

1/ Toccata

Toccata

**Deductive Verification, Certified Tools
and Numerical Computations**

Research Group Members

Permanent Members (June 30th, 2013)			
Name	First name	Position *	Institution
BENZAKEN	Véronique	PREX	PARIS SUD
BOLDO	Sylvie	CR1	Inria
CHARGUÉRAUD	Arthur	CR2	Inria
CONCHON	Sylvain	MCF	PARIS SUD
CONTEJEAN	Évelyne	CR1	CNRS
FILLIÀTRE	Jean-Christophe	CR1	CNRS
MANDEL	Louis	MCF	PARIS SUD
MARCHÉ	Claude	DR2	Inria
MELQUIOND	Guillaume	CR1	Inria
NGUYEN	Kim	MCF	PARIS SUD
PASKEVICH	Andrei	MCF	PARIS SUD
PAULIN-MOHRING	Christine	PR1	PARIS SUD

Doctoral Students (June 30th, 2013)			
Name	First name	Funding	Institution
DROSS	Claire	CIFRE	AdaCore
DUMBRAVA	Stefania	AM	PARIS SUD
IGUERNELALA	Mohamed	ATER	PARIS SUD
LELAY	Catherine	Digitéo grant	Inria
MEBSOUT	Alain	AM	PARIS SUD
TAFAT-BOUZID	Asma	ATER	PARIS SUD

Temporary Personnel** (2008-2013)					
Name	First name	Position *	Institution	Arrival	Departure
AYAD	Ali	Post-doc	Inria	09.2008	01.2009
BAELDE	David	Post-doc	CNRS	09.2010	12.2011
COUSINEAU	Denis	Post-doc	Inria	10.2011	09.2012
IM	Hyeonseung	Post-doc	PARIS SUD	11.2012	2014
KRISHNAMANI	Kalyan	Post-doc	Inria	09.2009	08.2011
MAKAROV	Evgeny	Post-doc	Inria	05.2011	10.2011
OUDOT	Aurélien	Engineer	Inria	09.2006	08.2008
ROUX	Cody	Post-doc	Inria	05.2011	06.2012
RÉGIS-GIANAS	Yann	Post-doc	Inria	10.2007	09.2008
STOULS	Nicolas	Engineer	Inria	10.2007	09.2008

Visitors for 3 months or more (2008-2013)					
Name	First name	Position *	Institution	Arrival	Departure
COURTIEU	Pierre	CRCT	CNAM, CEDRIC laboratory	10.2012	03.2013
ISHII	Daisuke	invited re-searcher	National Institute of Informatics, Japan	05.2011	12.2011
VIEIRA	Bárbara	PhD student	Universidade do Minho, Portugal	03.2009	05.2009

** past and current PhD students are listed in Section Thesis

Group evolution

In Nov. 2008, G. Melquiond was hired as CR Inria, strengthening our axis on floating-point program analysis. In Sep. 2009, A. Paskevich was hired as Maitre de Conférences, bringing new competences both on

automated deduction and program verification. In Mar. 2010, M. Pouzet left the team and went to É.N.S. Paris, consequently the axis on synchronous programming from our research programme got thinner. V. Benzaken joined the team in Sep. 2010, moving from the LRI “BD” team, bringing a new competence on programming languages and advanced type systems for databases. K. Nguyen was hired as Maître de Conférences at the same time, to support this new axis. L. Puel left the team in Sep. 2012, when she retired. A. Charguéraud was hired as CR Inria in Sep. 2012, bringing new competences on several aspects: verification of higher-order imperative programs, formalization of programming languages and verification of concurrent programs.

1/ Toccata

Research Description

Safety-critical software applications appear in various domains like transportation, telecommunication, banking, health services. In such contexts, a high assurance in the reliability of software is required. The general objective of the team is to promote the use of formal methods to provide such a level of assurance.

Deductive methods, that are based on computer-assisted theorem proving are central in the approaches we propose. We characterize ourselves by the will to consider both theory and practice. We develop a significant amount of software, that are distributed as open source, and used in external applications.

Below we describe our research programme, structured into six activities. For each of them, we present an overview and then detail a few important results obtained since 2008.

Activity 1: Formally Verified Programs

The use of automated theorem proving to statically check that a program respects a formal specification is an old idea originating from Floyd and Hoare in the early 1970s. Yet, it is only quite recently that some concrete achievements were obtained using deduction-based verification. One of the first example, around 1998, is the development of critical software embedded on driver-free trains like Paris metro line 14, using the *Atelier B* system. Other success stories of that kind happened since 2000, such as the *L4-verified* project developing a formally verified micro-kernel with high security guarantees, using analysis tools on top of the Isabelle/HOL proof assistant.

The first activity of our team is centered on deductive program verification. We develop several tools which interact with each other and with other external tools, as illustrated on Figure 1.1. The tools in pink boxes are designed by us, while those in blue boxes are designed by partners. The central tool is Why3 (103, 26), which includes both a Verification Condition generator and a set of encoders and printers. The VC generator reads source programs in a dedicated input language that includes both specifications and code. It produces verification conditions that are encoded and printed into various formats and syntax so that a large set of interactive or automatic provers can be used to discharge the verification conditions. As front-ends, our tool Krakatoa (134) reads annotated Java source code and produces Why3 code. The tool Jessie (146, 16) is a plug-in for the Frama-C environment (which we designed in collaboration with CEA-List); it does the same for annotated C code. The GnatProve tool is a prototype developed by AdaCore company; it reads annotated Ada code and also produces Why3 code. Last but not least, the modeling of programs semantics and the specification of their expected behaviors is based on some libraries of mathematical theories that we develop, either in the logic language of Why3 or in Coq. These are the yellow boxes of the diagram.

Environments for Deductive Verification The development of our tools and environments leads to publications, typically tool descriptions. We published the original concepts behind the Why3 logic language, where logic theories are structured and reused (103), our proof sessions system for maintaining proofs when specifications evolve (52), and the description of the WhyML intermediate language for both programming and proving (55). Why3 is used as an intermediate language by several other tools in the world. An evidence of its impact is the number of invited conferences that we gave to present it (25, 26, 27, 28, 29).

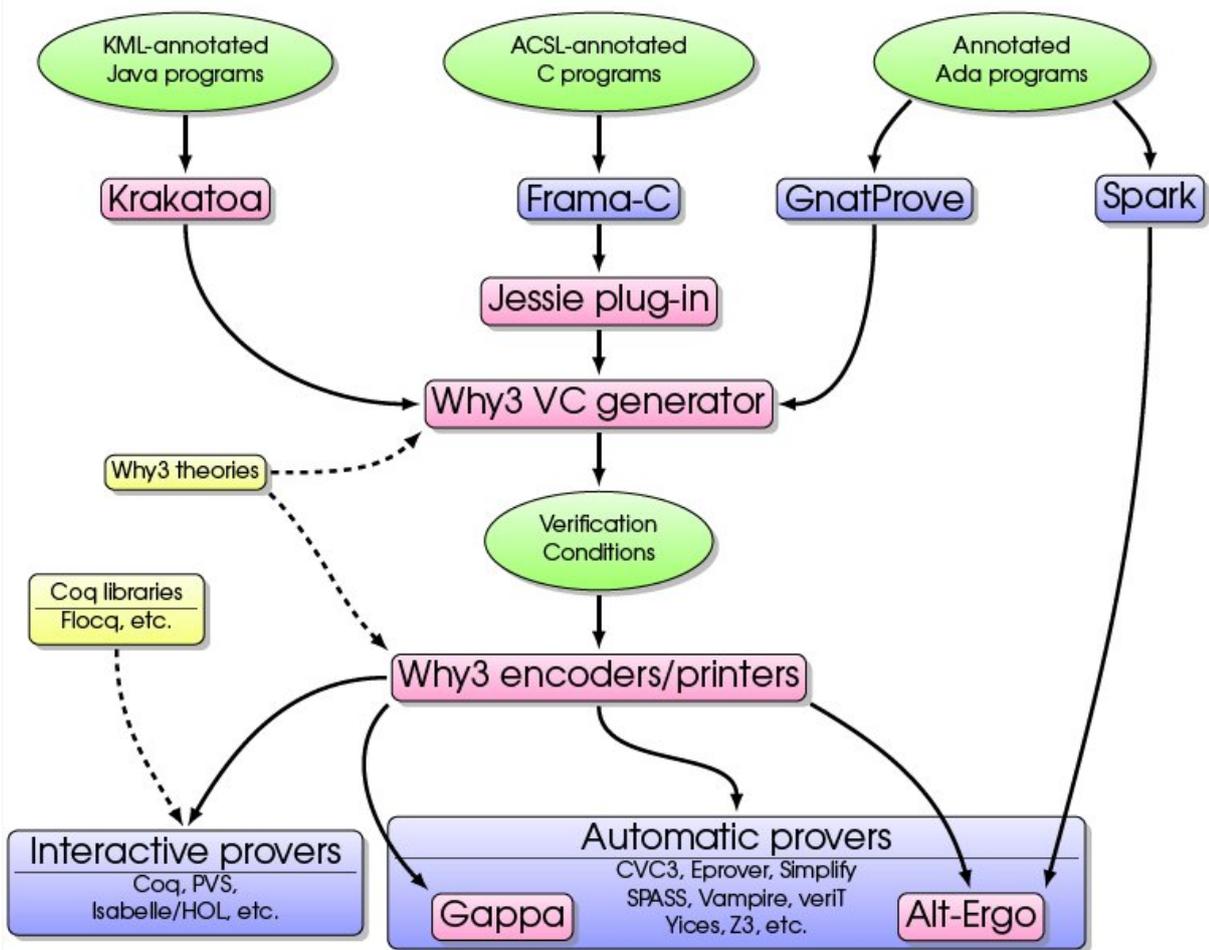


Figure 1.1: Interactions between our tools and with others

Memory models, Modularity, Reusability An important part of this activity is the design of suitable formal models of the semantics of programs. Regarding models for pointer programs underlying the front-ends for C and Java, we proposed models based on fine-grained representations of the heap memory, based on regions and permissions (114). We proposed an approach for specifying pointer programs inspired from Separation Logic but still making use of classical first order logic (51). On top of a representation using regions, we proposed a new approach for refinement of pointer programs (99), allowing for a more modular reasoning and the reusability of components, which is a key requirement. Still regarding reusability, we proposed new constructs for specifying generic components (97).

We also investigated the issues related to the combination of higher-order programs and side-effects (107, 187).

Inference of contracts A general drawback of deductive verification is the need to provide formal specifications to each functions of the code, under the form of a contract, and each loop, under the form of loop invariants. We investigated the possibility of generating parts of such contract automatically, either by abstract interpretation techniques (73, 16, 197) or by predicate abstraction (168).

Case studies and Applications To emphasize the usability of our tools, one first method is to publish representative case studies. For example, we published some solutions to the VACID-0 challenges (<http://vacid.codeplex.com/>): sparse arrays (85), binary heaps (157). Others published case studies a C code for computing solutions to the n -queens problem (54), and containers of Ada (44). All our case studies are available on a so-called “gallery of verified programs” on our web page (<http://toccata.lri.fr/gallery/index.en.html>). Another mean to publicize our tools is to participate to the verification competitions, which have been organized since 2010 (91). We even organized the competition affiliated to VSTTE’2012 (105).

Concerning applications, apart from the use of Why3 as intermediate language in Frama-C and in

Spark2013, we can mention applications to cryptography, either by directly using Why3 (89, 1), or again using why3 as intermediate language by the EasyCrypt project (<http://www.easycrypt.info/>). We have also investigated the verification of assembly code, such as ARM programs (96).

Hybrid systems The deductive approach is not limited to programs. We have also extended it to verifying the safety of hybrid automata, that is, systems comprised of discrete states and continuous transitions. The idea is to handle such systems as if they were programs, to infer loop invariants, and to prove the resulting verification conditions (40).

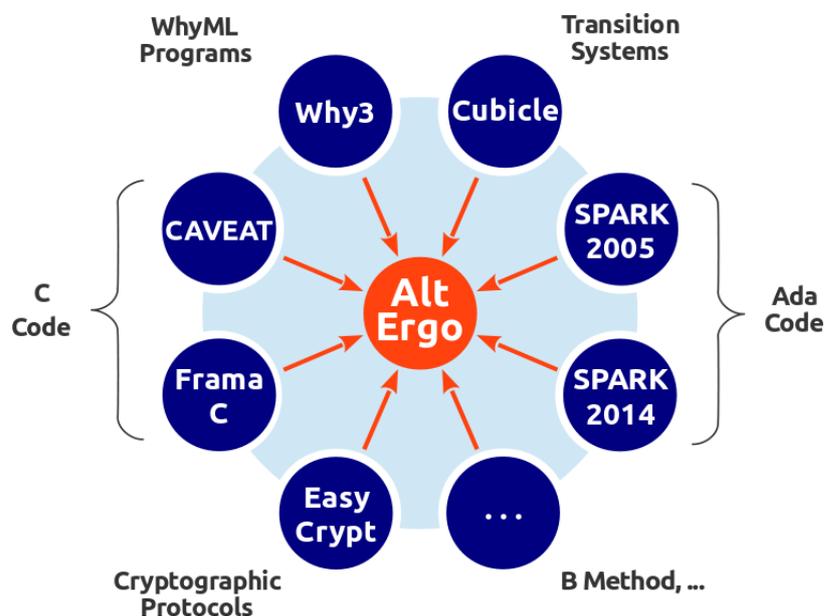
Activity 2: Automated Deduction

Automated theorem provers play a central role in the verification field. As shown in the previous section (Activity 1), provers like Alt-Ergo or Gappa are used in the Why3 plate-form to discharge verification conditions automatically. Theorem provers are also used as back-ends in other tools like testing tools, model-checkers etc. As a consequence, improving the efficiency and expressiveness of automatic provers has a strong impact in the all field of computer-aided verification.

The Toccata team has a long historical background on automated deduction. Starting from rewriting techniques in the 90's, it has evolved towards the Satisfiability Modulo Theory (SMT) paradigm in the mid-2000s in order to prove logical formulas generated by program verification toolboxes (see Activity 1). Along all these years, Toccata (formerly Démons and ProVal) has always associated theory to practice by implementing state-of-the-art automated deduction tools: the CiME rewriting toolbox, the SMT solver Alt-Ergo, etc. This list has been completed during the report period with the Gappa prover, developed by G. Melquiond who joined our team in 2008.

