7.1.2. The ANR VERASCO project

Participants: Sandrine Blazy, Delphine Demange, Vincent Laporte, André Oliveira Maroneze, David Pichardie.

Static program analysis, Certified static analysis

The VERASCO project (2012–2015) is founded by the call ISN 2011, a program of the Agence Nationale de la Recherche. It investigates the formal verification of static analyzers and of compilers, two families of tools that play a crucial role in the development and validation of critical embedded software. It is a joint project with the Inria teams ABSTRACTION, GALLIUM, The VERIMAG laboratory and the Airbus company.

7.1.3. ANR DECERT project

Participants: Frédéric Besson, Thomas Jensen, David Pichardie, Pierre-Emmanuel Cornilleau.

The DECERT project (2009–2012) is funded by the call Domaines Emergents 2008, a program of the Agence Nationale de la Recherche.

The objective of the DECERT project has been to design an architecture for cooperating decision procedures, with a particular emphasis on fragments of arithmetic, including bounded and unbounded arithmetic over the integers and the reals, and on their combination with other theories for data structures such as lists, arrays or sets. 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.

This is a joint project with Systerel, CEA List and Inria teams Mosel, Cassis, Marelle, Proval and Celtique (coordinator).

7.1.4. Labex COMIN Labs Seccloud project

Participants: Frédéric Besson, Thomas Jensen, Alan Schmitt, Martin Bodin.

The SecCloud project, started in 2012, will provide a comprehensive language-based approach to the definition, analysis and implementation of secure applications developed using Javascript and similar languages. Our high level objectives is to enhance the security of devices (PCs, smartphones, ect.) on which Javascript applications can be downloaded, hence on client-side security in the context of the Cloud. We will achieve this by focusing on three related issues: declarative security properties and policies for client-side applications, static and dynamic analysis of web scripting programming languages, and multi-level information flow monitoring.

This is a joint project with Supelec Rennes and Ecole des Mines de Nantes.

7.2. European Initiatives

7.2.1. Collaborations with Major European Organizations

Imperial College (UK)

The JScert project (http://jscert.org) aims to really understand JavaScript by building models of ECMAScript semantics in the Coq proof assistant, and automated logical reasoning tools built on those semantics.

7.3. International Initiatives

7.3.1. Inria International Partners

Delphine Demange and David Pichardie have been working with Gilles Barthe from IMDEA Software, Madrid, Spain about the new verified SSA middle-end.

7.4. International Research Visitors

7.4.1. Visits to International Teams

David Pichardie has spent one year at Purdue University, Indiana, US (from September 2011 to August 2012) working with Jan Vitek and Suresh Jagannathan. This was a one year Inria sabbatical leave. The collaboration deals with the formal verification of a Java compiler, taking into account concurrency. As a first result, a paper will appear at POPL 2013 where we provide a new intermediate memory model for the Java language.

COMETE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR projects

7.1.1.1. ANR-09-BLAN-0169-01

Project acronym: PANDA

Project title: Analysis of Parallelism and Distribution

Duration: October 2009 - March 2013

URL: http://lipn.univ-paris13.fr/~mazza/Panda/

Coordinator: Catuscia Palamidessi, Inria Saclay

Other PI's and partner institutions: Dale Miller, EPIs Parsifal at Inria Saclay. Emmanuel Haucourt, CEA Saclay. Damiano Mazza, Pôle Parisien (ENS Cachan, Paris VII and Paris XIII). Emmanuel Godard, Pôle Méditerranéen (ENS Lyon and the University of Marseille). Jean Souyris, Airbus.

Abstract: The aim of PANDA is to bring together different mathematical models of parallel and concurrent computation (geometric models, rewriting theory, higher category theory, stochastic processes), along with theoretical frameworks for static analysis (spatial logics, proof construction), in order to guide the development of software tools that meet industrial needs of program specification and verification (in particular, fault detection of parallel programs involved in avionics).

7.1.1.2. ANR-09-BLAN-0345-02

Project acronym: CCP

Project title: Confidence, Proof and Probabilities

Duration: October 2009 - March 2013

URL: http://www.lix.polytechnique.fr/~bouissou/cpp/

Coordinator: Jean Goubault-Larrecq, ENS Cachan

Other PI's and partner institutions: Catuscia Palamidessi, Inria. Olivier Bouissou, CEA LIST. Gilles Fleury, Supelec SSE. Michel Kieffer, Supelec L2S.

Abstract: In the context of proofs of safety properties for critical software, The CPP project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs.

7.1.2. Large-scale initiatives

Project acronym: CAPPRIS

Project title: Collaborative Action on the Protection of Privacy Rights in the Information Society

Duration: October 2011 - September 2015

Coordinator: Daniel Le Metayer, Inria Grenoble

Other partner institutions: The project involves four Inria research centers (Saclay, Saphia-Antipolis, Rennes and Grenoble), CNRS-LAAS, Eurecom and the university of Namur. Besides computer scientists, the consortium also includes experts in sociology and in law, thus covering the complementary areas of expertise required to reach the objectives.

Abstract: The goal of this project is to study the challenges related to privacy in the modern information society, trying to consider not only the technical, but also the social and legal ones, and to develop methods to enhance the privacy protection.

7.2. European Initiatives

7.2.1. FP7 Projects

Program: FP7-PEOPLE-2011-IRSES

Project acronym: MEALS

Project title: Mobility between Europe and Argentina applying Logic to Systems

Duration: October 2011 - September 2005

URL: http://www.meals-project.eu/

Coordinator: Holger Hermans, Saarland University, Germany

Other partner institutions: Rheinisch-Westfälische Technische Hochschule Aachen, Germany. Technische Universität Dresden, Germany. Inria, France. Imperial College of Science, Technology and Medicine, UK, University of Leicester, UK. Technische Universiteit Eindhoven, NL. Universidad Nacional de Cordoba, AR. Universidad de Buenos Aires, AR. Instituto Tecnologico de Buenos Aires, AR. Universidad Nacional de Rio Cuarto, AR.

Abstract: In this project we focus on three aspects of formal methods: specification, verification, and synthesis. We consider the study of both qualitative behavior and quantitative behavior (extended with probabilistic information). We aim to study formal methods in all their aspects: foundations (their mathematical and logical basis), algorithmic advances (the conceptual basis for software tool support) and practical considerations (tool construction and case studies).

7.3. International Initiatives

7.3.1. International Partners

Geoffrey Smith. School of Computing and Information Sciences, Florida International University, USA.

Vladimiro Sassone. School of Electronics and Computer Science, University of Southampton, UK.

Camilo Rueda. Department of Computer Science, Pontificia Universidad Javeriana, Colombia.

7.3.2. Participation in International Programs

Program: ANR Blanc International

Project acronym: LOCALI

Project title: Logical Approach to Novel Computational Paradigms

Duration: October 2011 - September 2015

Coordinator: Gilles Dowek, Inria Rocquencourt

Other PI's and partner institutions: Catuscia Palamidessi, Inria Saclay. Thomas Erhard, Paris VII. Ying Jiang , Chinese Academy of Science in Beijin (China).

Abstract: This project aims at exploring the interplays between logic and sequential/distributed computation in formalisms like the lambda calculus and the π calculus. Going back to the fundamentals of the definitions of these calculi, the project plans to design new programming languages and proof systems via a logical approach.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Carlos Olarte. Associate professor at the Pontificia Universidad Javeriana, Colombia. He visited for one month in July 2012, funded by the Ecole Polytechnique.

Moreno Falaschi. Full professor at the Università di Siena, Italy. He visited for one month in June 2012, funded by the Ecole Polytechnique.

Elaine Pimentel. Associate professor at the Universidade Federal de Minas Gerais, Belo Horizonte, Brazil. She visited for one month in July 2012, funded by the Ecole Polytechnique/Digiteo.

Linda Brodo. Assistant professor at the Università di Sassari, Italy. She visited for one month in June 2012, funded by the Ecole Polytechnique/Digiteo.

Vladimiro Sassone. Full professor at the University of Southampton, UK. He visited for two months in October and November 2012, funded by the Ecole Polytechnique/Digiteo.

Camilo Rueda. Full professor at the Pontificia Universidad Javeriana,Colombia. He visited for two months in October and November 2012, funded by the Ecole Polytechnique.

7.4.2. Internships

Name: Lili Xu

Duration: From October 2011 until October 2012)

Subject: Compositionality of privacy on a probabilistic process calculus

Institution: Chinese Academy of Sciences of Beijin (China)

Support: ANR project PANDA, Inria, and Chinese Academy of Sciences

Name: Marco Stronati

Duration: From October 2011 until March 2013

Subject: Compositional analysis of queries' sensitivity

Institution: University of Pisa, Italy

Support: Ecole Polytechnique and University of Pisa

Name: Fernán Martinelli

Duration: From September 2012 until March 2013

Subject: Computation of bounds on the information flow

Institution: University of Rio Cuarto, Argentina

Support: FP7 project MEALS

Name: Michela Paolini

Duration: From September 2012 until December 2012

Subject: Compositionality of privacy on a probabilistic process calculus.