Proving Termination Since the last decade, a great deal of attention has been given to termination in the rewriting community, and since some termination tools were found faulty during termination tools' competitions, producing *certificates* of termination became a challenging domain. Coccinelle (92) is a formal Coq library which models universel algebras, term rewriting, various term orderings, and termination criteria. Formally proving paper and pencil known theorems allows to remove irrelevant hypothesis, and to propose some new, more general, termination criteria (49). Coccinelle has been used in combination with the CiME rewriting tool box in order to produce concrete termination certificates for a large set of rewriting systems coming from the termination problem database (48).

SMT Solvers. Among automated provers, our tool Alt-Ergo (176) is an SMT solver that is able to deal with quantifiers, arithmetic in integers or real numbers, and a few other theories. Its main originality is to handle, without encoding, polymorphic first-order formulas (104). As shown by the following picture, Alt-Ergo is used as a back-end of numerous verification plate-forms.



Decision procedures for specific theories. We worked on several theories in order to improve the efficiency and expressiveness of Alt-Ergo. For instance, we have developed an efficient algorithm for combining the free theory of equality with Shostak theories (115). We designed a new decision procedure to natively handle associative and commutative symbols found, for instance, in models of finite sets (63, 64, 9). We proposed an original extension of the simplex algorithm for linear integer formulas (53). We started to work on the treatment of floating-point numbers in Alt-Ergo. For that purpose, we designed a decision procedure based on the approach of the Gappa tool (116). Finally, we also proposed a framework to reason about triggers, the main mechanism used by SMT solvers to handle quantifiers (100).

Encoding schemes for polymorphic logics. The ML-like polymorphism of Why3's logic requires a subtle translation scheme to external prover logics. In (50) we have proposed a new approach for encoding polymorphic theories into monomorphic ones. In order to further the TPTP community to polymorphism, we have proposed an extension of the TFF0 syntax with rank-1 polymorphism (33).

Model-checking. In collaboration with the Strategic Cad Lab at Intel, we develop Cubicle (SP-2), a model checker for verifying safety properties of parameterized systems. Cubicle implements the Model Checking Modulo Theory (MCMT) framework and it is written on top of Alt-Ergo.

Benchmarks and applications. We are concerned by the effectiveness of our automatic deduction tools. In order to measure their efficiency, we conduct experiments on a large number of benchmarks, including industrial case studies (95).

Activity 3: Certified Tools and Libraries

An emerging trend in formal verification methods is the verification of the analysis tools themselves, as exemplified by the CompCert verified compiler. We have conducted several studies in this direction in the past, that we detail below. We are not interested in verifying standalone tools, but also in the design of verified reusable libraries, in particular on top of the Coq proof assistant.

Certified Mathematical Libraries A first category of libraries that we design on top of Coq aims at formalizing mathematical concepts. First, we developed several formalizations of floating-point arithmetic. This started with the PFF library (<http://lipforge.ens-lyon.fr/www/pff/>). An alternative independent library is the one used by the Gappa prover to produce Coq certificates (3). Both are now subsumed by our Floccq library (70).

We also designed the Coquelicot library (<http://coquelicot.saclay.inria.fr/>), an extension of the Coq standard library for reals. It is a user-friendly library for real analysis with an easier way of writing formulas and theorem statements, a comprehensive set of theorems and some automations (74, 119).

We also formalized in Coq mathematical concepts around probability theory, this is provided by the Alea library (2). This formalization is the basis for reasoning on randomized algorithms. Alea is notably used by the CertiCrypt environment (<http://certicrypt.gforge.inria.fr/>) for the certification of cryptographic codes. Unlike the majority of approaches of verification of cryptographic protocols, CertiCrypt relies on a concrete randomized programming language, which permits to model attacks at the code level and not only at the protocol level.

Formalized Semantics Formalization of the semantics of languages is also typically done using Coq. We designed the Coccinelle library (92) to formalize term rewriting systems. It is used for the construction of Coq certificates by automated termination tools (49). It can be used to build proof certificates for other properties of term rewriting systems (48). An application is the formalization of high-level properties of distributed algorithms, as studied in the Pactole project.

Concerning semantics in general, we proposed the new concept of "Pretty-big-step" semantics (43), intermediate between small-steps and big-steps ones. We have shown that it is not mandatory to use a prover as expressive as Coq to formalize semantics: the Why3 language is expressive enough, and allows a much higher degree of automation in the proofs (75).

Functional Programming We have worked on the design of several functional programming libraries, mainly using the OCaml language. Although a bit aside from the main research topics of the team,

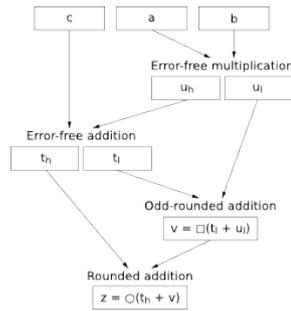


Figure 1.2: Emulating the FMA.

this topic is very important for us in term of impact. We present a general view of *Semi-persistent data-structures* (65) which permit to program efficient data structures while keeping a purely functional interface for them. Such an efficient data structures is the structure of ropes (77).

We designed OCaml libraries for graphs (117), for map-reduce style distributed programming (76, 106), for solving combinatoric problems (78). We also developed and distribute programming tools like OcamlViz (87) for monitoring OCaml programs, MLPOST (84) to produce graphical figures from OCaml code. We also maintain our bibtex2html for producing HTML documents from BibTeX files, used to produce hundreds of thousands of pages in the world.

Tools Verification A quite recent research topic in our team is the verification of tools. The first project we conducted in this direction is the design of certified kernel of the Alt-Ergo prover, on top of Coq (193). Although not covering all aspects of Alt-Ergo, it demonstrated it was possible for a fairly large kernel that includes a SAT solver, a decision procedure for equality and linear integer arithmetic.

A second project is the design of a certified VC generator for C programs annotated in ACSL. A first step was the design of the certified VC generator analogous to Why (61), and then a certified compiler from C/ACSL to Why (191). That second part is based upon the operational semantics of C provided by CompCert, upon which we formalized the semantics of ACSL.

Our objective is to go further into such a direction, and to scale-up on larger tools we aim at automatizing the proof as much as possible. This is why we proposed another formalization of a VC generator (75), done using Why3 instead of Coq, for which we showed that the degree of automation is high.

Activity 4: Verified Computer Arithmetic

In industrial applications, numerical computations are very common (e.g. control software in transportation) and they typically involve floating-point numbers. In order to analyze numerical programs, we have developed several tools. There are some Coq libraries (see above), namely PFF and Flocq. There is also the Gappa solver for automatically proving numerical properties (3). In recent years, we have demonstrated our capability toward specifying and proving properties of floating-point programs, properties which are both complex and precise about the behavior of these programs.

Floating-point arithmetic For the purpose of verifying numerical programs, the first step is the modeling of floating-point numbers. The Flocq library (70) provides a multi-radix and multi-precision Coq formalization for various floating- and fixed-point formats, coming with a comprehensive set of theorems and automations based on Gappa (120). This model interacts with our tool chain thanks to a Jessie model of floats (42), so that exceptional behavior may either be allowed or prevented by proof obligations.

We have also an expertise on floating-point arithmetic, exercised independently from programs. This includes several algorithms: emulation of the FMA (14) described in Figure 1.2, error of the FMA (12), argument reduction (11), predecessor and successor (6). We also contributed to the Handbook of Floating-Point Arithmetic in 2009 (122).

Verified numerical computations We of course applied our methodology to numerous numerical programs. See for instance the web galleries of certified programs of our team¹, Hisseo², S. Boldo³, and industrial case studies in the U3CAT ANR project. Several of these examples are presented in (13). An implementation of an elementary function is studied in (4). A program for accurately computing the area of a triangle is presented in (67) and for the discriminant in (17). Investigations about finite field arithmetic are in (118). Interval arithmetic was used to correctly approximate the Masser-Gramain mathematical constant (19).

A challenging case study was the analysis and the proof of both the method error and the rounding error of a numerical analysis program solving the one-dimension acoustic wave equation, using the second-order centered finite difference explicit scheme. It was presented in part for the method error (68) and in another part for the rounding error (66) and fully in a paper in the JAR journal (10).

Compiler- and architecture-related problems Unfortunately, even C programs that were carefully proved may end up failing, as floating-point operations will be subjected to several transformations, e.g. compilation, before being actually executed. There are several ways to circumvent this. We may take into account all the possible compilation features and issues (71, 22). We may also prove programs directly on the assembly code (121). Lastly, we may design a verified compiler that correctly supports floating-point arithmetic (69).

Activity 5: Data-Centric Programming Languages and Systems

Internet explosion and the ever growing importance of data in applications has given birth to a whirlwind of new data models (XML, JSON, RDF), languages (XPath, XQuery, Pig, Jaql, Sparql, JavaScript, ...) and data engines. Data, in all forms, is increasingly large in volume. The availability and reliability of such large data volumes is a gold mine for companies, scientists and simply citizens.

On one hand, it is clear that languages manipulating such data can greatly benefit from formal uniform foundations, and we argue that such foundations should account for novel features critical to various application domains. Also, most of those languages provide limited type checking, or ignore it altogether. We believe type checking is essential for many applications, with usage ranging from error detection to optimization.

On the other hand, and surprisingly, while the amount of data stored and managed by data engines has drastically increased, little attention has been devoted to ensure that such (complex) systems are indeed reliable. Obtaining strong guarantees relies on the use of formal tools.

The data-centric languages and systems thematic aims at (i) designing and developing programming languages as well as systems that seriously take into account massive data (ii) improving existing languages and/or systems and (iii) provide certified implementations of data intensive management systems and/or languages. The final purpose is to build robust and efficient platforms on well founded theoretical grounds.

Data-centric Languages Based on the approach of semantic subtyping (5) we began working on NoSQL languages very popular in the context of big data and/or cloud computing. We defined a general framework that can both express and type such languages via an encoding into a core calculus. Each such language can in this way preserve its execution model but obtain for free a formal semantics, a type inference system and, as it happens, a prototype implementation. This contribution has been published at the ACM International Symposium on Programming Language (POPL 2013) (72).

The design and implementation of CDuce started in the early 2000 and is still going on. We are extending CDuce (and the semantic subtyping approach (5)) with polymorphism in collaboration with G. Castagna from PPS - CNRS - Université Paris Diderot. To this end a first highly challenging step consisted in defining an explicitly typed polymorphic calculus (with recursive types, arrows, unions, intersection and negation), such a definition required the definition of a calculus explicitly typed for intersection types: a problem left open for twenty years. This work will appear in POPL 2014. Another part of this extension of

¹<http://toccata.lri.fr/gallery/index.en.html>

²<http://hisseo.saclay.inria.fr/>

³<http://www.lri.fr/~sboldo/research.html>

CDuce to polymorphism was the study of the calculus in order to be able to generate typing constraints in order to provide local type inference for polymorphic function application (Castagna Nguyen Xu). Based on this, we obtained an implementation technique, relying on a smart extension of the closure technique, that allows to execute polymorphic function application with the same efficiency than in the monomorphic case. This is quite standard in the case of languages such as ML but absolutely astonishing for a language such as CDuce which allows for dynamic dispatch on types thus preventing type erasure.

Data-centric Systems: automata based XML query engines A first line of research consisted, based on previous work, to provide type-based optimizations for XPath/XQuery engines. The approach proposed various static analysis in order to prune the documents to be queried, only loading the relevant part that the query need to compute its result. This led to the ACM TODS publication (15).

Complementarily to the previously mentioned static analyses aspects, we also focus on *efficient* implementations of XML standards (XPath in particular) based on tree automata. A first result is the SXSI query engine (on which we report in (41)) which uses a novel dynamic analyses of tree automata that makes SXSI on par with state of the art query engines. Building on SXSI, the TAToo library (Tree Automata TOOLkit) aims at providing both an efficient runtime and powerful static analyses (query containment/emptiness checking) in the same framework (<http://typex.lri.fr/software.html>).

Data-centric Systems: toward mechanized and verified implementations In this line of research, we are highly interested in the certification of data intensive systems such as relational database systems, XPath/XQuery and semi structured data engines using formal tools such as Solvers (The WAM-Solver), SMT provers (e.g., Alt-ergo) embedded in the Why(3) platform as well as interactive theorem provers (e.g., Coq).

In the context of a PhD that began in October 2012, we designed and implemented a Coq library for the relational data model. Based on this library, we are currently verifying an SQL compiler. This includes proving the correction of the translation of queries into their relational algebra counterpart but also prove that the algorithms used to implement relational operators conform to their (Coq formalized) specification and finally prove the correction of the query optimizer. We are also addressing the problem of formally verifying database updates.

Activity 6: Synchronous Programming

Synchronous languages have demonstrated in the past their pertinence for the development of the most critical embedded systems, both from the theoretical point of view and from the industrial point of view (Airbus airplanes, EDF nuclear plants, railway signaling, etc.). They belong to a wide range of programming and modeling tools allowing to describe in a unique formalism both an embedded controller and its environment, to simulate/verify the whole and to generate target code. Among those tools, the most representative ones are SCADE based on a synchronous language and Simulink which offers a wider expressiveness as it combines both discrete and continuous time.

Our research group worked on the design, semantics, and compilation of synchronous languages considering their relationship with typed functional languages. In the past years, we addressed the following topics: (1) providing new abstraction mechanisms, compilation techniques, and dedicated type systems to increase the expressiveness and safety of synchronous languages; (2) the theory of n-synchronous systems, a relaxed model of synchrony allowing to deal with the communication with bounded buffers; (3) the semantics and compilation of hybrid modelers where programs mix continuous and discrete time. Our results are experimented in several programming languages developed in the group: Lucid Synchrone, ReactiveML (20), Lucy-n (112); used both to validate them and to communicate with industrial partners. We have a solid experience of collaboration with production team from industry, in particular with Esterel-Technologies, Dassault-Systèmes and NXP. Several research results have been developed jointly or come directly from problems they encountered. As an example, various features from Lucid Synchrone are integrated to the compiler of SCADE 6 developed at Esterel-Technologies and distributed since 2008 (among others, type and clock calculus, initialization analysis, hierarchical automata). A compiler of Lucid Synchrone has also been developed at Dassault-Systèmes (Grenoble) and is now integrated inside the CATIA environment. The work on n-synchrony is the result of a close collaboration with the group of Marc Duranton at NXP (Eindhoven).

n-Synchronous Kahn Networks In collaboration with Albert Cohen, Christine Eisenbeis (INRIA Alchemy), and Marc Duranton (NXP, Eindhoven), we introduced the theory of n -synchronous Kahn networks as a relaxed model of synchrony. The n -synchronous model allows to compose streams that have *almost the same clock* and can be synchronized through the use of a finite buffer. This relaxed model is achieved by introducing a sub-typing rule in the clock calculus to localize places where synchronization code must be inserted. Sub-typing can be checked for ultimately periodic clocks (82, 108). Nevertheless, this check can be costly when clock patterns are long, and is restricted to periodic behaviors only. An abstraction mechanism, allowing to deal with sets of (non necessarily periodic) clocks has been proposed in (37, 81).

Based on those ideas, we have designed and implemented the language Lucy-n (83, 112). This language provides a dedicated type system, the clock calculus, which is able to verify properties like the absence of buffer overflows and deadlocks. Moreover, it computes static schedules of the programs and sufficient buffer sizes. It has been applied to the static scheduling of latency insensitive designs (58). The theory has been formalized in the proof assistant Coq (81, SP-5, 112, 184).

We also worked on other extensions of the synchronous model, for example an object oriented features (34) or distributed applications (38).

Semantics and Compilation of Hybrid System Modelers Hybrid systems modelers such as Simulink have become the corner stone of embedded system development. They allow both *discrete* controllers and their *continuous* environments to be expressed *in a single language*. Despite the availability of such tools, there remain a number of issues related to the lack of reproducibility of simulations and of a clear semantics or the whole.

In collaboration with Albert Benveniste, Benoit Caillaud, and Timothy Bourke (INRIA Rennes), we proposed using nonstandard analysis as a semantic domain for hybrid modelers (32). Then, we considered a minimal, yet full-featured synchronous language, where data-flow equations can be mixed with ordinary differential equations (ODEs) with possible reset. A type system is proposed to statically distinguish discrete computations from continuous ones and to ensure that signals are used in their proper domains. The extended data-flow language is realized through a source-to-source transformation into a synchronous subset, which can then be compiled using existing tools into routines that are both efficient and bounded in their use of memory. These routines are orchestrated with a single off-the-shelf numerical solver (SUNDIALS) using a simple but precise algorithm which treats causally-related cascades of zero-crossings.

Modular and formally defined Code Generation Our research activity has also concerned the development of compilation methods.

In collaboration with P. Raymond (VERIMAG, Grenoble), we have worked on the modular generation of sequential imperative code from synchronous data-flow networks. Though this question has been identified almost twenty years ago, it has almost been left aside until the recent work of Lublinerman, Szegedy, and Tripakis presented at POPL'09. The problem is proven to be intractable and the authors derive an iterative algorithm where each step is encoded as a SAT problem. Despite the apparent intractability of the problem, it appears that real problems rarely fall in this category. Based on an analysis of input/output dependences, we have proposed a polynomial algorithm that (1) either gives an optimal solution or (2) gives a non trivial lower bound on the number of classes to start an iterative combinatorial search (59, 21). In all the examples we have considered (the whole SCADE library and two industrial examples from Airbus), the polynomial algorithm finds an optimal scheduling.

We also worked on the formal description of a reference compiler for a Lustre-like language extended with automata. The formal description of a compiler is given in (45). An implementation in Coq, together with a formalization of the semantics of all intermediate languages has been done (183). This work is under revision for a journal publication.

Synchrony for interactive applications The synchronous model is used to program safety critical embedded systems because it has good properties such as a simple semantics and a deterministic model of concurrency. These properties can also be useful in a more general context like the programming of discrete simulations. Therefore, we develop the ReactiveML language which embeds the synchronous model inside a subset of OCaml.

The possibility to define complex data structures and the expressiveness of the language has allowed to write an interpreter of Antescofo (31). Antescofo⁴ is a language dedicated to mixed music, that is

⁴<http://repmus.ircam.fr/antescofo>



musical pieces where human musicians interact with electronic parts. The electronic part have to handle in particular, tempo variations, synchronizations and errors. The read-eval-print loop of ReactiveML (109) has permitted to extends the Antescofo system with live coding (90).

Besides, for the programming of systems that exhibits multiple time scales, we proposed an extension of the synchronous model of concurrency, called reactive domains (57). Reactive domains allow the creation of local time scales and enable refinement, that is, the replacement of an approximation of a system with a more detailed version without changing its behavior as observed by the rest of the program. This is the kind of patterns that are really common in discrete simulations.

1/ Toccata

Collaborations

Our collaborations that are materialized by contracts are listed in Section 5.1.

Visits to and from International Teams

- J. Siméon from IBM research Watson - USA visited our team in October 2011 working on type systems for NoSQL languages (72).
- K. Nguyễn visited J. Siméon and K. Rose IBM research Watson - USA in April 2011
- V. Benzaken visited J. Siméon and K. Rose at IBM research Watson - USA in April 2011 and gave a seminar on CDuce.
- J.-C. Filliâtre visited Alwyn Goodloe at the National Institute of Aerospace (Hampton, USA) in September 2009 and gave a tutorial on the Why tool. J.-C. Filliâtre also presented the ACSL specification language (143) and the Frama-C platform.
- M. Pouzet visited Arvind (MIT, Boston, USA) and Grégoire Hamon (TheMathworks, USA) in July 2009. He presented the N-synchronous model.
- S. Conchon visited Intel Strategic Cad Labs during summer 2012.
- J.C. Filliâtre visited SRI (Menlo Park, California, USA) during summer 2012.
- M. Pouzet visited TheMathworks (Natick, USA) in July 2010 and gave a talk on VeLus, a formally certified Lustre compiler.
- Dr César Muñoz from the National Institute of Aerospace (NIA, Hampton, Virginia, USA) visited the Proval team for one month, in July 2008, with Digiteo funding support. The cooperation will continue in particular in relation with the Hisseo project, on the subject on analysing avionics code involving floating-point computations.
- We had two visits associated with the Orchid project in collaboration with National Taiwan University: Pr. Yih-Kuen Tsay together with his student Ming-Hsien Tsai for one week in July 2008 and Tyng-Ruey Chuang from Academia Sinica for one week in August 2008.
- Barbará Vieira, Ph.D. student at Universidade do Minho (Braga, Portugal), visited ProVal from March to May 2009. She worked with J.-C. Filliâtre on a verification tool for CAO, a domain-specific language for cryptographic protocols (<http://www.cs.bris.ac.uk/~page/research/cao.html>).
- D. Ishii (National Institute of Informatics, Japan) visited the team for 8 months to work on applying program verification methods to hybrid systems.
- Thierry Coquand (University of Gothenburg, Sweden) visited our team in January as part of the Digiteo invitation program. He worked with C. Paulin and other researchers from Typical and MSR-INRIA research center on the use of the Coq proof assistant for the development of formal mathematics.
- Simão Melo de Sousa (Universidade da Beira Interior, Portugal) visited ProVal from September to November 2010. He worked with J.-C. Filliâtre on the deductive verification of ARM7 assembly programs, with application to the WCET problem.
- L. Mandel visited IBM Watson for 6 weeks (148).

Other Collaborations

- V. Benzaken, and K. Nguyễn, PPS-CNRS: Data Centric Languages work on NoSQL and XQuery 3.0 types systems (72)

- 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 (SP-2).
- J.-C. Filliâtre has collaboration with University do Minho (Braga, Portugal) on the use of Why as intermediate for verification of cryptographic programs (1).
- J.-C. Filliâtre has collaboration with Universidade da Beira Interior (Covilhã, Portugal) on the use of Why as intermediate language for verification of ARM programs (96).
- Our on-going development of a verified JavaScript interpreter, described above, is an active collaboration with people from Imperial College, London, UK.

Participation to National and International Networks

FoVeOOS project: Formal Verification of Object-Oriented Software

- European Program COST (European Cooperation in the field of Scientific and Technical Research, <http://www.cost.esf.org/>)
- project IC-0701, <http://www.cost-ic0701.org/>
- 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.
- C. Marché, coordinator for France, and coordinator of working group 2: Modularisation and Components

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.

Coordination Action TYPES TYPES was a working group in the EU's 6th framework programme. It started in September 2004 lasted until april 2008. It was a continuation of a number of successful European projects starting in 1997. <http://www.cs.chalmers.se/Cs/Research/Logic/Types/>

The project involved not less than 33 academic groups in Sweden, Finland, Italy, Portugal, Estonia, Serbia, Germany, France, United Kingdom, Poland ; and industrial research groups at France Telecom and Dassault Aviation.

The aim of the research was to develop the technology of formal reasoning and computer programming based on Type Theory. This is done by improving the languages and computerised tools for reasoning, and by applying the technology in several domains such as analysis of programming languages, certified software, formalisation of mathematics and mathematics education.

Participation to "Investissements d'avenir" Programme

Labex "DigiCosme" C. Paulin is the director of the Labex "DigiCosme" (<http://www.labex-digicosme.fr/>).

DigiCosme is an excellence laboratory center (labex) in the area of Information and Communication Science and Technology. It is funded for 9M euros for the 2012-2019 period as part of the program "Investissements d'Avenir" launched by the French ministry of research. It is operated by the *fondation de coopération scientifique Paris-Saclay* as part of the "initiative d'excellence" Paris-Saclay.

DigiCosme is both concerned with Research and Education. Regarding research topics, it emphasizes three main action lines: Software Reliability and Security, Intelligent network structures and Data intelligence.

Management Positions in Scientific Organisations

- V. Benzaken, elected member of the CNU 27th section ("Conseil National des Universités") since 2011
- V. Benzaken, elected member of the CNESER ("Conseil National de l'Enseignement Supérieur et de la Recherche") since 2011
- V. Benzaken, member of the council of the faculty of science d'Orsay ("Conseil d'UFR") since 2011
- V. Benzaken, vice head (in charge of research) of the computer science department since Jan. 2012
- S. Boldo, elected representative of the researchers at the "comité de centre" of the INRIA Saclay - Île-de-France, 2008-2010.
- S. Conchon, elected member of the "*Conseil scientifique de l'Université Paris-Sud*" since June 2012.
- É. Contejean, elected member of the "*Comité National de la Recherche Scientifique*" (CoNRS), 6th section, since september 2012.
- C. Paulin, elected member of the board ("*conseil d'administration*") of University Paris-Sud 11 until july 2008.
- C. Paulin, déléguée scientifique of the Inria Saclay Île-de-France center, and member of the national evaluation board of Inria (2008-2010).
- C. Paulin, director of the Graduate school in Computer Science at University Paris Sud <http://dep-info.u-psud.fr/ed/> (2008-2012).
- C. Paulin, deputy director of the LRI in 2011.
- C. Paulin, head of the new *Digicosme* laboratory of excellence (<http://labex-digicosme.fr/>) since 2012.
- C. Paulin, in charge of the assembly of directors of graduate schools at Université Paris-Sud, since 2012.
- C. Paulin, member of the board of the "Commission Académique Consultative" of the Initiative d'Excellence Paris-Saclay, since 2012.
- C. Paulin, president of the Computer Science Department of the University Paris-Sud <https://www.dep-informatique.u-psud.fr/>, since February 2012.
- 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".

Organisation of Conferences and Scientific Events

- J.-C. Filliâtre co-organized (with Leo Freitas, University of York, UK) the VSTTE'09 workshop (November 2009, Eindhoven, the Netherlands). <http://vstte09.lri.fr/>.
- J.-C. Filliâtre co-organized (with Cormac Flanagan, University of California, Santa Cruz, CA, USA) the PLPV'10 workshop (January 2010, Madrid, Spain). <http://slang.soe.ucsc.edu/plpv10/>.
- C. Paulin co-organized the *Digiteo Annual Forum 2009* (http://www.digiteo.fr/Digiteo_Annual_Forum_2009) which happened on Oct 21, 2009 at École Polytechnique. 335 participants. C. Marché was responsible for a session on critical software at this Forum.
- C. Marché co-organized (with B. Beckert, Karlsruhe Institute of Technology, Germany) the International Conference on Formal Verification of Object-Oriented Software (Paris, France, June 28-30, 2010). <http://foveos2010.cost-ic0701.org/> (132).
- On behalf of the VSTTE 2012 conference (Philadelphia, USA, January 2012), A. Paskevich and J.-C. Filliâtre organized the first formal VSTTE program verification competition (<https://sites.google.com/site/vstte2012/compet>). It lasted for 48 hours, from November 8 to November 10. A set of five verification problems was proposed to the participants. Each problem consisted of an algorithm given in pseudocode, together with a set of properties to be mechanically proved. A total of 29 teams (79 participants) sent solutions, which is considered an excellent success.
- C. Paulin organizer of the first DigiCosme Colloquium (<http://labex-digicosme.fr/Colloque2012>), Sept. 12-13, École Polytechnique, France.
- C. Paulin organizer of the 4th Conference on Interactive Theorem Proving (<http://itp2013.inria.fr/>, July 2013).
- C. Marché organizer of the first DigiCosme Spring School (<http://labex-digicosme.fr/Spring+School+2013>, <https://www.lri.fr/~marche/DigiCosmeSchool/index.html>) whose theme was *Program Analysis and Verification*, April 2013.

Working Groups

- V. Benzaken, member of BDA steering committee (since 2005).
- M. Pouzet, member of IFIP Working Group 2.11 (Program Generation) <http://www.cs.rice.edu/~taha/wg2.11/>.
- J.-C. Filliâtre, member of IFIP Working Group 1.9/2.15 (Verified Software) <http://www.ifip.org/bulletin/bullfcs/memtc01.htm#wg19>
- C. Paulin, member of the steering committee of the european TYPES working group, until 2008.