Institution: IMT Institute for Advanced Studies, Lucca, Italy

Support: Grant from IMT

CONTRAINTES Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

- ANR Investissement Avenir Iceberg project (2011-2016) “From population models to model populations”, coordinated by Grégory Batt, with Pascal Hersen (MSC lab, Paris Diderot Univ./CNRS), Reiner Veitia (Institut Jacques Monod, Paris Diderot Univ./CNRS), Olivier Gandrillon (BM2A lab, Lyon Univ./CNRS), Cedric Lhoussaine (LIFL/CNRS), and Jean Krivine (PPS lab, Paris Diderot Univ./CNRS).
- ANR Blanc Net-WMS-2 (2011-2015) on “constraint optimization in Wharehouse Management Systems”, coordinated by F. Fages, with N. Beldiceanu, Ecole des Mines de Nantes, EPI TASC, and Abder Aggoun, KLS optim.
- ANR Cosinus Syne2arti project (2010-2013) coordinated by Grégory Batt, with Oded Maler, CNRS Verimag, Dirk Drasdo, EPI Bang, and Ron Weiss, MIT.
- ANR Blanc BioTempo project (2010-2013) coordinated by Anne Siegel, CNRS IRISA Rennes, with Ovidiu Radulescu, U. Montpellier, Irina Rusu, U. Nantes.
- AE REGATE (2008-2012) on the “REgulation of the GonAdoTropE axis”, coordinated by Frédérique Clément, SISYPHE, with E. Reiter, INRA Tours, J.P. Françoise, Univ. Paris 6, B. Laroche Orsay, P. Michel Centrale Lyon, N. Ayache ASCLEPIOS, A. Goldbeter, ULB Bruxelles.
- AE COLAGE (2008-) on the “control of growth and aging in *E. coli* using synthetic biology approaches”, coordinated by H. Berry, COMBINING, with F. Taddei, A. Lindner, INSERM Necker, H. de Jong, D. Ropers, IBIS, J.-L. Gouzé, and M. Chaves, COMORE.
- GENCI (2009-) attribution of 300000 computation hours per year on the Jade cluster of 10000 processors of GENCI at CINES, Montpellier.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7

Program: EraNet SysBio

Project acronym: C5Sys

Project title: Circadian and cell cycle clock systems in cancer

Duration: mars 2010 - mars 2013

Coordinator: Francis Lévi, INSERM Hopital Paul Brousse, Villejuif, France and David Rand, Warwick Systems Biology, UK,

Other partners: EPI BANG, Erasmus University Medical Center, Rotterdam, University College London, UK, CNRS Nice, and L2S, Orsay.

Abstract: Mammalian cells are endowed with biological oscillators which time their activities. The circadian clock (circa, about; dies, day) generates a 24-hour rhythm which controls both cellular metabolism and cell division. The cell division cycle is an oscillator which times DNA synthesis, mitosis, and related apoptosis and DNA repair. Our understanding of the molecular mechanisms at work in both oscillators has greatly improved. In sharp contrast, little is known about how these two crucial oscillators interact, and how these interactions affect cellular proliferation in normal or cancer cells. On the one hand, the disruption of circadian clocks impairs cell physiology and quality of life. On the other hand, disruption of cell cycle, DNA repair or apoptosis impacts on cell and organism survival. Experimental and clinical data show that circadian disruption accelerates

malignant proliferation, and that DNA damage can reset the circadian clock. The central question addressed is how interactions between the circadian clock and cell cycle affect cellular proliferation and genotoxic sensitivity in normal and cancer cells, and how this knowledge translates into new prevention or therapeutic applications. Seven teams in France, Netherlands and United Kingdom integrate experimental, mathematical and bioinformatic approaches, so as to develop novel cell lines, biomarker monitoring methods and mathematical tools. C5Sys triggers innovative chronotherapeutic research for human cancers and advances systems medicine for improving patient care.

8.3. International Initiatives

8.3.1. Inria Associate Teams

Title: Artificial tissue homeostasis: combining synthetic and computational biology approaches (TISHOM)

Inria principal investigator: Gregory Batt

International Partner (Institution - Laboratory - Researcher):

Massachusetts Institute of Technology (United States) - Weiss Lab - Ron Weiss

Duration: 2012 - 2014

See also: TISHOM

Cell-based gene therapy aims at creating and transplanting genetically-modified cells into a patient in order to treat an illness. Ideally, actively-growing cells are used to form a self-maintaining tissue in the patient, thus permanently curing the disease. Propelled forward by the development of stem cell biology, this research domain has recently attracted significant interest. Still, before any real therapeutic use, many important issues need to be addressed. In particular, one should guarantee tissue homeostasis, that is, that the size of the newly-introduced tissue remains within admissible bounds.

Using a synthetic biology approach, we propose to reprogram mammalian cells so as to enforce tissue homeostasis. The proposed design relies on growth control and cell-cell communication mechanisms. The design and tuning of such engineered tissues are particularly challenging. Indeed, the correct functioning of the system depends on its specific molecular implementation. To relate cell population behavior with molecular details, extensive modelling work and in-depth in silico analysis are needed. Therefore, a tight integration between dry lab and wet lab efforts will be essential for the success of the project.

8.3.2. Inria International Partners

We also have a collaboration with the Center for Systems and Control at the Delft University of Technology (The Netherlands) on developing formal probabilistic approaches for robust control of gene expression. This collaborative project is funded by the Frans/Nederlandse Academie as part of the van Gogh Programm (Coordination Alessandro Abate/Grégory Batt).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Visits of International Scientists

Prof. Fernando Buarque (from February 2012 until April 2012)

Subject: Fish School Optimization

Institution: University of Pernambuco, Brazil

8.4.1.2. Internships

Hui-Ju Katherine CHIANG (from Jul 2012 until Oct 2012)

Subject: Theory of temporal logic constraint solving

Institution: National Taiwan University (Taiwan)

Anthony LINS (from Mar 2012 until Jun 2012)

Subject: Particle swarm optimization for systems biology

Institution: Federal University of Pernambuco (Brazil)

8.4.1.3. Short visits

Andreas Weber, University of Bonn, Germany

Chris Banks, University of Edinburgh, UK

Francesco Santini, CWI, Amsterdam, Netherlands

Ron Weiss, MIT, USA

Alessandro Abate and Ilya Tkachev, TU Delft, Netherlands

Liu Bing, National University of Singapore, Singapore

8.4.2. Visits to International Teams

Xavier Duportet: 6 months with the Weiss lab at MIT

Szymon Stoma: two times two weeks with the Weiss lab at MIT

François Bertaux: two times two weeks with the Weiss lab at MIT

DEDUCTEAM Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR Locali

We are coordinators of the ANR-NFSC contract Locali with the Chinese Academy of Sciences. This year we mostly developed in proof in a finite structure project of this contract.

6.1.2. ANR BWare

We are members of the ANR Beware which started on last September (David Delahaye is the national leader). The objective is to provide a proof platform for B proof obligations. We are in particular involved in the introduction of Deduction modulo in the automated proved tableaux-based Zenon and also in the combination of Deduction modulo and superposition.

6.1.3. ANR Tarmac

We are members of the ANR Tarmac, coordinated by Pierre Valarcher, on models of computation.

6.2. International Research Visitors

6.2.1. Visits of International Scientists

Nachum Dershowitz (Tel Aviv) has been visiting our group for three months.

Cecilia Englander (Puc-Rio) has been visiting our group for four months.

6.2.2. Visits to International Teams

Pierre Néron has been visiting César Muñoz group in Nasa-Langley for three months.

FORMES Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Tsinghua Grant

contract: Tsinghua National Laboratory for Information Science and Technology, Cross-discipline Foundation grant 2011-9

title: An Intensional Logical Framework and Its Implementation

PIs: Jean-Pierre Jouannaud, Jianqi Li

duration: 2011 - 2012

Amount: 100,000 RMB

8.1.2. NSFC Grant

contract: National Science Foundation of China grant 61272002

title: The meta-theories of higher-order rewriting and their proof automation: toward the next generation theorem prover

PIs: Jean-Pierre Jouannaud, Jianqi Li

duration : 2013-2016

Amount: 600,000 RMB

8.2. International Initiatives

8.2.1. Inria International Partners

FORMES is an international project from LIAMA in China, located on two sites, Tsinghua University in Beijing, and CAS Shenzhen Institute of Advanced Technologies in Shenzhen. In addition this project has had collaborations with CAS Institute of Software and Harbin Engineering University in 2012.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

FORMES received visiting Pr Nachum Dershowitz from Israel at Tsinghua for a short stay.

8.3.1.1. Internships

Rémi Nollet (L3, ENS Lyon) did an internship at Inria Rocquencourt co-supervised by Frédéric Blanqui and Pierre Weis on the certification of construction functions generated by Moca.

8.3.2. Visits to International Teams

Jean-Pierre Jouannaud, invited in Barcelone, UTC, LSI-Lab, September 2012.

Frédéric Blanqui visited the Institute of Applied Mechanics and Informatics (IAMI) of the Vietnamese Acadamy of Sciences at Ho Chi Minh City.

GALLIUM Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ADN4SE (FSN)

Participant: Damien Doligez.

The "ADN4SE" project (2012-2016) is coordinated by the Sherpa Engineering company and funded by the *Briques Génériques du Logiciel Embarqué* programme of *Fonds national pour la Société Numérique*. The aim of this project is to develop a process and a set of tools to support the rapid development of embedded software with strong safety constraints. Gallium is involved in this project to provide tools and help for the formal verification in TLA+ of some important aspects of the PharOS real-time kernel, on which the whole project is based.

8.1.2. BWare (ANR)

Participant: Damien Doligez.

The "BWare" project (2012-2016) is coordinated by David Delahaye at Conservatoire National des Arts et Métiers and funded by the *Ingénierie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. BWare is an industrial research project that aims to provide a mechanized framework to support the automated verification of proof obligations coming from the development of industrial applications using the B method and requiring high guarantees of confidence.

8.1.3. CEEC (FSN)

Participants: Thomas Braibant, Xavier Leroy.

The "CEEC" project (2011-2014) is coordinated by the Prove & Run company and also involves Esterel Technologies and Trusted Labs. It is funded by the *Briques Génériques du Logiciel Embarqué* programme of *Fonds national pour la Société Numérique*. The CEEC project develops an environment for the development and certification of high-security software, centered on a new domain-specific language designed by Prove & Run. Our involvement in this project focuses on the formal verification of a C code generator for this domain-specific language, and its interface with the CompCert C verified compiler.

8.1.4. LaFoSec

Participant: Damien Doligez.

The LaFoSec study, commissioned by ANSSI, aims at studying the security properties of functional languages, and especially of OCaml. The study is done by a consortium led by the SafeRiver company. Last year, it produced more than 600 pages of documents, including recommendations for security-aware development in OCaml.

The study continued this year with the production of a prototype of a secure XML/XSD validator following these recommendations, and a security evaluation of the prototype by an independent company.

Most of these documents will be made available in 2013 on the ANSSI Web site (http://ssi.gouv.fr/).

8.1.5. Paral-ITP (ANR)

Participant: Damien Doligez.

The "Paral-ITP" project (2011-2014) is coordinated by Burkhart Wolff at Université Paris Sud and funded by the *Ingénierie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. The objective of Paral-ITP is to investigate the parallelization of interactive theorem provers such as Coq and Isabelle.

8.1.6. U3CAT (ANR)

Participant: Xavier Leroy.

The "U3CAT" project (2009-2012) ended in August 2012. It was coordinated by Virgile Prevosto at CEA LIST and funded by the *Arpège* programme of *Agence Nationale de la Recherche*. This action focused on program verification tools for critical embedded C codes. We were involved in this project on issues related to memory models [35] and formal semantics for the C language, at the interface between compilers and verification tools.

8.1.7. Verasco (ANR)

Participants: Jacques-Henri Jourdan, Xavier Leroy.

The "Verasco" project (2012-2015) is coordinated by Xavier Leroy and funded by the *Ingéniérie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. The objective of this 4-year project is to develop and formally verify a static analyzer based on abstract interpretation, and interface it with the CompCert C verified compiler.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

Gabriel Dos Reis, assistant professor at Texas A&M University, visited the Gallium team in July 2012, to work on the formal semantics of the C and C++ languages.

8.2.1.1. Internships

Joseph Tassarotti, undergraduate student at Harvard University, did an internship at Gallium from June to August 2012. He worked on register allocation and instruction scheduling for the CompCert verified compiler.

MARELLE Project-Team

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 Götegorg (Sweden)

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

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

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

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).

MEXICO Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

The research involving the PhD thesis of Aiswarya Cyriac on temporal logics for concurrent recursive programs is supported by the DIGITEO project LOCOREP, 2010-2013. Hernán Ponce de León's research on conformance testing for concurrent systems through event structures is supported by the DIGITEO project TECSTES, 2011-2014.

7.2. National Initiatives

7.2.1. ANR

Participants: Sandie Balaguer, Thomas Chatain, Stefan Haar, Serge Haddad.

The Project ANR **ImpRo** ANR-2010-BLAN-0317 involves *IRCCyN* (Nantes), *IRISA* (Rennes), *LIP6*(Paris), *LSV* (Cachan), *LIAFA* (Paris) and *LIF* (Marseille). It addresses issues related to the practical implementation of formal models for the design of communication-enabled systems: such models abstract away from many complex features or limitations of the execution environment. The modeling of *time*, in particular, is usually idealized, with infinitely precise clocks, instantaneous tests or mode communications, etc. Our objective is thus to study to what extent the practical implementation of these models preserves their good properties. We aim at a generic mathematical framework to reason about and measure implementability, and then study the possibility to integrate implementability constraints in the models. A particular focus is on the combination of several sources of perturbation such as resource allocation, the distributed architecture of applications, etc. We also study implementability through control and diagnosis techniques, and apply the developed methods to a case study based on the AUTOSAR architecture, a standard in the automotive industry.

7.3. European Initiatives

7.3.1. FP7 Projects

7.3.1.1. Hycon2

Title: Highly Complex and Networked Control Systems

Type: COOPERATION (ICT)

Defi: Engineering of Networked Monitoring and Control Systems

Instrument: Network of Excellence (NoE)

Duration: September 2010 - August 2014

Coordinator: CNRS (France)

Others partners: Inria (France), ETH Zurich (Switzerland), TU Berlin (Germany), TU Delft (Netherlands) and many others.

See also: http://www.hycon2.eu

Abstract: Hycon 2 aims at stimulating and establishing a long-term integration in the strategic field of control of complex, large-scale, and networked dynamical systems. It focuses in particular on the domains of ground and aerospace transportation, electrical power networks, process industries, and biological and medical systems.

7.3.1.2. Univerself

Title: Univerself

Type: COOPERATION (ICT)

Defi: The Network of the Future

Instrument: Integrated Project (IP)

Duration: September 2010 - August 2013

Coordinator: Alcatel Lucent (France)

Others partners: Universiteit Twente, Alcatel Lucent Ireland, Alcatel Lucent Deutschland, Valtion Teknillinen Tutkimuskeskus (Finland), University of Piraeus, France Telecom, Telecom Italia, National University of Athens, Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung, Interdisciplinary Institute for Broadband Technology, Telefonica Investigacion y Desarrollo,Thales Communications, Inria,Nec Europe, University of Surrey, University College London, IBBT (Belgium).

See also: http://www.univerself-project.eu/

Abstract: UniverSelf unites 17 partners with the aim of overcoming the growing management complexity of future networking systems, and to reduce the barriers that complexity and ossification pose to further growth. Univerself has been launched in October 2010 and is scheduled for four years.

7.4. International Initiatives

7.4.1. Inria International Partners

The CMI (Chennai Mathematical Institute) is a long-standing partner of our team. The project *Île de France/Inde* in the *ARCUS* program from 2008 to 2011 has allowed several exchange visits between Cachan and Chennai, organizations of ACTS workshops with french and indian researchers in Chennai, internships in Cachan, and two theses in *co-tutelle* (Akshay Sundararaman, defended in 2010) and Aiswarya Cyriac (thesis in progress).

Currently, Paul Gastin is co-head (with Madhavan Mukund) of the new International Associated Laboratory (LIA) INFORMEL (INdo-French FORmal Methods Lab). This LIA was created in January 2012 by an agreement between CNRS, ENS Cachan, University Bordeaux 1 on the french side and the Chennai Mathematical Institute, the Institute of Mathematical Sciences of Chennai, and the Indian Institute of Science of Bangalore on the Indian side.

7.4.2. Participation In International Programs

Benedikt Bollig, Aiswarya Cyriac, and Benjamin Monmege are participating in LeMon, a joint Procope project with LIAFA, (Paris) and the University of Lübeck, supported by EGIDE/DAAD. The aim of the project is to develop techniques for the inference of systems that deal with infinite data domains.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

Supported by the LIA INFORMEL,

- K. Narayan Kumar from CMI visited our team from May 2nd to 27th, and
- Madhavan Mukund from CMI visited our team from May 8th to June 3rd.