Other Responsibilities

- V. Benzaken, elected member of the CCSU-27ième section (Commission Consultative des Spécialistes de l'Université)
- M. Pouzet, member of the "commission de spécialistes", section 27, INPL Nancy, 2008.
- C. Marché, member of the "commission de spécialistes", Section 27, University Paris-Sud 11, 2008.
- C. Marché, French National Coordinator for the COST action "Formal Verification of Object-Oriented Programs", 2008-2012.
- G. Melquiond is an elected officer of the IEEE-1788 standardization committee on interval arithmetic (2008-?).
- S. Conchon, member of the "commission de spécialistes", Section 27, University Paris-Sud 11, 2008-2009.
- S. Conchon is an elected member of the board ("conseil du laboratoire") of Laboratoire de Recherche en Informatique (LRI), 2008-2009.
- M. Pouzet is an elected member of the "conseil du laboratoire" of LRI, 2008-2009.
- S. Boldo, member of the CLHS ,comité local hygiène et sécurité and member of the CLFP, comité local de formation permanente of Inria, 2010-2011.
- E. Contejean and C. Marché, nominated members of the "conseil du laboratoire" of LRI since April 2010.
- G. Melquiond, C. Paulin, members of the "commission consultative de spécialistes de l'université", Section 27, University Paris-Sud 11 since April 2010.
- S. Boldo, elected member of the Inria Evaluation Committee, since 2011.
- S. Boldo, member of the committee for the monitoring of PhD students (commission de suivi des doctorants), 2011-2013
- S. Boldo, member of the MECSI group for networking about computer science popularization inside INRIA, since 2011. Scientific head for Saclay since 2012.
- C. Marché is member of the program committee of Digiteo (<http://www.digiteo.fr/>), 2008-2013.
- C. Paulin, member of the program committee of Digiteo, <http://www.digiteo.fr/>, since 2010.
- C. Marché, member of the selection committee of the "DIM Logiciels et Systèmes Complexes", providing grants to research projects, funded by Île-de-France regional council and Digiteo cluster, <http://www.dimlsc.fr/>.
- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- A. Charguéraud is vice-president of "France-IOI", the organization in charge of the selection and the training of the French team to the International Olympiads in Informatics, since 2004.
- C. Lelay, elected member of the "conseil du laboratoire" of LRI since November 2011.
- C. Lelay, elected representative of the students at the Doctoral School in Computer Science at University Paris-Sud since November 2011.
- A. Paskevich is in charge (together with C. Bastoul) of Licence professionnelle PER (L3) at IUT d'Orsay, Paris-Sud University since September 2012.

1/ Toccata

Honors

Prizes and Awards

- S. Conchon, E. Contejean, M. Iguernelala, award 2011 of the European Association for Theoretical Computer Science <http://www.eatcs.org/index.php/best-etaps-paper> for the best theoretical paper of all ETAPS Conferences (64), 2011.
- C. Paulin, Doctor Honoris Causa, University of Gothenburg, Sweden, October 21, 2011.
- Marc Pouzet, junior member of the IUF ("Institut Universitaire de France"), that distinguishes each year a few French university professors for the high quality of their research activities, 2008-2010.
- Project Pactole won the best Digiteo poster award at the annual Digiteo forum on the 21st of October http://www.digiteo.fr/Digiteo_Annual_Forum_2009.

Keynote Addresses

International

- J.-C. Filliâtre was invited speaker at SMT 2008 (Princeton, USA) (24): *Using SMT solvers for deductive verification of C and Java programs*.
- M. Pouzet was invited speaker at ISOR 2008 (Alger, Algeria, 2-6/2008): *Synchrony and Clocks in Khan Process Networks*.
- J.-C. Filliâtre was invited speaker at AFM'09 (Grenoble, France): *Invited tutorial: Why — an intermediate language for deductive program verification* (25).
- M. Pouzet was invited to the annual meeting of IFIP WG2.8 on Functional Programming (Frauenchiemsee, Germany, June 7-12, 2009).
- C. Paulin was invited to the conference "*Philosophy and Foundations of Mathematics : Epistemological and Ontological Aspects*" dedicated to Per Martin-Löf on the occasion of his retirement in Uppsala, May 5-8, 2009.
- G. Melquiond was invited to present the IEEE-1788 standardization process (39) at the Arith 19 symposium in Portland, OR, June 8-10, 2009.
- S. Boldo, invited speaker at the Third International Workshop on Numerical Software Verification (NVS-3) on July 15th 2010: *Formal verification of numerical programs: from C annotated programs to Coq proofs*.
- L. Mandel, invited lecture at Journées Francophones des Langages Applicatifs: *Cours de ReactiveML*
- J.-C. Filliâtre, "Memo Tables", invited at the IFIP Working Group 2.8 *Functional Programming* (Marble Falls, Texas, USA, March 7–11, 2011).
- P. Herms, "Certification of a Verification Condition Generator in Coq", seminar of the Gallium-Moscova teams, Rocquencourt, June 20th.
- C. Marché, "Verifying Behavioral Specifications of Programs: the Why Approach", seminar of the ELP team, Departamento de Sistemas Informáticos y Computación, Universidad Politécnica de Valencia, Spain, March 25th.
- C. Paulin, "About Inductive-Recursive Definitions in Coq", invited speaker at the workshop on Proofs and Programs, Gothenburg, Sweden, Oct. 22th.
- G. Melquiond, "Wave Equation Numerical Resolution: a Comprehensive Mechanized Proof of a C Program", CaCoS Workshop, Grenoble, July 26th.
- J.-C. Filliâtre, "Combining Interactive and Automated Theorem Proving in Why3", Automation in Proof Assistants 2012, Tallinn, Estonia, April 2012.
- J.-C. Filliâtre, "Combining Interactive and Automated Theorem Proving using Why3 (invited tutorial)", Second International Workshop on Intermediate Verification Languages (BOOGIE 2012), Berkeley, California, USA, July 2012.
- J.-C. Filliâtre, "One Logic To Use Them All", 24th International Conference on Automated Deduction, Lake Placid, USA, June 2013.

France

- T. Nguyen, "Hardware-independent proofs of numerical programs", seminar of the Arenal team, Lyon, January 20th.
- G. Melquiond was invited speaker at the arithmetic workshop of GDR IM (RAIM'09) in Lyon, October 26-28, 2009.
- S. Boldo was invited to the main INRIA Paris-Rocquencourt seminar, "*Le modèle et l'algorithme*" (<http://www.inria.fr/rocquencourt/rendez-vous/modele-et-algo/>), on October 1st.
- M. Pouzet was invited speaker at "journées de l'AFSEC, Toulouse, 27 janvier 2009: *Abstraction d'horloges dans les systèmes synchrones*.
- S. Boldo, "Contours de la communauté", invited talk at the *4es Rencontres Arithmétique de l'Informatique Mathématique* (RAIM'11) in Perpignan. (Collected data about the outline of the computer arithmetic community in France: sites, themes, fundings...).
- S. Boldo, "Preuve de programmes d'analyse numérique", seminar of the AriC team, Lyon, January 5th.
- K. Nguyen, "Programmation XML, de la théorie aux outils", invited lecture at "24^e Journées Francophones des Langages Applicatifs", Aussois, February 3-6, 2013.
- C. Lelay, "Improving Real Analysis in Coq: a User-Friendly Approach to Integrals and Derivatives", Co-qapprox seminar (for the Tamadi ANR), Lyon, July 11th.

- C. Lelay, "Improving Real Analysis in Coq: a User-Friendly Approach to Integrals and Derivatives", LAC/LaMHA/LTP Days, Orléans, October 25th.

1/ Toccata

Evaluation of Research

Editorial Boards

International

- C. Paulin co-edited with Ph. Audebaud the proceedings of the conference MPC'08 as a Springer volume in the serie Lectures Notes in Computer Science, she also co-edited a special issue of Science of Computer Programming devoted to selected papers of this conference.
- Marc Pouzet is associate editor of the EURASIP Journal on Embedded systems (<http://www.hindawi.com/journals/es/>). He is "directeur de collection" for Hermes publisher.
- J.-C. Filliâtre is member of the editorial board of the *Journal of Functional Programming*.
- C. Paulin is member of the editorial board of the *Journal of Formalized Reasoning*.
- C. Marché co-edited with B. Beckert a special issue of Elsevier Lectures Notes in Computer Science devoted to selected papers of the conference FoVeOOS'10 (132).
- J.-C. Filliâtre edited a special issue of Software Tools for Technology Transfer devoted to selected papers of the workshop VSTTE 2009. This includes an introduction paper on deductive software verification (8).

National

- S. Boldo is member of the editorial committee of the popular science web site *interstices*, <http://interstices.info/>.

Program Committees

Chair

- C. Paulin, program co-chair of the 9th International Conference on Mathematics of Program Construction, MPC 2008.
- C. Paulin, program co-chair of the 4th International Conference on Interactive Theorem Proving, ITP 2013.
- C. Marché, program co-chair of the 1st International Conference on Formal Verification of Object-Oriented Software, FoVeOOS 2010.
- C. Marché, *Tool Chair* of the program committee of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013, Rome, Italy, <http://www.etaps.org/2013/tacas13>), part of the ETAPS joint Conference. The tool chair is responsible for the evaluation and selection of tool papers and tool demonstrations, following precise guidelines given in the call for papers. This initiative of TACAS aims at making the selection of such submissions more accurate (<http://www.etaps.org/2013/tacas13/tacas13-tool-papers-menu>).
- S. Conchon, program co-chair of the Journées Francophones des Langages Applicatifs, JFLA 2010.
- S. Conchon, program chair of the Journées Francophones des Langages Applicatifs, JFLA 2011, La Bresse, France, January 2011.
- M. Pouzet, member of the steering committee of the workshop on synchronous programming (SLAP) since 2006.

Member (international events)

- V. Benzaken, European Symposium on Programming- ETAPS ESOP, 2013.
- V. Benzaken, International Conference on Data Engineering ICDE, 2011.
- V. Benzaken International XML Symposium (XSYM 2010)
- V. Benzaken International Conference on Very Large Databases VLDB, 2009.
- V. Benzaken ACM International workshop on Programming Languages for XML (PLAN-X 2008).



- S. Boldo, 4th International Workshop on Numerical Software Verification, NSV 2011, affiliated to CAV.
- S. Conchon, ACM Sigplan Workshop on ML, 2008.
- S. Conchon, 10th International SMT workshop 2012, Manchester, UK.
- É. Contejean, ACM SIGPLAN 2011 Workshop on Partial Evaluation and Program Manipulation, PEPM 2011, co-located with POPL, Austin, Texas.
- É. Contejean, the International Workshop on Proof Search in Axiomatic Theories and Type Theories (PSATT 2011, affiliated to CADE, Wroclaw, Poland).
- É. Contejean, 23rd International Conference on Rewriting Techniques and Applications, RTA 2012, <http://rta2012.frs.cm.is.nagoya-u.ac.jp/>.
- É. Contejean, 24th International Conference on Automated Deduction, CADE-24, 2013, <http://www.cade-24.info/>.
- J.-C. Filliâtre, 21st International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2008, Montréal, Québec, Canada.
- J.-C. Filliâtre, 3rd Automated Formal Methods workshop, AFM 2008, Princeton, USA.
- J.-C. Filliâtre, AFM 2009
- J.-C. Filliâtre, PLMMS 2009
- J.-C. Filliâtre, TPHOLs 2009
- J.-C. Filliâtre, VSTTE 2009
- J.-C. Filliâtre, PLPV 2010.
- J.-C. Filliâtre, AFM 2010.
- J.-C. Filliâtre, IWS 2010
- J.-C. Filliâtre, PLPV 2010.
- J.-C. Filliâtre, 2nd conference on Interactive Theorem Proving (ITP 2011).
- J.-C. Filliâtre, workshop Analyze to Compile, Compile to Analyze, ACCA 2011.
- J.-C. Filliâtre, conference Verified Software: Theories, Tools and Experiments, VSTTE 2012.
- J.-C. Filliâtre, conference NASA Formal Methods, NFM 2012.
- J.-C. Filliâtre, 10th Asian Symposium on Programming Languages and Systems, APLAS 2012.
- C. Marché, 7th International Workshop on Rewriting Logic and its Applications, WRLA 2008.
- C. Marché, 22th International Conference on Automated Deduction, CADE 2009.
- C. Marché, 2nd International Conference on Formal Verification of Object-Oriented Software, FoVeOOS 2011, Turin, Italy.
- C. Marché, 23rd International Conference on Automated Deduction, CADE 2011, Wroclaw, Poland.
- C. Marché, 1st International Workshop on Intermediate Verification Languages, BOOGIE 2011, affiliated to CADE.
- K. Nguyen, DBPL 2011, 13th International Symposium on Database Programming Languages August 29th, 2011, Seattle, Washington, USA, co-located with VLDB 2011
- K. Nguyen, PADL 2013, 15th International Symposium on Practical Aspects of Declarative Languages, January 21-22, 2013, co-located with POPL 2013
- K. Nguyen, WebDB 2013, 16th International Workshop on the Web and Databases, New York, NY, USA, June 23, 2013, co-located with ACM Sigmod 2013
- C. Paulin, 21st International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2008, Montreal, Quebec, Canada.
- C. Paulin, 10th International Conference on Mathematics of Program Construction, MPC 2010.
- C. Paulin, 2nd conference on Interactive Theorem Proving (ITP 2011).
- C. Paulin, 5th ACM SIGPLAN Workshop on Programming Languages meets Program Verification, PLPV 2011, affiliated to POPL.
- C. Paulin, 3rd conference on Interactive Theorem Proving, ITP 2012.
- M. Pouzet, Real-Time and Network Systems Conference, 2008.
- M. Pouzet, Real-Time and Network Systems Conference 2009.
- M. Pouzet, MSR 2009.
- M. Pouzet, workshop on Hardware Functional Languages, 2009.
- M. Pouzet, 31st IEEE Real-Time Systems Symposium conference, RTSS 2010.
- M. Pouzet, Formal Methods in Computer Aided Design, FMCAD 2010.
- M. Pouzet, Design, Automation & Test in Europe, DATE 2010.
- M. Pouzet, Conference on Real-Time and Network Systems, RTNS 2010.
- M. Pouzet, workshop of Design Correct Circuits, DCC 2010, affiliated to ETAPS.

Member (national events)

- D. Baelde, Journées Francophones des Langages Applicatifs, JFLA 2012.
- V. Benzaken, Bases de Données Avancées (BDA) 2013.
- V. Benzaken, Bases de Données Avancées (BDA) 2011.
- S. Boldo, Journées Francophones des Langages Applicatifs, JFLA 2011

- S. Conchon, Journées Francophones des Langages Applicatifs, JFLA 2009.
- J.-C. Filliâtre, Inforum 2010.
- L. Mandel, Journées Francophones des Langages Applicatifs, JFLA 2012.
- G. Melquiond, Journées Francophones des Langages Applicatifs, JFLA 2012.
- M. Pouzet, Journées Francophones des Langages Applicatifs, JFLA 2008.
- M. Pouzet, Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2008.
- M. Pouzet, Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2010.

Evaluation Committees and Invited Expertise

International

- C. Paulin participated to the hiring committee for a senior lecturer position at in Logic of Programs at University of Göteborg in Sweden, 2012.
- C. Paulin participated to the review panels for the German Excellence Initiative proposals for Graduate Schools in informatics, 2011.

National

- V. Benzaken, 2011, member of the AERES evaluation commission for LIF and LSIS CNRS labs.
- V. Benzaken, 2009, member of the commission for "*prime d'excellence scientifique (PES) 27ème section*".
- É. Contejean, member of the "*jury de l'agrégation externe de mathématiques*" as an expert in computer science for the hiring session, 2008-2011.
- C. Marché and S. Boldo, members of the "*jury de l'agrégation externe de mathématiques*" as experts in computer science, since 2012.
- G. Melquiond is an examiner for the computer science entrance exam to École Normale Supérieure since 2010.
- C. Paulin is a member of the "Commission Scientifique", in charge of selecting PhD students, post-doc, invited researchers funded by Inria Saclay - Île-de-France), 2011-2012.
- J.-C. Filliâtre is *correcteur au concours d'entrée à l'École Polytechnique* (computer science examiner for the entrance exam at École Polytechnique) since 2008.
- S. Conchon is *correcteur au concours d'entrée à l'École Polytechnique* (computer science examiner for the entrance exam at École Polytechnique), 2009-2011.

Other evaluation activities

Hiring Committees

- V. Benzaken, Professor position at Paris Sud (2013).
- V. Benzaken, Professor position at Paris Sud (2012).
- V. Benzaken, President of the recruiting commission Assistant Professor position at Paris Sud (2011).
- V. Benzaken, Inria Rocquencourt CR1 hiring committee (2010).
- V. Benzaken, Inria Rocquencourt CR2 hiring committee (2010).
- V. Benzaken, Inria Lille, CR1 hiring committee (2010).
- V. Benzaken, Inria Lille, CR2 hiring committee (2010).
- V. Benzaken, Assistant Professor Paris Sud IUT (2009).
- V. Benzaken, Professor position at INPG (2009).
- V. Benzaken, Inria Saclay, CR2 hiring committee (2008).
- V. Benzaken, Inria de Rennes, CR2 hiring committee (2008).
- S. Boldo, national CR1 and CR2 hiring committee in 2012.
- S. Boldo, Saclay and Sophia-Antipolis CR2 hiring committees in 2013.
- É. Contejean, hiring committee for an assistant professor position at IRCAM & University Paris 6 (Spring 2013).
- S. Boldo, member of hiring committee of a communication engineer (IR-COM1) for the INRIA, 2010.
- C. Marché, M. Pouzet and X. Urbain: hiring committee for one assistant professor position at ENSIE, in Evry (spring 2010).
- M. Pouzet, hiring committee for a full professor position at Ecole Supérieure d'Informatique et Applications de Lorraine (ESIAL) in Nancy (spring 2010).

- L. Mandel, hiring committee for one assistant professor position at ENSIMAG, in Grenoble (spring 2010).
- C. Paulin, Saclay CR2 hiring committee (2008), national DR2 hiring committee (2008, 2009, 2010), Sophia-Antipolis CR2 committee (2009), Nancy-Lorraine CR2 committee (2010).
- C. Paulin, hiring committees of assistant professor positions at ENS Cachan (2009) Ecole des Mines de Nantes (2009) University Paris 7 (2010, 2011, 2013), professor positions at ENS Lyon (2009), ENSEEIHT Toulouse (2011) CNAM (2012) ENS Cachan (2013).
- C. Paulin, hiring committees of assistant professor and positions at University Paris-Sud (MCF chaire INRIA 2010, Professor 2012 & 2013), president of an hiring committee for a professor position at University Paris-Sud in 2011.
- X. Urbain, hiring committee for two assistant professor positions at UPB/ENSEIRB-MATMECA, Bordeaux (Spring 2010).
- X. Urbain, hiring committee for an assistant professor position at École Centrale, Paris (Spring 2011).
- S. Boldo was in the committee in charge of selecting an Inria support staff (TR, *technicien de recherche*) for the Saclay finance and accounting service (SAF), 2012.

PhD and Habilitation Juries

- V. Benzaken: president (2) reviewer (6 PhD) examiner (8 PhD -3 HdR)
- S. Boldo: examiner (1)
- J.-C. Filliâtre: reviewer (3 times), examiner (2)
- C. Marché: president (5), reviewer (4), examiner (3)
- C. Paulin: president (2), reviewer (5), examiner (3)
- M. Pouzet: president (2), reviewer (3)

1/ Toccata

Interactions with the social, economic and cultural environment

Industrial Collaborations, Transfer

Industrial contracts are listed in Section 5.1.

Direct transfer

- Airbus France expressed in 2009 the wish to integrate our tool Alt-Ergo in its process of certification of the critical softwares in their next generation planes. We thus started the procedure of *qualifying* Alt-Ergo in the sense of the DO-178B norm, which fixes the constraints on software development to achieve certification of an avionics software. This was done as part of the *ADT Alt-Ergo* and also funded by a bilateral contract. The technical documents (functional specifications and benchmark suite) have been accepted by Airbus in 2011. These documents are submitted by Airbus to the certification authorities in 2012.
- Since 2010, Alt-Ergo is used in the Spark Pro toolset, developed by Altran-Praxis, for the engineering of high-assurance software. Alt-Ergo can be used by customers as an alternate prover for automatically proving verification conditions. Its usage is described in the new edition of the Spark book (<http://www.altran-praxis.com/book/>, Chapter "Advanced proof tools")
- since 2010, in the context of the Hi-Lite project, the AdaCore company (Paris) implements a new tool GnatProve which aims at formal verification of Ada programs. They translate annotated Ada code into the Why3 intermediate language and then use the Why3 system to generate proof obligations and discharge them with Alt-Ergo, or other available back-end provers. GnatProve is a prototype that aims at becoming the successor "Spark2014" of Spark (<http://www.open-do.org/2012/11/30/future-version-of-spark-will-be-based-on-ada-2012/>).

Industrial collaborations

- S. Conchon has started a collaboration with S. Krstic and A. Goel (Intel Strategic Cad Labs in Hillsboro, OR, USA) that aims in the development of an SMT-based model checker. With A. Mebsout and F. Zaidi (ForTesSe, LRI), they implement the Cubicle model checker which uses the Alt-Ergo theorem prover to discharge its proof obligations.
- J.-C. Filliâtre and C. Marché started in 2011 a collaboration with D. Mentré at Mitsubishi Electric R&D Centre Europe (Rennes), about the use of the Why3 environment and its back-end provers as an alternative to the built-in prover of Atelier B. This collaboration leaded first to a publication (95) and then become part of the new ANR project BWare.
- S. Conchon, A. Mebsout and F. Zaidi (ForTesSe team, LRI) continued their collaboration with S. Krstic and A. Goel (Intel Strategic Cad Labs in Hillsboro, OR, USA) that aims in the development of the SMT-based model checker Cubicle (<http://cubicle.lri.fr>).

Standardization efforts

- S. Boldo and G. Melquiond have participated in the revision of the IEEE-754 (1985) standard on floating-point arithmetic. The new 2008 standard has been approved in June and it is the official standard since August 2008. Both names appear in the author list; An article by S. Boldo appears in the bibliography.
- G. Melquiond also participates in the meetings of the IEEE-1788 standardization committee on interval arithmetic. The "Technology Transfer and Innovation" INRIA department is funding his travel expenses till late 2011.

Invited presentations at various Transfer forums

- C. Marché presented the techniques of deductive verification for checking safety properties at the "séminaire de réflexion-programmes du CEA-LIST", Dreux, France, March 25th, 2008.
- C. Marché presented our deductive verification approach for C programs at the "Workshop Airbus/partners on formal verification tools strategy", Toulouse, France, December 4-5, 2008.
- The tools Frama-C, Why and Alt-Ergo were presented at the Imatch day on 23 november 2010, on the themes of security and proof of programs (C. Marché, S. Conchon, C. Paulin) <http://www.inria.fr/centres-de-recherche-inria/saclay-ile-de-france/agenda/imatch-securite-preuve-de-programmes>
- Journées INRIA-Industrie in Toulouse, 2010: Sylvain Conchon presented a demo of the Alt-Ergo theorem prover.

Popularisation of Research Results

Fête de la science and other such events

- F. Plateau and Y. Moy prepared an activity related to logics for the "Fête de la science" 2008. Six team members animated this activity that one hundred children attended to.
- S. Boldo prepared an activity related to programs and astronomy for the event "10e Salon de la culture et des jeux mathématiques" (2009). It is based on an OCaml program that gives an accurate graphical representation of the night sky, from any location on Earth, at any date and time. Three team members animated this activity that was reused for the event "Fête de la science" 2009. Four team members animated this activity.
- C. Auger and S. Conchon gave a talk at "Fête de la science" 2009 about the order of magnitude of problems computer science has to deal with. The goal of this talk was to show that naive brute force algorithms can not solve many problems occurring in practice, even with the help of billions of supercomputers. This talk has also been given by S. Conchon during the award ceremony of "Olympiades de mathématiques" on May 2009.
- Three team members created and animated the event "Salon de la Culture et des Jeux Mathématiques", Paris, May 2010 jointly with Y. Régis-Gianas, pi.r2 team, INRIA Paris-Rocquencourt. This activity was reused for the event "Fête de la science" 2010. Four team members animated this activity for children and the general public.
- S. Boldo, head for the Fête de la science for the LRI laboratory in 2012. The laboratory welcomed both industrials, pupils and general public: 6 different stands, 6 classes, a total of more than 250 visiting persons. Two other team members welcomed the public.
- S. Boldo and A. Charguéraud belong to the organization committee of the *Castor informatique* <http://castor-informatique.fr/>, an international competition to present computer science to pupils (from 6ème to terminale). More than 91,000 teenagers played on the 40 proposed exercises in November 2012.

Talks and documents

- S. Boldo was interviewed in March 2008 by J. Jongwane for a podcast on the interstices web site: <http://interstices.info/a-propos-calcul-ordinateurs>.
- S. Boldo gave a talk at "Unithé ou café" on January 2008 to popularize issues related to floating-point arithmetic flaws to all the INRIA Saclay - Île-de-France staff.
- S. Boldo was invited to write a popular science article about programming in DocSciences, a magazine edited by the "Académie de Versailles". This special issue of November 2008 is co-edited with the INRIA and is about the basics of computer science (136). This article was then put on the popular science web site interstices.
- S. Boldo gave a talk for mathematic and technology secondary school teachers. On June 10 th and 16th 2009, the teachers attended several talks in a seminar called "Formation Informatique et Objets Numériques" in order to prepare a computer science option in the secondary schools of the academy of Versailles. A CD was edited by the INRIA with all participants' talks, and the talks are also available on <http://www.inria.fr/rocquencourt/ressources/multimedia/formation-informatique-et-objets-numerique/>.
- S. Boldo gave several talks for mathematic teachers: at the assembly of secondary school teachers on October 14th, 2009, at Intertice on May 10th 2010 (a meeting for teachers about teaching and TICE), at the IUFM on June 3rd 2010.

- G. Melquiond animated the INRIA stand at the European Research Carrier Fair in Berlin, May 28, 2009.
- S. Boldo is invited speaker on December 8th 2009 at a special day for a hundred secondary school girls (15-16 years old) to promote women in mathematics and computer science.
- S. Boldo wrote an article in 2010 for the popular science web site *interstices* about the fact that it is always the computer's fault: <http://interstices.info/idee-recue-informatique-18> (137).
- S. Boldo was invited to participate to the web-TV of the Cité des Sciences et de l'Industrie for the show *Qui veut gagner des neurones?* about computer science in 2010: <http://www.universcience.tv/media/1340/l-informatique.html> (138).
- S. Boldo, in collaboration with T. Viéville (INRIA Nancy Grand-Est) wrote two chapters of the book "Introduction à la science informatique", edited by G. Dowek (127, 128). This 2011 book aims at helping the secondary school teachers for the incoming computer science teaching.
- S. Boldo, brief news on "Mathématiques de la planète Terre" <http://mpt2013.fr/meme-les-ordinateurs-font-des-erreurs/>
- C. Paulin gave a talk at "Unithé ou café" on February 2012 to popularize issues related to proof theory to all the INRIA Saclay - Île-de-France staff.
- C. Paulin was interviewed by 01 Business & Technologies about education in Computer Science in the context of the labex DigiCosme, the paper was published in May 2012.

Management

- Since April 2008, S. Boldo is member of the editorial committee of the popular science web site *interstices* <http://interstices.info/>.
- From July 2009 to 2011, S. Boldo is elected member of the board of the Animath association that promotes mathematics among young people.
- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- S. Boldo, member of the popularization committee, *comité de médiation scientifique*, of Inria.
- S. Boldo is responsible for a *mission doctorale* for popularization. She is in charge of Li Gong of the LIMSI laboratory.

1/ Toccata

Strategy and five-year project

The Toccata group fused — as part of a general restructuring of the LRI — in July 2013 with the ForTesSE team to a new group VALS. A self-assessment of the former Toccata team and the resulting strategy and five-year project of the new VALS group can be found in Section 3.1.