From April 10 to April 13, Victor Khomenko from Newcastle University (UK) visited the team.

Estibaliz Fraca, PhD student from Zaragossa, is visiting from november 2012 trough February 2013.

7.5.1.1. Internships

Umang Mathur (IIT Bombay, India) effected a two-month internship from May to July at ENS Cachan, co-financed by the Inria Internship program, which was jointly supervised by Rohit Chadha (of the Secsi team) and Stefan Schwoon. The co-operation is being continued remotely, with Rohit Chadha now at the University of Missouri.

Subject: Estimating the Information Leakage of a Recursive Probabilistic Program.

Institution: IIT Bombay, India

Gaurav MAHAJAN (from May 2012 until Jul 2012)

Subject: Probabilistic Unfolder for Petri Nets

Institution: IIT Delhi (India)

7.5.2. Visits to International Teams

The team members made several *short* visits:

- Supported by the LIA INFORMEL, Paul Gastin visited the Chennai Mathematical Institute (CMI) in India from January 9 to 21.
- Benedikt Bollig and Aiswarya Cyriac were visiting Thomas Schwentick's group at TU Dortmund University (March 13 – 16).
- Benjamin Monmege was visiting Martin Leucker's group at the University of Lübeck (July 9 – 14 and October 28 – November 2).
- Stefan Schwoon visited Javier Esparza's group at TU Müchen and gave a talk in April 2012.
- Serge Haddad visited Rolf Hennicker's group at LMU Munich in November 2012.

PAREO Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

We participate in the "Logic and Complexity" part of the GDR–IM (CNRS Research Group on Mathematical Computer Science), in the projects "Logic, Algebra and Computation" (mixing algebraic and logical systems) and "Geometry of Computation" (using geometrical and topological methods in computer science).

7.1.1. FRAE QUARTEFT (2009-2012)

Participants: Jean-Christophe Bach, Horatiu Cirstea, Pierre-Etienne Moreau.

"QUARTEFT: QUAlifiable Real TimE Fiacre Transformations" is a research project funded by the FRAE (Fondation de Recherche pour l'Aéronautique et l'Espace). A first goal is to develop an extension of the Fiacre intermediate language to support real-time constructs. A second goal is to develop new model transformation techniques to translate this extended language, Fiacre-RT, into core Fiacre. One of the main difficulties consists in proposing transformation techniques that could be verified in a formal way. A more detailed presentation is available at http://quarteft.loria.fr/dokuwiki/.

7.2. International Research Visitors

7.2.1. Visits of International Scientists

Cooperation with Prof. Mark van den Brand from Technical University of Eindhoven.

PARSIFAL Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. FP7 Projects

7.1.1.1. Proofcert

Title: ProofCert: Broad Spectrum Proof Certificates

Type: IDEAS

Instrument: ERC Advanced Grant (Advanced)

Duration: January 2012 - December 2016

Coordinator: Inria (France)

See also: https://team.inria.fr/parsifal/proofcert/

Abstract: The ProofCert proposal aims at building a foundation that will allow a broad spectrum of formal methods—ranging from automatic model checkers to interactive theorem provers—to work together to establish formal properties of computer systems. This project starts with a wonderful gift to us from decades of work by logicians and proof theorist: their efforts on logic and proof has given us a universally accepted means of communicating proofs between people and computer systems. Logic can be used to state desirable security and correctness properties of software and hardware systems and proofs are uncontroversial evidence that statements are, in fact, true. The current state-of-the-art of formal methods used in academics and industry shows, however, that the notion of logic and proof is severely fractured: there is little or no communication between any two such systems. Thus any efforts on computer system correctness is needlessly repeated many times in the many different systems: sometimes this work is even redone when a given prover is upgraded. In ProofCert, we will build on the bedrock of decades of research into logic and proof theory the notion of proof certificates. Such certificates will allow for a complete reshaping of the way that formal methods are employed.

7.1.2. Collaborations in European Programs, except FP7

7.1.2.1. STRUCTURAL: ANR blanc International

Participants: Kaustuv Chaudhuri, Nicolas Guenot, Willem Heijltjes, François Lamarche, Dale Miller, Lutz Straßburger.

Title: Structural and computational proof theory

Duration: 01/01/2011 – 31/12/2013

Partners:

University Paris VII, PPS (PI: Michel Parigot)

Inria Saclay–IdF, EPI Parsifal (PI: Lutz Straßburger)

University of Innsbruck, Computational Logic Group (PI: Georg Moser)

Vienna University of Technology, Theory and Logic Group (PI: Matthias Baaz)

Total funding by the ANR: 242 390,00 EUR (including 12 000 EUR pôle de compétivité: SYSTEMTIC Paris région)

This project is a consortium of four partners, two French and two Austrian, who are all internationally recognized for their work on structural proof theory, but each coming from a different tradition. One of the objective of the project is build a bridge between these traditions and develop new proof-theoretic tools and techniques of structural proof theory having a strong potential of applications in computer science, in particular at the level of the models of computation and the extraction of programs and effective bounds from proofs.

On one side, there is the tradition coming from mathematics, which is mainly concerned with first-order logic, and studies, e.g., Herbrand's theorem, Hilbert's epsilon-calculus, and Goedel's Dialectica interpretation. On the other side, there is the tradition coming from computer science, which is mainly concerned with propositional systems, and studies, e.g., Curry-Howard isomorphism, algebraic semantics, linear logic, proof nets, and deep inference. A common ground of both traditions is the paramount role played by analytic proofs and the notion of cut elimination. We will study the inter-connections of these different traditions, in particular we focus on different aspects and developments in deep inference, the Curry-Howard correspondence, term-rewriting, and Hilbert's epsilon calculus. As a byproduct this project will yield a mutual exchange between the two communities starting from this common ground, and investigate, for example, the relationship between Herbrand expansions and the computational interpretations of proofs, or the impact of the epsilon calculus on proof complexity.

Besides the old, but not fully exploited, tools of proof theory, like the epsilon-calculus or Dialectica interpretation, the main tool for our research will be deep inference. Deep inference means that inference rules are allowed to modify formulas deep inside an arbitrary context. This change in the application of inference rules has drastic effects on the most basic proof theoretical properties of the systems, like cut elimination. Thus, much of the early research on deep inference went into reestablishing these fundamental results of logical systems. Now, deep inference is a mature paradigm, and enough theoretical tools are available to think to applications. Deep inference provides new properties, not available in shallow deduction systems, namely full symmetry and atomicity, which open new possibilities at the computing level that we intend to investigate in this project. We intend to investigate the precise relation between deep inference and term rewriting, and hope to develop a general theory of analytic calculi in deep inference. In this way, this project is a natural continuation of the ANR project INFER which ended in May 2010.

7.1.2.2. PHC Procope: From Proofs to Counterexamples for Programming

Participants: Kaustuv Chaudhuri, Nicolas Guenot, Willem Heijltjes, Lutz Straßburger.

Title: From Proofs to Counterexamples for Programming

Duration: 01/01/2012 – 31/12/2013

German Partner: University of Bonn, Institute for Computer Science (Department III)

Finding counterexamples is an endeavor which is as important as proving theorems. But while the latter has seen a huge amount of research effort—we have nowadays a large quantity of tools for automated and interactive theorem proving—the former has mainly been neglegted by proof theorists. One of the reasons is that finding counterexamples or countermodels has been considered a model theoretical activity, rather than a proof theoretical one. Only recently, researchers have begun to explore the well-known duality between "proof search" and "search for countermodels" in a purely proof theoretical way. The main objective of this collaboration is to develop the necessary proof theory for automatically generating such counterexamples in a more general setting.

7.1.2.3. PHC Germaine de Staël: Extending the Realm of the Curry-Howard-Correspondence

Participants: Nicolas Guenot, Willem Heijltjes, Lutz Straßburger.

Title: Extending the Realm of the Curry-Howard-Correspondence

Duration: 01/01/2011 – 31/12/2012

Swiss Partner: University of Bern, Institut für Informatik und angewandte Mathematik (IAM)

The Curry-Howard correspondence between proofs and programs is probably the most interesting and surprising connection between mathematics and computer science. It was discovered in the 1960s, but its main development started in the 1980s. The basis of the correspondence is a correspondence between intuitionistic proofs and typed functional programs (written as terms of lambda-calculus).

Our goal is to develop such a correspondence for new formalisms, like hypersequents, nested sequents and deep inference, in order to better understand their proofs and, we hope, either to discover new programming constructs or to give a new logical interpretation to existing ones.

7.2. International Initiatives

7.2.1. Inria Associate Teams

7.2.1.1. RAPT

Participants: Beniamino Accattoli, Kaustuv Chaudhuri, Quentin Heath, Dale Miller, Yuting Wang.