Notice that Toccata's life will continue as an Inria project-team, which is still in the Inria creation process at the current time, which must continue independently of LRI restructuring.



2/ Implication dans la formation par la recherche

Implication dans la formation par la recherche

Tocata

2/ Implication dans la formation par la recherche

Training and Education

Schools for Junior Researchers

- Winter School on Verification of Object-Oriented Programs (Viinistu, Estonia, 25-29 January 2009), C. Marché, lecture on the Krakatoa tool (4h course + 1h practical lab, <http://krakatoa.lri.fr/ws/>) (?).
- 1st Asian-Pacific Summer School on Formal Methods (Beijing, China, August 24-31, 2009, <http://formes.asia/cms/coqschool/2009>), G. Melquiond, lecture on the SSreflect Coq tactic, and lecture on the Why tool.
- 8th LASER Summer School on Software Engineering <http://laser.inf.ethz.ch/2011/>: "Tools for Practical Software Verification", C. Paulin (4h) (?)
- GDR Informatique-Mathématique school for young researchers: "Arithmétique des ordinateurs et preuves formelles" (?), S. Boldo (2h), G. Melquiond (2h).
- École Jeunes Chercheurs en Programmation (EJCP 2012): J.-C. Filliâtre, "Vérification Dédutive de Programmes avec Why3" (4h, <http://why3.lri.fr/ejcp-2012/>) (?).
- Organization of DigiCosme Spring School 2013, April 22-26, 2013, C. Marché, <http://digicosme.lri.fr/Spring+School+2013>
- DigiCosme Spring School 2013, J.-C. Filliâtre, "Deductive Program Verification with Why3" (3h, <https://www.lri.fr/~marche/DigiCosmeSchool/filliatre.html>)

Graduate Courses

- Master Parisien de Recherche en Informatique (MPRI) <http://mpri.master.univ-paris7.fr/>
 - *Automated Deduction* (<https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-5>): É. Contejean, 2008-2009 (12h), 2009-2010 (12h), 2010-2011 (12h), 2011-2012 (12h) 2012-2013 (10h30); X. Urbain, 2009-2010 (12h), 2010-2011 (12h), 2011-2012 (12h) ; S. Conchon 2011-2012 (9h)
 - *Proof assistants*: C. Paulin, 2008-2009 (12h), 2009-2010 (6h), 2010-2011 (6h), 2011-2012 (6h) ; G. Melquiond, 2010-2011 (9h), 2011-2012 (9h)
 - *Synchronous Systems*: M. Pouzet, 2008-2009 (12h), 2009-2010 (12h)
 - *Foundations of proof assistants*: S. Boldo, 2009-2010 (10h), 2010-2011 (2h)
 - *Proofs of Programs* (<http://www.lri.fr/~marche/MPRI-2-36-1/>): C. Marché, 2011-2012 (12h), 2012-2013 (12h) ; G. Melquiond, 2011-2012 (12h), 2012-2013 (12h).
- Professional Master ISIC *Ingenierie des Systèmes Industriels Complexes* (École Polytechnique, University Paris-Sud 11 and INSTN, <http://www.dix.polytechnique.fr/chaire-systemes-complexes/>)
 - *Synchronous Programming*: Marc Pouzet, 2008-2009 (24h), 2009-2010 (24h)
- Master Informatique (Université Paris-Sud)
 - *Compilation* (M1): C. Paulin, 2010-2011 (50h), D. Baelde 2010-2011 (28h) , S. Conchon, 2011-2012.
 - *Compilation* (Polytech): C. Dross, 2011-2012
 - *Projet de compilation* (M1): R. Bardou, 2010-2011 (64h) A. Tafat, 2011-2012 (33h), M. Iguernelala 2011-2012 (33h)



3/ Strategy and five-year project

Strategy and five-year project

VALS

3/ Strategy and five-year project

Strategy and five-year project

Following the general policy of the LRI that suggests to group similar activities in larger teams, we decided to join the former teams ForTesSE and Toccata. The name of this new team is VALS, standing for "Verification/Validation of Algorithms, Languages and Systems". We detail below why this fusion makes sense in a scientific point of view.

VALS team members

The new team is directed by Burkhard Wolff, aside with Claude Marché as co-director.

Permanent Members (October 1st, 2013)			
<i>Name</i>	<i>First name</i>	<i>Position *</i>	<i>Institution</i>
BENZAKEN	Véronique	PREX	PARIS SUD
BOLDO*	Sylvie	CR1	Inria
CHARGUÉRAUD*	Arthur	CR2	Inria
CONCHON*	Sylvain	PR2	PARIS SUD
CONTEJEAN*	Évelyne	CR1	CNRS
FILLIÀTRE*	Jean-Christophe	CR1	CNRS
GAUDEL	Marie-Claude	PR émérite	PARIS SUD
LONGUET	Delphine	MCF	PARIS SUD
MANDEL**	Louis	MCF	PARIS SUD
MARCHE*	Claude	DR2	Inria
MELQUIOND*	Guillaume	CR1	Inria
NGUYEN	Kim	MCF	PARIS SUD
PASKEVICH*	Andrei	MCF	PARIS SUD
PAULIN-MOHRING*	Christine	PREX	PARIS SUD
VOISIN	Frédéric	MCFHC	PARIS SUD
WOLFF	Burkhard	PR1	PARIS SUD
ZAÏDI	Fatima	MCF	PARIS SUD

* member of the LRI-Inria joint team Toccata, directed by C. Marché.

** currently on leave ("détachement") at the Collège de France.

Temporary Personnel (October 1st, 2013)				
Name	First name	Position *	Institution	
AÏSSAT	Romain	Doc.	PARIS (AM)	SUD
CLOCHARD	Martin	Doc.	ENS Paris	
DROSS	Claire	Doc.	AdaCore (CIFRE)	
DUMBRAVA	Stefania	Doc.	PARIS (AM)	SUD
FELIACHI	Abderrahmane	Post-doc	EURO-MILS	
GONDELMAN	Léon	Doc.	PARIS (ANR grant)	SUD (BWare grant)
IM	Hyeonseung	Post-doc	PARIS (ANR grant)	SUD (Typex grant)
KHEFIFI	Rania	Doc.	PARIS (CDD)	SUD
LELAY	Catherine	Doc.	Inria (Digiteo PhD grant)	
MARTIN-DOREL	Erik	Post-doc.	Inria (ANR Verasco grant)	
MEBSOUT	Alain	Doc.	PARIS (AM)	SUD
NEMOUCHI	Yakoub	Doc.	PARIS (CDD)	SUD
NGUYEN	Huu Nghia	Doc.	PARIS (AM)	SUD
TAFAT-BOUZID	Asma	Post-doc	PARIS (ATER)	SUD
TUONG	Frédéric	Doc.	IRT (CDD)	SystemX
WENZEL	Markus	Post-doc	ANR Paral-ITP	

Self Assessment

Strengths: One of the particular strengths of both former teams ForTesSE and Toccata are their tradition of combining theory and practice, fundamental and applied research. Their research ranges from semantic models for specification- and programming languages, over concrete know-how in automated and interactive theorem-prover technology, down to the design and implementation of recognized tools and tool-chains for a variety of verification techniques. Successful applications, partly in collaboration with industrial partners, demonstrate that VALS will belong to the global players in the field of applied formal methods.

Both former parts of the VALS team have a strong national and international network with academic and industrial partners. We engage in various ANR and European projects. We also have intense local cooperation with major scientific players on the plateau de Saclay such as the CEA; here lies the key for its success in the development of recognized formal methods tools in an academic environment, together with the fact that it attracted a high number of permanent researchers.

Both former parts of VALS have a strong publication record and a high academic recognition in their respective fields, which is reflected in the participation of numerous program committees and conference organizations.

We'd like to add that we enjoy our collaborative style of research and the vividness of our group.

Weaknesses: While VALS has a clear focus on the foundational research axes, it can be asserted that its efforts in the various application domains is quite scattered driven by a perhaps too large variety of partnerships and collaborations. It would be desirable if the number of collaborations could be reduced to a smaller number of larger/more intensive partnerships.

With respect to the former Toccata part of the VALS team, it was criticized in the past that its collaborations are too French-centric. It was also recommended to address fundamental computing trends like concurrency more actively.

With respect to the former ForTesSE part of the VALS team, it can be criticized that its permanent staff is slightly over-aged, and needs a more active recruiting strategy to attract strong personal and to achieve a size which is more sane. It is particularly desirable that full-time researchers join the team on testing issues.

In order to maintain the quality of tools and documentation, the team should be reinforced by engineers.

Opportunities: The world of computing is changing: becoming ubiquitous, there are larger, more complex and more safety- and security-critical software systems whose quality must be assured by appropriate verification technologies. This is reflected by the growing demand for formal certification processes, e.g. Common Criteria ISO/IEC 15408 require the use of formal methods, both in Test and Proof, as developed in VALS.

Finally, it can be observed that there is for all tools (Frama-C, SparkAda, Isabelle, HOL-TestGen) an increasing number of users — reflected both by downloads and mailing list traffic.

New computing architectures — parallel / grid / cloud — represent new ways to master the inherent complexity of symbolic computing as is fundamental for the technologies developed in VALS. Such changes of basic technologies will have a profound effect both on verification methods, their demand by industrial partners, as well as their implementation.

Last but not least, we view the changes of the academic environment (catchword: Université Paris-Saclay) as a means to integrate verification engineering into traditional software engineering, which can be anchored more intensively into the bachelor and master programme of this institution — a way, to instruct and attract new scientific staff.

Threats: Advancing both fundamental research *and* tool development in an academic environment puts a team inevitably under a certain stress: Development of research tools is time-consuming and not always rewarding in terms of publications. While both former parts of VALS managed this balancing act quite well in the past, it can be safely stated that the complexity of underlying technology (e.g. multi-core architectures) and the demands of wider user groups (user interfaces, documentation) is growing. There is a perceivable threat that in the competition with industrial research institutions such as Microsoft Research, VALS might be outperformed simply by their investments both in terms of time and money. Just an example for the kind of concurrency we face: the white-box fuzz-testgeneration tool SAGE uses a ca. 100 man year effort involving a massive parallel server farm to solve billions of constraints by Z3; the approach is used to systematically detect errors in Win7, Windows and Office.

As mentioned earlier, it is particularly difficult to attract PhD students and scientific staff that fits into our profile: the necessary combination of mathematics, logic and software engineering is difficult to find on the national and international market of applicants.

In principle, the underlying technologies of our research are remarkably computing intensive, which is a problem when scaling-up to industrial size systems. An obvious answer to this threat are new computing paradigms (massive parallel computing, multi-core and grid computing); in order to cope with these trends, additional training and personnel will be necessary.

Strategy

Why does the fusion make sense? Test and proof, originally perceived as adversaries, have a lot in common in leading edge approaches: as “formal methods” (FM), they have both their roots in logic and discrete mathematics, and they share an interest in formal semantics for programming and specification languages, in modeling-approaches for programs and systems, as well as constraint-solving technologies and theorem provers. This mutual interest is reflected by recent collaborations between Toccata and ForTesSE (the Cubicle project). Last but not least, we identified a set of challenges that both former parts of the team would like to address together, listed below.

General objectives. We identified the following general trends in the scientific community that corresponds to our potential in the new VALS team:

1. making verification an easier to use, more wide-spread technology ;
2. gaining experience in non-standard application domains, for example hybrid and concurrent systems ;
3. advancing the prover technology: e.g. by non-linear arithmetic and parallel prover design ;
4. combining test and proof, e.g. by invariant-generation, verified optimized test-generations, etc. ;
5. combining proofs and probability.

We believe that the fused VALS team is an adequate structure, joining complementary skills and expertise of its members, to address these objectives. The detailed scientific programme below corresponds to the way we plan to implement solutions to these objectives.

Scientific Programme

The scientific programme of VALS is structured into six activities. We detail each of these activities below, together with the list of participants. We then provide a list of a few challenges that we want to address in the future. The interest in those challenges is shared between the former parts of the team. We then discuss the application domains we target, and finally give a few elements of positioning.

Activities

Automated Deduction. Participants: S. Conchon (contact), F. Zaïdi, E. Contejean, G. Melquiond, A. Paskevich.

Automated Theorem Proving and its applications will remain an important activity of the team. This includes research around satisfiability modulo theories (Alt-Ergo prover), numerical constraint solving (Gappa solver), and applications like SMT-based model-checking (Cubicle).

Verified Computer Arithmetic. Participants: S. Boldo (contact), G. Melquiond, C. Marché, B. Wolff.

The research around numerical programs took a lot of importance in the past 5 five years in particular in Toccata. We want to pursue these efforts, towards several directions such as the verification of numerical analysis systems, hybrid systems.

Formalisation of Languages. Participants: B. Wolff (contact), E. Contejean (contact), A. Charguéraud, D. Longuet, V. Benzaken, Ch. Paulin, C. Marché, S. Boldo.

Formalizing in a broad sense is indeed an activity of all members of former teams, in particular using assistants like Coq and Isabelle. It will continue in the future, for formalizing semantics of languages, concurrency, mathematical/numerical theories, etc.

Data-Centric Languages and Systems. Participants: V. Benzaken (contact), K. Nguyen, E. Contejean. This activity aims at designing and developing programming languages as well as systems that seriously take into account massive data. This includes improving existing languages and systems. Ultimately it aims at providing formally verified implementations of data intensive management systems.

Formal Model-based Testing. Participants: F. Zaïdi (contact), B. Wolff, D. Longuet, F. Voisin, M.-C. Gaudel. Testing will remain a strong research activity of the team. Important directions will be to scale up testing techniques by handling efficiently the concurrency aspects of distributed systems (Web services, wireless self-organised networks, etc.) as well as by advancing symbolic approaches. Moreover, we will investigate how to overcome the infeasible paths issues for the test of C programs by finding suitable combinations with static analysis methods.

Deductive Program Verification. Participants: J.-C. Filliâtre (contact), A. Charguéraud, A. Paskevich, C. Marché, G. Melquiond, Ch. Paulin, B. Wolff.

Our approach of deductive program verification is in need for improved techniques for modular reasoning, support for genericity, for higher-order programs, for refinement-based approaches. This is a key towards scaling-up, in particular via the development of reusable verified libraries.