Title: Applying Recent Advances in Proof Theory for Specification and Reasoning

Inria principal investigator: Kaustuv Chaudhuri

International Partner:

Institution: McGill University (Canada)

Laboratory: School of Computer Science

Researcher: Prof. Brigitte Pientka

International Partner:

Institution: Carnegie Mellon University (United States)

Laboratory: Department of Computer Science

Researcher: Prof. Frank Pfenning

International Partner:

Institution: University of Minnesota (United States)

Laboratory: Department of Computer Science and Engineering

Researcher: Prof. Gopalan Nadathur

Duration: 2011 - 2013

See also: http://www.lix.polytechnique.fr/~kaustuv/rapt/

Many aspects of computation systems, ranging from operational semantics, interaction, and various forms of static analysis, are commonly specified using inference rules, which themselves are formalized as theories in a logical framework. While such a use of logic can yield sophisticated, compact, and elegant specifications, formal reasoning about these logic specifications presents a number of difficulties. The RAPT project will address the problem of reasoning about logic specifications by bringing together three different research teams, combining their backgrounds in type theory, proof theory, and the building of computational logic systems. We plan to develop new methods for specifying computation that allow for a range of specification logics (eg, intuitionistic, linear, ordered) as well as new means to reason inductively and co-inductively with such specifications. New implementations of reasoning systems are planned that use interactive techniques for deep meta-theoretic reasoning and fully automated procedures for a range of useful theorems.

7.2.2. Inria International Partners

7.2.2.1. Eternal: Inria ARC

Participants: Kaustuv Chaudhuri, Dale Miller, Lutz Straßburger.

Title: Interactive Resource Analysis

webpage: http://eternal.cs.unibo.it/

Inria principal investigator: Dale Miller

Inria Partner:

Institution: Inria

Team: FOCUS

Researcher: Ugo Dal Lago

Inria Partner:

Institution: Inria

Team: pi.r2

Researcher: Pierre-Louis Curien

Duration: 2011 - 2013

This project aims at putting together ideas from Implicit Computational Complexity and Interactive Theorem Proving, in order to develop new methodologies for handling quantitative properties related to program resource consumption, like execution time and space. The task of verifying and certifying quantitative properties is undecidable as soon as the considered programming language gets close to a general purpose language. So, full-automatic techniques in general cannot help in classifying programs in a precise way with respect to the amount of resources used and moreover in several cases the programmer will not gain any relevant information on his programs. In particular, this is the case for all the techniques based on the study of structural constraints on the shape of programs, like many of those actually proposed in the field of implicit computational complexity. To overcome these limitations, we aim at combining the ideas developed in the linear logic approach to implicit computational complexity with the ones of interactive theorem proving, getting rid of the intrinsic limitations of the automatic techniques. In the obtained framework, undecidability will be handled through the system's user, who is asked not only to write the code, but also to drive the semi-automatic system in finding a proof for the quantitative properties of interest. In order to reduce the user effort and allow him to focus only on the critical points of the analysis, our framework will integrate implicit computational complexity techniques as automatic decision procedures for particular scenarios. Moreover, in order to be widely applicable, the modularity of the framework will permit to deal with programs written in different languages and to consider different computational resources. The kind of study proposed by this project has been almost neglected so far. Here, we aim at providing such a framework for both theoretic investigations and for testing in practice the effectiveness of the approach.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Brigitte Pientka, Associate Professor, McGill University
February 21 – 24

Gopalan Nadathur, Professor, University of Minnesota
July 10 – 12

Elaine Pimentel, Associate Professor, Universidade Federal de Minas Gerais
June 6 – July 17

Chuck Liang, Professor, Hofstra University
March 6 – May 6 and December 17 – 24

7.3.2. Internships

Yuting WANG (May – August)

Subject: Development of the Abella theorem prover.

Institution: University of Minnesota (United States)

Florence Clerc (March – July)

Subject: Relating double-negation translations and focused proof systems

Institution: Master Parisien de Recherche en Informatique

Zakaria Chihani (April – September)

Subject: Proof certificates for some basic proof systems in classical logic

Institution: Master Parisien de Recherche en Informatique

7.3.3. Visits to International Teams

Stefan Hetzl has visited the Vienna University of Technology four times, for a total of 36 days, within the framework of the FWF/ANR Structural project.

PI.R2 Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

Matthieu Sozeau, Hugo Herbelin, Lourdes del Carmen Gonzalez Huesca and Yann Régis-Gianas are members of the ANR Paral-ITP started November 2011. Paral-ITP is about preparing the Coq and Isabelle interactive theorem provers to a new generation of user interfaces thanks to massive parallelism and incremental type-checking.

Hugo Herbelin is the coordinator of the PPS site for the ANR Récré accepted in 2011, which started in January 2012. Récré is about realisability and rewriting, with applications to proving with side-effects and concurrency.

Matthieu Sozeau is member of the ANR Typex project (Types and certification for XML) and is coordinator of one of the tasks of the project on formalisation and certification of XML tools. The project kicked-off on January 8th, 2012 and is a joint project with LRI, PPS and Inria Grenoble.

7.2. European Initiatives

7.2.1. FP7 Projects

Yann Régis-Gianas is a participant of the EU-FP7 Certified Complexity project (CerCo). This European project started in February 2010 as a collaboration between Bologna university (Asperti, Sacerdoti Coen), Edinburgh university (Stark) and Paris 7 university (Amadio, Régis-Gianas). The CerCo project aims at the construction of a formally verified complexity preserving compiler from a large subset of the C programming language to some typical micro-controller assembly language, of the kind traditionally used in embedded systems. François Bobot's postdoc is funded by this project.

7.2.2. Collaborations in European Programs, except FP7

Hugo Herbelin is participating to a PHC Pavle Savić with the university of Novi Sad in Serbia, the mathematical institute of Belgrade, ENS Lyon and the university of Turin. This project, called TLIT and headed by Silvia Ghilezan on the Serbian side, is about the properties of resource λGtz calculus; subject reduction for the $\overline{\lambda}\mu\widetilde{\mu}$-calculus; explicit substitutions and confluence; the diagrams and termination for ${}^{*}X$ calculus; introducing imperative features in classical logic; the $\lambda\mu$ calculus and its properties; the symmetries in classical logics.

Pierre-Louis Curien, Yves Guiraud and Philippe Malbos are collaborators of the Applied and Computational Algebraic Topology (ACAT) networking programme of the European Science Foundation.

7.3. International Initiatives

7.3.1. Inria Associate Teams

Title: Proof theory and functional programming languages (SEMACODE)

Inria principal investigator: Alexis SAURIN

International Partner:

Institution: University of Oregon (United States)

Laboratory: Computer and Information Science Department

Researcher: Zena ARIOLA

International Partner:

Institution: University of Novi Sad

Laboratory: Faculty of Engineering

Researcher: Silvia GHILEZAN

Duration: 2011 - 2013

See also: http://www.pps.univ-paris-diderot.fr/~saurin/EA-SEMACODE

Activity report: http://www.pps.univ-paris-diderot.fr/~saurin/EA-SEMACODE/en/activite.html

Cross-fertilisation between logic and programming languages theory is at the root of many striking developments in programming concepts as well as tools for formal analysis of programs. Our associated team project aims at gathering senior and young researchers from both sites in order to put a joint research effort on the following research themes: formalising particular evaluation strategies of functional languages based on logical techniques coming from sequent calculi. More specifically, we shall be interested in incorporating control operators directly in call-by-need and in developing a uniform framework for call-by-value and call-by-name calculi with delimited control, in particular to unveil the logical interpretation of delimited control (that is its logical counterpart with respect to Curry-Howard correspondence), and developing connections between delimited control and stream calculi; developing the logical content of realistic abstract machines and associated formal analysis tools for realistic abstract machines building on Curien-Herbelin $\overline{\lambda}$ calculi. The project will gather πr^2 expertise in proof theory and in the logical foundations of functional programming languages, the expertise of the Oregonian group on call-by-need evaluation and delimited control as well as respective crucial inputs of Gaboardi and Ghilezan on stream calculi, delimited control, semantics and type theory. The project will in particular allow to have the Inria and American students and post-docs involved in the project (7 out of 13 people involved) to travel between both sites and to organise joint workshops (one such workshop is planned in June 2011).

7.3.2. PHC

Hugo Herbelin started a PHC STAR with Gyesik Lee and Sungwoo Park in Korea on reverse mathematics and Coq, and on the role that polarisation can play in this respect.

7.3.3. Inria International Partners

πr^2 has strong relations with the following universities: Cambridge (Tim Griffin), Nottingham (Thorsten Altenkirch), Münich (Andreas Abel, Martin Hofmann), Strathclyde (Conor McBride), Chalmers in Göteborg (Thierry Coquand, Peter Dybjer), Technical University in Tallinn (Tarmo Uustalu, Keiko Nakata), Yale University (Zhong Shao), Harvard University (Greg Morrisett).

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Thorsten Altenkirch (University of Nottingham) visited πr^2 for one month April 2012.

Conor McBride (University of Strathclyde) visited πr^2 for three weeks April-May 2012.

Keiko Nakata (University of Tallin) visited πr^2 for 4 days in September and worked with Zena Ariola and Hugo Herbelin on typing the continuation-passing-style semantics of call-by-need λ-calculus.

Tim Griffin visited πr^2 from January to June 2012 (and was funded 3 months by the Inria Paris-Rocquencourt invitation programme). He worked on the formalisation of routing protocols in Coq, and had many exchanges with Coq and ssreflect implementors.

Zena Ariola is visiting πr^2 during the whole academic year 2012-2013. She works on call-by-need, continuation-passing translations and related subjects.

Beta Ziliani (MPI Saarbrücken) visited πr^2 for one week in January 2012 and one week in July 2012 to work with Matthieu Sozeau on formalising the unification algorithm of Coq.

Jael Kriener (University of Kent) visited πr^2 for one week in January 2012 to work with Matthieu Sozeau on proof-search for Type Classes.

7.4.2. Internships

We host Paul Downen (PhD student of Zena Ariola, University of Oregon), during the entire academic year 2012/2013.

7.4.3. Visits to International Teams

Hugo Herbelin and Matthieu Sozeau have spent three months at the IAS as part of the special year on Univalent Foundations (October-December 2012).

7.4.4. Shorter International Visits Abroad

Pierre-Louis Curien visited Zena Ariola (Univ. of Oregon) for 2 weeks in May-June, and Tarmo Uustalu (Institute of Cybernetics of Technical University, Tallinn) for 2 weeks in December.

Hugo Herbelin visited Silvia Ghilezan at the University of Novi Sad in Serbia for one week in January 2012. He visited Predrag Janičić at the University of Belgrade for 2 days. He visited Danko Ilik in Skopje for one week.

Hugo Herbelin visited 4 days Gyesik Lee in Seoul and 3 days Sungwoo Park in Pohang in May as part of their joint project on Reverse Mathematics in Coq.

Guillaume Munch-Maccagnoni also visited Seoul (as part of the PHC STAR programme) 10 days in December.

Matthieu Sozeau was invited by the French Ministry of Foreign Affairs to visit Keiko Nakata and Tarmo Uustalu (IoC, Tallinn) for 4 days in June 2012. He gave a seminar on Equations there.

PROSECCO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. ProSe

Title: ProSe: Security protocols : formal model, computational model, and implementations (ANR VERSO 2010.)

Partners: Inria/Cascade, ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Verimag.

Duration: December 2010 - December 2014.

Coordinator: Bruno Blanchet, Inria (France)

Abstract: The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. CRYSP

Title: CRYSP: A Novel Framework for Collaboratively Building Cryptographically Secure Programs and their Proofs

Type: IDEAS ()

Instrument: ERC Starting Grant (Starting)

Duration: November 2010 - October 2015

Coordinator: Karthikeyan Bhargavan, Inria (France)

Abstract: The goal of this grant is to develop a collaborative specification framework and to build incremental, modular, scalable verification techniques that enable a group of collaborating programmers to build an application and its security proof side-by-side. We propose to validate this framework by developing the first large-scale web application and full-featured cryptographic protocol libraries with formal proofs of security.

8.3. International Initiatives

8.3.1. Inria International Partners

- We work closely with Microsoft Research in Cambridge, Redmond, and Bangalore (C. Fournet, N. Swamy, P. Naldurg)
- We work closely with University of Venice, Italy (R. Foccardi).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Michael May (Faculty Lecturer, Kinneret College on the Sea of Galilee, Israel) visited us for three months as professeur invité.

- Sergio Maffeis (Imperial College, London) visited us as part of an ongoing collaboration.

8.4.1.1. Internships

- Jean Karim Zinzindohoue did his M1 stage with Karthikeyan Bhargavan. He won the "Prix du stage de recherche dit prix d'option" for his work on "Tracking Cryptographically Masked Flows in Android Applications"
- Antoine Delignat-Lavaud did his M2 stage with Karthikeyan Bhargavan on "Security Types for Web Applications"
- Chetan Bansal did a Master's stage with Karthikeyan Bhargavan on "Analysis and Verification of Security for Web Applications"
- Avinash Thummala did a Master's stage with Karthikeyan Bhargavan on "Verifying JavaCard Applets"
- Sneha Popley did a PhD summer internship with Karthikeyan Bhargavan on "Verifying Cryptographic Applications in Java"

8.4.2. Visits to International Teams

- Visits to Imperial College, London: Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Chetan Bansal
- Visits to Microsoft Research, Cambridge: Karthikeyan Bhargavan, Alfredo Pironti
- Visits to University of Birmingham: Ben Smyth, Miriam Paiola

SECSI Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

- DIM Digiteo project RedPill: Malware Detection on Virtualized Architectures, Oct. 2009-Sept. 2012. Sole partner: LSV. Funds Hedi Benzina's PhD Thesis.
- DIM Digiteo project API: Automated Proofs of Indistinguishability, 2010-2013. Partners: EPI SECSI, EPI CASCADE. Oct. 2010-Sept. 2013. Funds Vincent Cheval's PhD Thesis.

7.2. National Initiatives

7.2.1. ANR

- ANR programme blanc CPP ("Confidence, Probability, and Proofs"), 2009-2012. Partners: LSV (scientific leader), CEA LIST (co-leader), Inria (Comète, Parsifal), Ecole Supérieure d'Electricité (L2S, SSE). External partners: Safran, Dassault Systèmes.

  In the context of proofs of safety properties for critical software, The CPP project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs. See http://www.lix.polytechnique.fr/~bouissou/cpp/index.php.
- ANR SeSur ("Sécurité et Sûreté Informatique") project AVOTÉ, 2008-2012. Partners: Inria (Cassis, leader), LSV, Verimag and, until September 2009 France Télécom R&D.

  Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. The AVOTÉ project aims at proposing formal methods to analyze electronic voting protocols. See http://www.lsv.ens-cachan.fr/anr-avote/.
- ANR VERSO program ProSe ("Proofs of Security"), 2010-2014. Partners: Inria (Cascade, leader; Cassis), LSV, Verimag.

  The goal of the ProSe project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the *symbolic* level, in which messages are terms; the *computational* level, in which messages are bitstrings; and the *implementation* level: the program itself. This project is a continuation of the FormaCrypt project. See https://crypto.di.ens.fr/projects:prose:main.
- ANR JCJC project VIP, 2012-2015. Awarded to Stéphanie Delaune.

  The aim of this project is to formally analyze modern applications in which privacy plays an important role. Many applications having an important societal impact are concerned by privacy, e.g. electronic voting, electronic auction protocols, RFID tags, safety critical application in vehicular ad hoc networks, routing protocols in mobile ad hoc networks, etc. Moreover, each application comes with its own specificities. E.g. e-voting protocols often rely on complex cryptographic primitives, some routing protocols rely on recursive tests, and so on. In mobile ad hoc networks, taking into account mobility issues is also an important challenge.

  Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. However, nearly all studies focus on trace-based security properties, and thus to not allow one to analyse privacy-type properties that play an important role in many modern applications. Moreover, the envisioned applications have some specificities that prevent them to be modelled in an accurate way with existing verification tools.

The goal of this project is to design verification algorithms to analyse privacy-type properties on several applications having an important societal impact. The project is accompanied by an effort in case studies and application domains which will allow at the end of the project an assessment of the pragmatic potential both in terms of modelling and effective analysis. More details are available on the web page of the project: http://www.lsv.ens-cachan.fr/Projects/anr-vip/.

7.3. International Initiatives

7.3.1. Participation In International Programs

- Inria Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society). Member: Stéphanie Delaune.

  The goal of CAPPRIS is to provide solutions to enhance the privacy protection in the Information Society. The tageted applications are Online Social Networks, Location Based Services, and Electronic Health Record Systems.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Myrto Arapinis, April 2012 (1 week) and in December 2012 (1 week).
- Alwen Tiu, December 2012 (1 week).

7.4.1.1. Internships

Umang MATHUR (from May 2012 until Jul 2012)

Subject: Estimating the information leakage of a recursive probabilistic program

Institution: IIT Bombay (India)

TASC Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

1. The goal of Ligéro is to create an internationally visible regional research group putting together the key actors in the domain of Operations Research in the Pays de la Loire region.
2. A regional grant from the Région Pays de la Loire for inviting in Nantes a senior researcher was obtained end of 2012 (6 months in 2013 and 2014 for Helmut Simonis) on *learning generic constraint models*.