Transverse challenges we want to address, shared by both former teams

Non-linear arithmetic. Critical software often involves numerical computations on physical quantities. *Hybrid systems* are those which mix continuous quantities and discrete ones. Such a system can be modeled typically by transitions systems guarded by numerical constraints. In all cases, the constraints involved are usually non-linear ones, hence both in the contexts of testing and proving, it is desirable to rely on automated decision procedures able to check the satisfiability of such kind of constraints.

Parallelism and verification. The challenge raised by parallelism in the context of verification is two-fold: a challenge as a target as well as an implementation means of verification tools. Besides the challenge of modeling concurrence, already addressed in the activity *Formalisation of Languages*, there is the necessity to profit from advances in recent hardware: since 2005, there are no further increases of CPU clock-rates; increasing computing power can only be gained by addressing multi-core and grid computing platforms. This represents a sensible paradigm shift both in algorithmic design as well as system architecture.

Combination of dynamic and static analysis. Combining the respective power of dynamic methods (test, run-time checking) and static analysis is an interesting research direction per se, and is certainly a way to leverage adoption of formal methods in industry. It is indeed required in certification processes in industry. We already have short-term plans to go in such a direction, in the context of platforms like Spark2014 for Ada, Frama-C for C code (and its executable-ACSL specification language), but also in our own platform Why3 for which we plan to provide an environment for directly executing annotated programs.

Verified languages, systems and tools An emerging trend is the verification of the analysis tools themselves, as exemplified by the CompCert verified compiler. The assurance level provided by a system is directly related to the size of its *Trusted Code Base*, i.e. the core of the system that is not verified, the remaining being verified on top of that core. Libraries (e.g. Flocq, ALEA) and tools (e.g. HOL-TestGen) built on top of assistants (e.g. Coq, Isabelle/HOL) have a small TCB, whereas standalone tools (e.g. automated theorem provers) have a large one. This challenge aims at reducing the TCB of such tools to small cores, thus producing “verified” tools. We target the development of verified theorem provers, verification condition generators, interpreters, compilers including compilers for data-centric languages, etc.

Probabilities and Verification Scaling-up to large size systems is always a challenge for formal methods. The use of randomized methods is a very promising approach to solve scaling-up issues, ensuring a probabilistic guarantee of the results. Randomized methods have a great potential to apply on many domains including formal testing and proving. Besides, studying verification of randomized programs and systems, which have important application in security, must be continued.

Application areas

VALS will continue to seek for academic and industrial partners to advance and apply its technologies; this covers in particular projects concerning code-verification (in particular numeric algorithms involving floats), security infrastructures, web services, embedded and operating systems, etc. We will try to find more strategic partnerships with companies and larger shares in research projects.

Positioning in the local, national and international context

The domain of formal methods for software engineering is historically a major axis of research in the LRI. This domain of research is important in the context of the institutional evolutions of the “Plateau de Saclay”, in the recent past, the present and for the future. In the past years, the RTRA Digiteo played an important role for the development of collaborative research on the Plateau, and Software Engineering was one of its seven themes of its research programme. In the present, software was also important in the “investissements d’avenir”: SciLex is one of the three action lines of the Labex DigiCosme, centered on the reliability of software ; the IRT SystemX, which is more focused on industrial applications, has one theme around embedded systems, where the same problematic appears. We are strongly involved in all these actions.

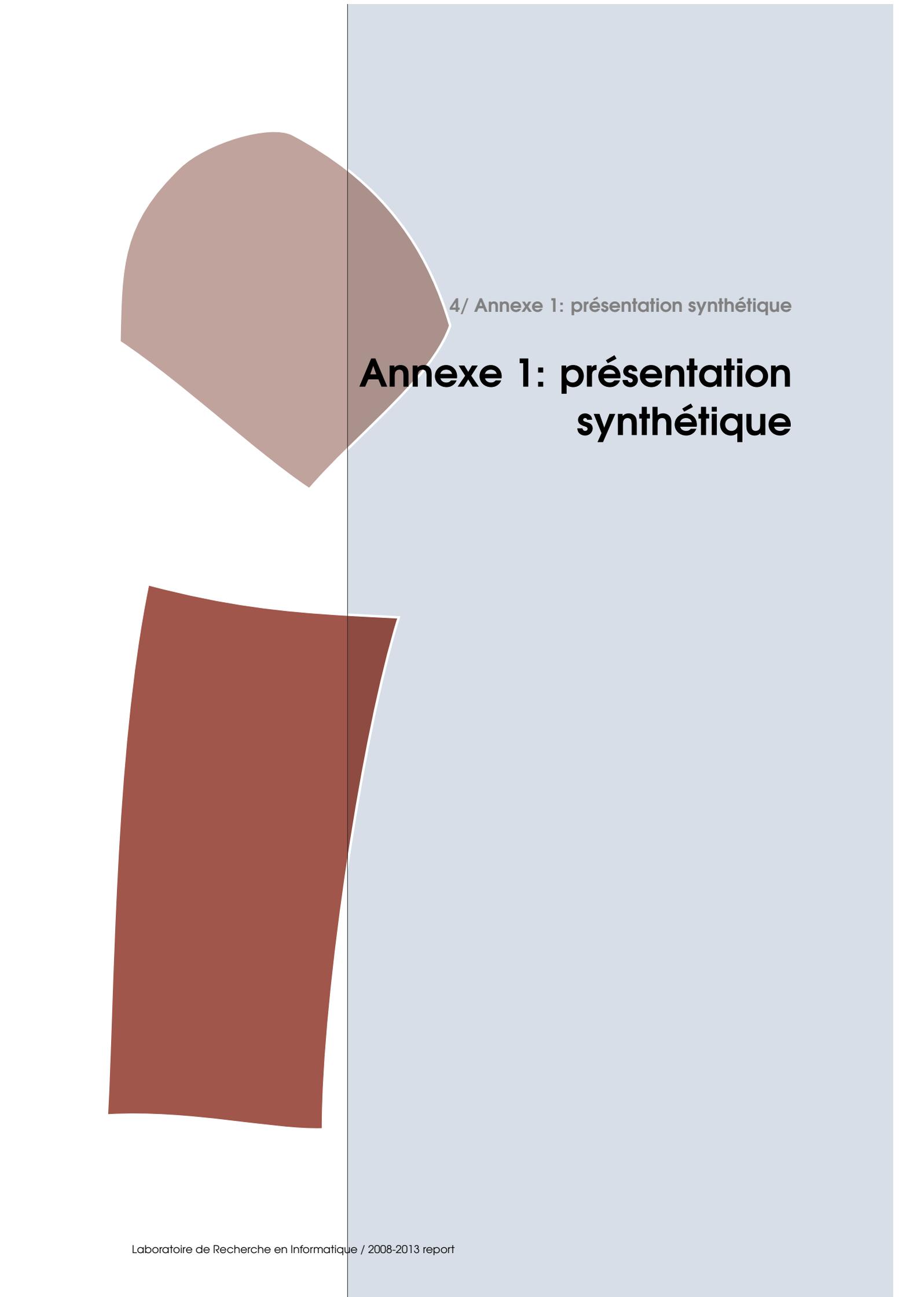
The near future is the creation of the Université Paris-Saclay, and the creation of a large computer science department. The interest in formal software engineering methods will be shared by several institutions: Inria Saclay, CEA, LSV, ENSTA ParisTech, etc. The new VALS team aims at playing a central role in this



future join of forces on the Plateau. Also, we are strongly involved in the new Master programme of the future STIC department. This would be a new mean to attract students, e.g. from engineering schools, to do a PhD thesis.

Our strategy also fits in the national context. We are members of both GDR of CNRS "Génie de la Programmation et du Logiciel" and "Informatique Mathématique". We will continue collaborations with many teams in France. At the international level, we want to develop our contacts with major institutions and sites of our domain, such as Microsoft Research, ETH Zürich, Imperial College London, etc. Our involvement in the IFIP WG 1.9/2.5 is also representative of our involvement in world-wide trends.

We plan to continue and improve our collaborations with industrial partners, in particular the companies that promote formal methods. These collaborations are not only a precious source of concrete challenges and real case studies: they are a key for the spreading and the transfer of our methods and tools in the industry.



4/ Annexe 1: présentation synthétique

Annexe 1: présentation synthétique

Toccata

Nom du responsable de l'équipe : **Claude MARCHÉ**, depuis janvier 2012 (Christine PAULIN jusqu'à décembre 2011)

Effectifs de l'équipe au 1er janvier 2008

5 enseignants-chercheurs ; 4 chercheurs ; 2 techniciens, ingénieurs et autres personnels ; 10 post-docs et doctorants.

Personnels ayant quitté l'équipe pendant le contrat en cours

- Marc Pouzet, Professeur Paris-Sud, mutation à l'UPMC mis à disposition de l'É.N.S. Paris en mars 2010.
- Laurence Puel, Professeur Paris-Sud, à la retraite depuis septembre 2012.
- total: 2 statutaires (71 mois) ; 13 doctorants, qui ont soutenu leur thèse durant cette période (326 mois) ; 7 post-docs (111 mois).

Nombre de recrutements réalisés au cours de la période considérée et origine des personnels

- Guillaume Melquiond, CR Inria 2008, était Post-doc lab. commun Inria-Microsoft-Research. Thèse É.N.S. Lyon 2006
- Andrei Paskevich, MCF Paris-Sud 2009, était Post-doc au CNAM. Thèse Univ. Paris 12 2007
- Véronique Benzaken, Professeur Paris-Sud, venue de l'équipe BD du LRI en 2010
- Kim Nguyen, MCF Paris-Sud 2010, était Post-doc au NICTA Sydney, Australie. Thèse Univ. Paris-Sud en 2008
- Arthur Charguéraud, CR Inria 2012, était Post-doc au Max Planck Institute for Software Systems, Kaiserslautern, Allemagne. Thèse Univ. Paris 7 en 2010

Production scientifique au cours de la période écoulée

1. Le développement de Why3, nouvelle génération de Why, a commencé en 2010. Il a rapidement atteint un état mature (articles Boogie 2011, ESOP 2013 et CADE 2013). Il est utilisé comme outil intermédiaire dans l'environnement Frama-C pour l'analyse statique de code C critiques (projet ANR U3CAT), et dans le futur environnement Spark2014 (projet FUI Hi-Lite) pour la vérification de codes Ada. Ces outils sont de plus en plus utilisés dans l'enseignement.
2. Le prouveur Alt-Ergo a atteint une maturité et un impact très significatif. Il a été qualifié par Airbus France pour utilisation dans le développement de code critiques. Il est utilisé depuis 2011 dans l'environnement SparkPro, et le sera dans Spark2014.
3. Étude d'un programme, écrit en langage C, résolvant numériquement (par discrétisation) une équation différentielle de propagation d'une onde acoustique le long d'une corde (projet ANR FOST). Preuve formelle complète de l'erreur de méthode introduite par le schéma de différences finies (article ITP 2010), et de l'erreur introduite par les arrondis dans les calculs (article ICALP 2009). Étude complète publiée dans le Journal of Automated Reasoning (2013).
4. La bibliothèque Coq ALEA (projet ANR SCALP) pour la formalisation des algorithmes randomisés a un impact important. Elle est utilisée dans d'autres développements certifiés, notamment pour l'environnement CertiCrypt pour la preuve de code cryptographiques, qui s'appuie sur un langage de programmation probabiliste au lieu du modèle algébrique de protocoles plus généralement adopté dans ce contexte.
5. Le model-checker Cubicle est le seul au monde à prouver automatiquement un protocole industriel de cohérence de cache (FLASH). Il a permis de recevoir un Academic Grant d'Intel pour l'année 2013, et continue à susciter de nombreux travaux de recherche (certification en Why3, nouveaux algorithmes d'inférence d'invariants, etc.). Collaboration fructueuse avec le Strategic Cad Lab d'Intel.

Bilan quantitatif des publications de l'équipe

- Articles de revue : internationales majeures 17 ; autres revues 5
- Articles dans des conférences et workshops : internationaux majeurs 48 ; autres conférences et workshops 51
- Livres et chapitres de livres : 8 ; éditions d'ouvrages : 3

5 publications majeures

- S. Conchon, É. Contejean, M. Iguernelala. "Canonized Rewriting and Ground AC Completion Modulo Shostak Theories". Tools and Algorithms for the Construction and Analysis of Systems (TACAS), volume 6605 of LNCS, pages 45-59, Saarbrücken, Germany, April 2011. Best EATCS paper award 2011.
- F. Bobot, S. Conchon, É. Contejean, M. Iguernelala, A. Mahboubi, A. Mebsout, G. Melquiond. "A Simplex-based extension of Fourier-Motzkin for solving linear integer arithmetic". 6th International Joint Conference on Automated Reasoning (IJCAR), volume 7364 of LNCS, pages 67-81, Manchester, UK, June 2012.

- S. Conchon, A. Goel, S. Krstic, A. Mebsout, F. Zaidi. "Cubicle: A parallel SMT-based model checker for parameterized systems". 24th International Conference on Computer Aided Verification (CAV), volume 7358 of LNCS, Berkeley, CA, USA, July 2012.
- A. Charguéraud. "Pretty-big-step semantics". 22nd European Symposium on Programming (ESOP), volume 7792 of LNCS, pages 41-60, March 2013.
- V. Benzaken, G. Castagna, K. Nguyen, J. Siméon. "Static and dynamic semantics of NoSQL languages". 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), Roma, Italy, January 2013.