8.2. National Initiatives

1. Cooperation with J.-C. Régin from Univ. Nice on efficient graph filtering algorithms.
2. Cooperation with A. Miné from ENS Paris on abstract domains by M. Pelleau and C. Truchet.

8.3. European Initiatives

8.3.1. Collaborations with Major European Organizations

SICS, Computer Systems Laboratory (Sweden)
Global Contraint Catalog, scalable global constraints.
4C, (Ireland)
Learning constraint models.
Uppsala University, (Sweden)
Automata and constraints.

8.4. International Initiatives

8.4.1. Inria International Partners

- SICS, Sweden: Work on the *global constraint catalog* and on *scalable constraints* with Mats Carlsson.
- Uppsala University, Sweden: Work on automata and dedicated filtering algorithms for some constraint patterns with the ASTRA group of Pierre Flener.
- École Polytechnique de Montreal, Canada: Work on graph constraints with Louis Martin Rousseau.
- JFLI, Japan: Work with Philippe Codognet.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Helmut Simonis (4C): work on model learning and work on learning constraints in the context of EDF, one month.

8.5.1.1. Internships

- Naina Razakarison (internship of ENS Cachan in summer 2012 on learning generic models).
- Mohamed Kebe (internship of Clermont University in summer 2012 on reformulations of the *cumulative* constraint).

8.5.2. Visits to International Teams

- N. Beldiceanu, 4C Cork Ireland: work on *learning generic models* and work on *learning constraints in the context of EDF* with H. Simonis.
- N. Beldiceanu, Uppsala University and SICS: work on *automata and constraints* with P. Flener and J. Pearson and on *learning generic models* with M. Carlsson.

TOCCATA Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Hisseo

Participants: Sylvie Boldo [contact], Claude Marché, Guillaume Melquiond, Thi-Minh-Tuyen Nguyen.

Hisseo is a 3 and half year Digiteo project that started in September 2008 and ended in June 2012. http://hisseo.saclay.inria.fr

The Hisseo project focuses on the problems related to the treatment of floating-point computations in the compilation process, especially in the case of the compilation of critical C code [12], [46].

Partners: CEA List (Saclay), Inria Paris-Rocquencourt (Team Gallium).

8.1.2. Coquelicot

Participants: Sylvie Boldo [contact], Catherine Lelay, Guillaume Melquiond.

Coquelicot is a 3 years Digiteo project that started in September 2011. http://coquelicot.saclay.inria.fr. S. Boldo is the principal investigator of this project.

The Coquelicot project aims at creating a modern formalization of the real numbers in Coq, with a focus on practicality [30], [22]. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

Partners: LIX (Palaiseau), University Paris 13

8.1.3. Pactole

Participants: Évelyne Contejean [contact], Jean-Christophe Filliâtre.

Pactole is a 3 year Digiteo project which started in October 2009.

The Pactole project focuses on automation and formal verification for ubiquitous, large scale environments. Tasks include proof automation techniques for distributed systems, verification conditions for fault tolerant distributed systems, specification and design of fundamental services for mobile sensor networks. The principal investigator of Pactole is Xavier Urbain.

Partners: CÉDRIC (CNAM/ENSIIE), LIP6 (UPMC).

8.2. National Initiatives

8.2.1. ANR BWare

Participants: Sylvain Conchon, Évelyne Contejean, Jean-Christophe Filliâtre, Andrei Paskevich, Claude Marché.

This is a research project funded by the programme “Ingénierie Numérique & Sécurité” of the ANR. It is funded for a period of 4 years and started on September 1, 2012. http://bware.lri.fr.

It is an industrial research project that aims to provide a mechanized framework to support the automated verification of proof obligations coming from the development of industrial applications using the B method and requiring high guarantees of confidence. The methodology used in this project consists in building a generic platform of verification relying on different theorem provers, such as first-order provers and SMT solvers. The variety of these theorem provers aims at allowing a wide panel of proof obligations to be automatically verified by the platform. The major part of the verification tools used in BWare have already been involved in some experiments, which have consisted in verifying proof obligations or proof rules coming from industrial applications [29]. This therefore should be a driving factor to reduce the risks of the project, which can then focus on the design of several extensions of the verification tools to deal with a larger amount of proof obligations.

The partners are: Cedric laboratory at CNAM (CPR Team, project leader) ; Inria teams Gallium, Deducteam and Asap ; Mitsubishi Electric R&D Centre Europe, the ClearSy company that mdevelop and maintains *Atelier B* and the OCamlPro start-up.

8.2.2. ANR DECERT

Participants: Sylvain Conchon, Évelyne Contejean.

DECERT (DEduction and CERTification) is an ANR "Domaines Emergents" project. It started on January 2009 for 3 years; the coordinator is Thomas Jensen from the Lande team of IRISA/Inria Rennes.

The goal of the project DECERT is to design and implement new efficient cooperating decision procedures (in particular for fragments of arithmetics), to standardize output interfaces based on certificates proof objects and to integrate SMT provers with skeptical proof assistants and larger verification contexts such as the Rodin tool for B and the Frama-C/Jessie tool chain for verifying C programs.

The partners are: CEA List, LORIA/Inria Nancy - Grand Est, IRISA/Inria Rennes - Bretagne Atlantique, Inria Sophia Antipolis - Méditerranée, Systerel

8.2.3. ANR FOST

Participants: Sylvie Boldo [contact], Jean-Christophe Filliâtre, Guillaume Melquiond.

FOST (Formal prOofs of Scientific compuTation programs) is a 3 years ANR "Blanc" project started in January 2009 and ended in April 2012. S. Boldo is the principal investigator of this project. http://fost.saclay.inria.fr

The FOST project follows CerPAN's footprints as it aims at developing new methods to bound the global error of a numerical program. These methods will be very generic in order to prove a large range of numerical analysis programs. Moreover, FOST aims at providing reusable methods that are understandable by non-specialists of formal methods.

Partners: University Paris 13, Inria Paris - Rocquencourt (Estime).

8.2.4. ANR U3CAT

Participants: Jean-Christophe Filliâtre, Claude Marché [contact], Guillaume Melquiond, Asma Tafat, Paolo Herms.

U3CAT (Unification of Critical C Code Analysis Techniques) is a project funded by ANR within its programme "Systèmes Embarqués et Grandes Infrastructures - ARPEGE". It aims at verification techniques of C programs, and is partly a follow-up of the former CAT project. It started in January 2009 and ended in August 2012.

The main goal of the project is to integrate various analysis techniques in a single framework, and make them cooperate in a sound way. We address the following general issues:

- Verification techniques for floating-point programs;
- Specification and verification of dynamic or temporal properties;
- Combination of static analysis techniques;
- Management of verification sessions and activities;
- Certification of the tools chains for compilation and for verification.

Partners: CEA-List (Saclay, project leader), Lande team (Inria Rennes), Gallium team (Inria Rocquencourt), Dassault Aviation (Saint-Cloud), Airbus France (Toulouse), ATOS Origin (Toulouse), CNAM Cedric laboratory (Evry), CS Communication & Systems (Toulouse), Hispano-Suiza/Safran (Moissy-Cramayel).

8.2.5. ANR Verasco

Participants: Guillaume Melquiond [contact], Sylvie Boldo, Arthur Charguéraud, Claude Marché.

This is a research project funded by the programme “Ingénierie Numérique & Sécurité” of the ANR. It is funded for a period of 4 years and started on January 1st, 2012. http://verasco.imag.fr

The main goal of the project is to investigate the formal verification of static analyzers and of compilers, two families of tools that play a crucial role in the development and validation of critical embedded software. More precisely, the project aims at developing a generic static analyzer based on abstract interpretation for the C language, along with a number of advanced abstract domains and domain combination operators, and prove the soundness of this analyzer using the *Coq* proof assistant. Likewise, it will keep working on the CompCert C formally-verified compiler, the first realistic C compiler that has been mechanically proved to be free of miscompilation, and carry it to the point where it could be used in the critical software industry.

Partners: teams Gallium and Abstraction (Inria Paris-Rocquencourt), Airbus avionics and simulation (Toulouse), IRISA (Rennes), Verimag (Grenoble).

8.2.6. Systematic: Hi-Lite

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Sylvain Conchon, Évelyne Contejean, Andrei Paskevich, Alain Mebsout, Mohamed Iguernelala, Denis Cousineau.

The Hi-Lite project (http://www.open-do.org/projects/hi-lite/) is a project in the SYSTEMATIC Paris Region French cluster in complex systems design and management http://www.systematic-paris-region.org.

Hi-Lite is a project aiming at popularizing formal methods for the development of high-integrity software. It targets ease of adoption through a loose integration of formal proofs with testing and static analysis, that allows combining techniques around a common expression of specifications. Its technical focus is on modularity, that allows a divide-and-conquer approach to large software systems, as well as an early adoption by all programmers in the software life cycle.

Our involvements in that project include the use of the Alt-Ergo prover as back-end to already existing tools for SPARK/ADA, and the design of a verification chain for an extended SPARK/ADA language to verification conditions, via the *Why* VC generator.

This project is funded by the french ministry of industry (FUI), the Île-de-France region and the Essonne general council for 36 months from September 2010.

8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7

8.3.1.1. FoVeOOS

Participants: Claude Marché [contact], François Bobot, Asma Tafat.

Program: COST (European Cooperation in the field of Scientific and Technical Research, http://www.cost.esf.org/)

Project acronym: FoVeOOS (IC-0701, http://www.cost-ic0701.org/)

Project title: Formal Verification of Object-Oriented Software

Duration: May 2008 - April 2012

Coordinator: B. Beckert, University Karlsruhe, Germany

Other partners: 40 academic groups among 18 countries in Belgium, Denmark, Estonia, France, Germany, Ireland, Israel, Italy, The Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland and United Kingdom.

Abstract: The aim of this action is to develop verification technology with the reach and power to assure dependability of object-oriented programs on industrial scale.

8.4. International Initiatives

8.4.1. Participation In International Programs

- C. Paulin is the representative of Univ. Paris-Sud for the education part of the EIT KIC ICT Labs. She contributed to the proposition of two master programs as well as the action on weaving Innovation and Entrepreneurship in Doctoral programs and the preparation of the Summer School “Imagine the future in ICT”.

8.4.2. Other International Partners

- S. Conchon has continued his collaboration with S. Krstic and A. Goel (Intel Strategic Cad Labs in Hillsboro, OR, USA) on the development of the Cubicle SMT-based model checker [24].
- J.-C. Filliâtre has collaboration with University do Minho (Braga, Portugal) on the use of *Why* as intermediate for verification of cryptographic programs [13].
- J.-C. Filliâtre has collaboration with Universidade da Beira Interior (Covilhã, Portugal) on the use of *Why* as intermediate for verification of ARM programs [34].
- Our on-going development of a verified JavaScript interpreter, described above, is an active collaboration with people from Imperial College, London, UK.

8.5. International Research Visitors

8.5.1. Visits to International Teams

- S. Conchon visited Intel Strategic Cad Labs during summer 2012.
- J.C. Filliâtre visited SRI (Menlo Park, California, USA) during summer 2012.

TYPICAL Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

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

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

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

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

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. FORMATH

Title: Formath

Type: COOPERATION (ICT)

Defi: FET Open

Instrument: Specific Targeted Research Project (STREP)

Duration: March 2010 - February 2013

Coordinator: Univ Götegorg (Sweden)

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

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

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

VERIDIS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

Participants: Pascal Fontaine, Stephan Merz.

The DeCert (Deduction and Certification) project has been funded by ANR from 2009 to 2012 within its "Domaines émergents" program. It was coordinated by the Celtique project team of Inria Rennes, the other partners are academic teams from Inria Saclay (Proval) and Inria Sophia Antipolis (Marelle) as well as the CEA and the Systerel company. In Nancy, the project also involves members of the Cassis team, in particular Alain Giorgetti and Christophe Ringeissen.

The objective of the project has been to study certified decision procedures, including the design of appropriate certificates, the development of new certifying decision procedures, their combination, their integration with skeptical proof assistants such as Coq or Isabelle, and their use in application domains such as software verification or static analysis. The main lines of research concern questions of expressiveness vs. efficiency, certificates vs. proof objects, and the integration of certificates into verification environments. Our work within the project is related to veriT (see section 5.1), its proof production, and its integration with verification environments such as Isabelle or the TLA$^+$ proof environments (see section 5.2).

8.1.2. Inria Development Action VeriT

Participants: Pablo Federico Dobal, Pascal Fontaine.

Inria funds this project (started in 2011) for the future development of the SMT solver veriT (see section 5.1), including added expressiveness, improved efficiency and code stability, and interfaces with tools that embed veriT as a backend solver. The project is coordinated by Pascal Fontaine and also includes Inria Rennes (Celtique) and Sophia Antipolis (Marelle). Federico Dobal has been hired in 2012 on a position funded by this project and has in particular contributed to improvements in the code of the solver as well as of the testing platform that allows us to detect bugs and the impact of changes on the performance of the tool.

8.2. European Initiatives

8.2.1. Cooperation with TU Wien, Austria

Participants: Pascal Fontaine, Stephan Merz.

This project started in 2012 and fosters bilateral cooperation with the team headed by Prof. Alexander Leitsch at TU Vienna. It focuses on aspects of proof production and proof compression in automated reasoning. It is headed by Bruno Woltzenlogel Paleo of TU Wien, who was formerly a post-doctoral researcher in VeriDis until March 2011, and Pascal Fontaine. The project is funded by the Amadeus Programme of the Partenariat Hubert Curien and the Österreichischer Austausch Dienst.

A first workshop of one week took place in Vienna in spring, and gathered around 15 people, including Pascal Fontaine and Stephan Merz as well as a student from TU Graz. A second one-week workshop was organized in Nancy in the fall, with 12 participants including 5 researchers from Vienna, and one student from Univ. Paul Sabatier, Toulouse. The web page gives more information on this project.

8.3. International Initiatives

8.3.1. Participation In International Programs

8.3.1.1. Cooperation with Córdoba, Argentina

Participants: Pascal Fontaine, Stephan Merz.

This cooperation with the team of Carlos Areces (formerly a researcher at Inria Nancy) at the University of Córdoba is along two axes. First, we study symmetries for automated reasoning (and SMT) as a means to reduce the search space and improve efficiency. Second, we investigate automated reasoning techniques (and more specifically SMT) for modal logics and similar fragments of first-order logic. The cooperation is funded within the context of the IRSES project MEALS coordinated for Inria by Catuscia Palamidessi (Saclay).

Two PhD students from Córdoba visited Inria Nancy in Summer 2012: Ezequiel Orbe for two weeks, and Raul Fervari for one month. Carlos Areces also came to Nancy for two weeks. Pascal Fontaine and Stephan Merz visited Argentina in November where they spent two weeks in Córdoba working on the above subjects, and one week visiting our contacts at the universities of Rosario and Buenos Aires.

The team has a long term relationship with the Universities of Córdoba, Rosario and Buenos Aires, with frequent exchanges of students. One Internship student in 2012 was from Buenos Aires, and the newly recruited engineer is from Rosario.

8.3.1.2. Cooperation with Universidade Federal do Rio Grande de Norte, Brazil

Participants: David Déharbe, Pablo Federico Dobal, Pascal Fontaine, Stephan Merz.

VeriDis has a close working relationship with a team at Universidade Federal do Rio Grande de Norte (UFRN), Brazil, and more particularly with Prof. David Déharbe. David Déharbe visited VeriDis in July and October. Pascal Fontaine is scheduled to visit Natal in early 2013. The project is centered around the development and applications of the veriT solver (section 5.1), of which David Déharbe and Pascal Fontaine are the main developers. Our cooperation is also supported by the Inria-CNPq project SMT-SAVeS from 2010 throughout early 2013.

8.3.1.3. Cooperation with Tiaret University

Participants: Dominique Méry, Stephan Merz.

Mostapha Belardi (Université Ibn Khaldoun de Tiaret), Camel Tanougast (LICM, Université de Lorraine), Dominique Méry and Stephan Merz have started a joint project entitled *CIPRONoC : Conception Incrémentale Prouvée pour pROtotypage rapide de NoC Tolérant aux Fautes à base de technologie FPGA*. The project is sponsored by the STIC Algérie program, which funded a visit of Mostapha Belardi and an internship of Hayat Daoud in 2012. The work led to the design of a model for a network on chip proposed by our partners from LICM. A short presentation has been published in a local workshop.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

David Déharbe from Universidade Federal do Rio Grande de Norte, Brazil, visited VeriDis from July 9 to July 27 and from October 15 to October 26 in the context of the Inria-CNPq project SMT-SAVeS. The work resulted in several improvements of the veriT solver.

Thomas Sturm, from MPI für Informatik, and Ulrich Loup and Florian Corzilius, from RWTH Aachen, visited VeriDis from October 22nd to 26th, in the context of the ADT veriT for discussing techniques for non-linear arithmetic in SMT solving.

8.4.2. International Internships

- Rodrigo Castaño (from Sep 2012 until Dec 2012)
  - Subject: Methods for efficient SMT solving
  - Institution: University of Buenos Aires (Argentina)