5 (max) documents majeurs (autres que publications) En dehors des publications, notre production scientifique est surtout représentée par les nombreux logiciels que nous développons, tous distribués en Open Source (<http://toccata.lri.fr/tools.en.html>)

- Chaîne de vérification de code C : Frama-C (développé avec le CEA-List), Jessie/Why (déposé à l'APP) et Why3.
- Prouveurs automatiques : Alt-Ergo (déposé à l'APP) et Gappa
- Librairies Coq : Flocq, Alea, Coccinelle, Coquelicot
- CDuce, un langage fonctionnel orienté XML (<http://www.cduce.org/>)
- Cubicle, un model-checker basé sur l'approche SMT (<http://cubicle.lri.fr/>)

5 (max) faits illustrant le rayonnement ou l'attractivité académique

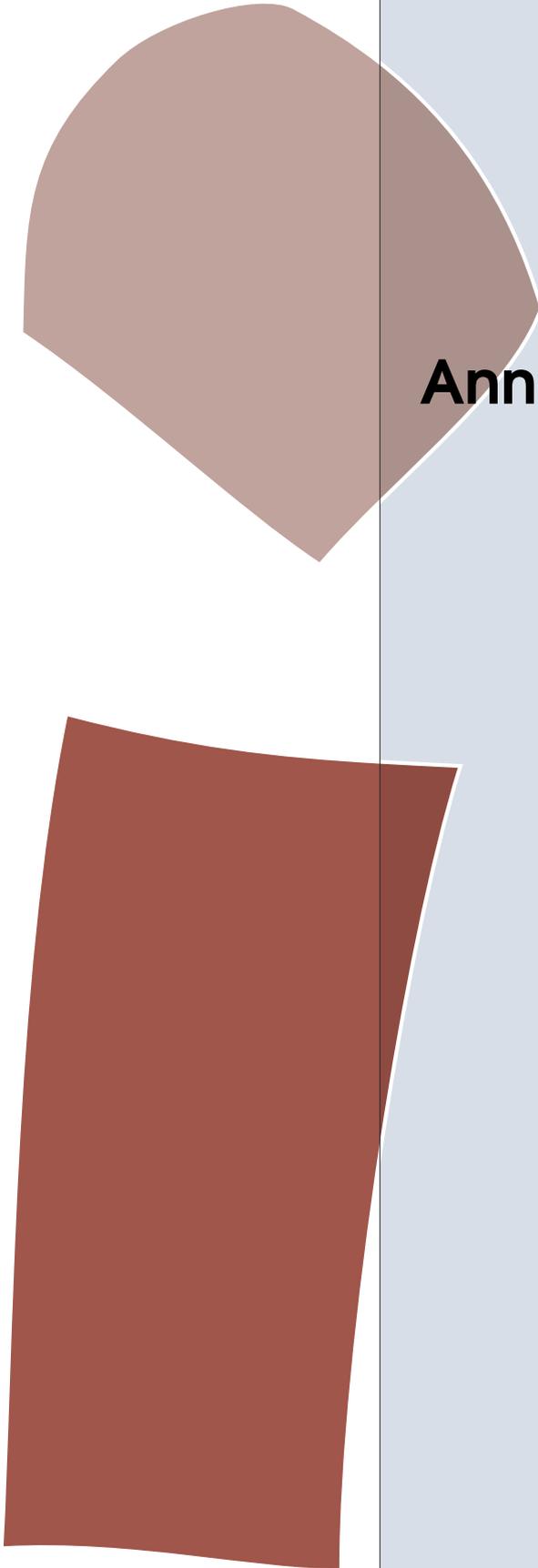
- S. Conchon, É. Contejean et M. Iguernelala ont obtenu le prix 2011 de l'EATCS (European Association for Theoretical Computer Science, <http://www.eatcs.org/index.php/best-etaps-paper>) pour le meilleur article théorique de l'ensemble des conférences ETAPS
- C. Paulin docteur honoris causa Université de Goteborg, Suède, octobre 2011
- Organisation de la conférence Internationale "Formal Verification of Object-Oriented Software", Paris, du 28 au 30 juin 2010, <http://foveoos2010.cost-ic0701.org/>
- Organisation de la compétition de vérification associée à la conférence VSTTE 2012, <https://sites.google.com/site/vstte2012/compet>
- J.-C. Filliâtre, membre de l'IFIP Working Group 1.9/2.15 (Verified Software) depuis 2011, <http://www.ifip.org/bulletin/bulltcs/memtc01.htm#wg19>

5 (max) faits illustrant les interactions de l'équipe avec son environnement socio-économique ou culturel

- Contrat industriel avec Airbus France : support pour maintenance et qualification d'Alt-Ergo pour son utilisation dans la certification de code critique avionique.
- Projet FUI Hi-Lite du pôle de compétitivité System@tic, <http://www.adacore.com/press/completion-of-project-hi-lite/>, débouchant sur le futur Spark2014.
- Plusieurs thèses CIFRE: avec Dassault Aviation, Gemalto, France Telecom, AdaCore.
- Concours Castor Informatique en lycées et collèges (<http://castor-informatique.fr/>). 92 000 participants en 2012.
- Articles de vulgarisation (<https://www.lri.fr/~sboldo/mediation.html>) et animations des fêtes de la science.

Principales contributions de l'équipe à des actions de formation

- Organisation de l'école de printemps DigiCosme 2013, "Program Analysis and Verification" du 22 au 26 avril 2013, <http://digicosme.lri.fr/Spring+School+2013>
- Cours au Master Parisien de Recherche en Informatique (<https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:cours2>) : "Démonstration automatique", "Assistants de preuve", "Preuve de programme".
- Cours donnés à des écoles de jeunes chercheurs : EJCP 2012 et 2013 (<http://why3.lri.fr/ejcp-2013/>), Laser 2011 (<http://laser.inf.ethz.ch/2011/>), FoVeOOS Winter School 2011 (<http://krakatoa.lri.fr/ws/>), EJCIM 2012 (<http://ejcim2012.irisa.fr/>), APSSFM 2009 et 2013 (http://sts.thss.tsinghua.edu.cn/APSSFM_2013)
- Articles sur le site Interstices https://interstices.info/jcms/c_36152/boldo



5/ Annexe 6: Realisations

Annexe 6: Realisations

Toccata

5/ Annexe 6: Realisations

Contracts and grants

Public contracts and grants (jan 2008 - jun 2013)				
Type	Name	Managing Institution	Start / Duration	Amount
ANR	Typex	Université Paris XI	01.2012 / 36 mo.	128.14 k€
ANR	FOST	INRIA	01.2009 / 36 mo.	56.64 k€
DIGITEO	HISSEO	INRIA	09.2008 / 36 mo.	106.32 k€
ANR	Bware	Université Paris XI	09.2012 / 48 mo.	166.99 k€
ANR	DECERT	Université Paris XI	01.2009 / 45 mo.	111.28 k€
ANR	A3PAT	CNRS	12.2005 / 42 mo.	93.50 k€
DIGITEO	PACTOLE	Université Paris XI	10.2009 / 36 mo.	7.00 k€
ANR	CAT	INRIA	12.2005 / 44 mo.	161.41 k€
ANR	CerPAN	CNRS	12.2005 / 42 mo.	56.00 k€
ANR	PARTOUT	Université Paris XI	01.2009 / 48 mo.	71.24 k€
ANR	VERASCO	INRIA	01.2012 / 48 mo.	164.37 k€
Subvention	CeProMi	INRIA	03.2008 / 21 mo.	25.00 k€
Subvention	CONVENTION D'ENSEIGNEMENT CATHER	INRIA	10.2011 / 12 mo.	6.17 k€
DIGITEO	DIM COQUELICOT	INRIA	09.2011 / 36 mo.	102.20 k€
Contrat européen	FVOOS	INRIA	05.2008 / 36 mo.	0.00 k€
Region IDF	HI-LITE	INRIA	05.2010 / 36 mo.	51.59 k€
ANR	U3CAT	INRIA	12.2008 / 36 mo.	123.54 k€
Contrat européen	EIT ICT LABS-KIC 2011	Université Paris XI	01.2011 / 12 mo.	23.81 k€
Contrat européen	EIT ICT LABS-KIC 2012	Université Paris XI	01.2012 / 12 mo.	54.81 k€
ANR	SCALP	CNRS	01.2008 / 48 mo.	18.32 k€
Contrat européen	TYPES	Université Paris XI	09.2004 / 44 mo.	43.00 k€
Subvention	IUF	Université Paris XI	01.2007 / 36 mo.	19.00 k€
ANR	SIESTA	Université Paris XI	12.2007 / 36 mo.	26.35 k€
Subvention	Synchronics	INRIA	01.2008 / 48 mo.	32.00 k€

Private contracts and grants (jan 2008 - jun 2013)

Type	Name	Managing Institution	Start / Duration	Amount
Industriel	AIRBUS - SPECIFICATION ALT-ERGO	INRIA	08.2010 / 5 mo.	35.00 k€
CIFRE	ADACORE	INRIA	01.2011 / 36 mo.	45.00 k€
CIFRE	DASSAULT-AVIATION	Université Paris XI	02.2005 / 36 mo.	20.00 k€
CIFRE	GEMALTO	Université Paris XI	05.2005 / 80 mo.	3.00 k€
CIFRE	FRANCE-TELECOM	Université Paris XI	01.2006 / 36 mo.	20.00 k€
Industriel	PFC	INRIA	01.2007 / 30 mo.	100.00 k€
CIFRE	ATHIS	Université Paris XI	02.2005 / 36 mo.	25.08 k€
Industriel	GENCOD	Université Paris XI	09.2007 / 24 mo.	79.36 k€

Deductive Program Verification

CAT

Partners: CEA List (Saclay, project leader), INRIA Rennes (Team Lande), Dassault Aviation (Saint-Cloud), Airbus France (Toulouse), Siemens.

See <http://frama-c.cea.fr>

Type: ANR
Amount: 161.41 k€
Duration: 44 months
Scientific director for LRI:
C. Marché

The goal of the project was to develop an open-source toolkit for analysing industrial-size C programs during development, verification, maintenance and evolution. The resulting environment is Frama-C.

CeProMi

Partners: Gallium team (INRIA Rocquencourt), Cassis team (INRIA Nancy), TFC team (LIFC, Besançon), DCS team (VERIMAG, Grenoble)

See <http://www.lri.fr/cepromi/>

Type: ARC Inria
Amount: 25.00 k€
Duration: 21 months
Scientific director for LRI:
C. Marché

The goal was to propose new theoretical bases for proving programs involving memory sharing and side effects (typically, pointer programs in C, objects in OO languages, records with mutable fields in ML).

There were three different levels of studies: extensions of specification languages with appropriate notions of invariants and description of side effects; design of advanced type systems and static analyses for detecting either alias or separation of pointers; design of verification conditions calculi incorporating notions of modules, pointer separation and refinement.

U3CAT

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).

See <http://frama-c.cea.fr>

Type: ANR
Amount: 123.54 k€
Duration: 36 months
Scientific director for LRI:
Marché

U3CAT (Unification of Critical C Code Analysis Techniques) aims at verification techniques of C programs, and is partly a follow-up of the former CAT project. 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.

Hi-Lite

Partners: AdaCore (project leader), Altran, Astrium Space Transportation, CEA-LIST, Thales Communications

See <http://www.open-do.org/projects/hi-lite/>

Type: FUI
Amount: 51.59 k€
Duration: 36 months
Scientific director for LRI:
C. Marché

Hi-Lite is a project in the SYSTEMATIC Paris Region French cluster in complex systems design and management. 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.

PFC

Partners: Gemalto, CEA-LIST, Trusted Logic

The PFC project (Plateforme de Confiance, trusted platforms) is a project in the SYSTEM@TIC Paris Region French cluster in complex systems design and management <http://www.systematic-paris-region.org>. This cluster involves industrial groups, SMEs and academic partners in the Paris-Region and is supported by the french government and the regional council.

Type: System@tic
Amount: 20.00 k€
Duration: 36 months
Scientific director for LRI:
C. Paulin-Mohring

The goal of the project is the conception and validation of secure and safe embedded applications.

Automated Deduction

BWare

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

See <http://bware.lri.fr>

Type: ANR
Amount: 166.99 k€
Duration: 48 months
Scientific director for LRI:
S. Conchon

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 (?). 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.

DECERT

Partners: IRISA/INRIA Rennes - Bretagne Atlantique (project leader), CEA List, LORIA/INRIA Nancy - Grand Est, , INRIA Sophia Antipolis - Méditerranée, Systeme

See <http://decert.gforge.inria.fr/>

The goal of the project DECERT (DEduction and CERTification) 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.

Type: ANR
Amount: 111.28 k€
Duration: 45 months
Scientific director for LRI:
S. Conchon

A3PAT

Partners: ENSIE (project leader), Inria Sophia, Labri, LRI

See <http://a3pat.ensie.fr/>

Aimed at helping proof assistants with trustworthy decision procedures, in particular by generating proof traces in order to build proof terms.

Type: ANR
Amount: 93.50 k€
Duration: 42 months
Scientific director for LRI:
É. Contejean

Alt-Ergo

Partners: External Collaborators: Airbus France (Toulouse), Dassault Aviation (Saint-Cloud), team Typical (INRIA, École Polytechnique).

See <http://alt-ergo.lri.fr/>

The goal is the maturation of the Alt-Ergo prover towards its use in an industrial context in particular for avionics. The expected outcomes of this ADT are the following:

- improving the efficiency of Alt-Ergo;
- fine tuning of Alt-Ergo for the SMT competition;
- generation of counter-examples;
- the qualification of Alt-Ergo for the norm DO-178B.

Type: ADT Inria
Amount: Montant k€
Duration: Duree months
Scientific director for LRI:
S. Conchon

Verified Libraries and Tools

SCALP

Partners: Verimag (leader), INRIA Sophia-Antipolis (Everest then Marelle team), ENS Lyon, LRI, CNAM.

See <http://scalp.gforge.inria.fr/>

The SCALP project (Security of Cryptographic Algorithms with Probabilities) aims at developing automated tools for the verification of cryptographic systems.

Type: ANR
Amount: 18.32 k€
Duration: 48 months
Scientific director for LRI:
C. Paulin-Mohring

Verasco

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

See <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

Type: ANR
Amount: 164.37 k€
Duration: 48 months
Scientific director for LRI:
G. Melquiond

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.

Coquelicot

Partners: LIX (Palaiseau), University Paris 13

See <http://coquelicot.saclay.inria.fr>

Type: Digiteo
Amount: 102.20 k€
Duration: 36 months
Scientific director for LRI:
S. Boldo

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

Pactole

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

See <http://pactole.lri.fr/>

Type: Digiteo
Amount: 7.00 k€
Duration: 36 months
Scientific director for LRI:
E. Contejean

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.

Computer Arithmetic

CerPAN

Partners: University Paris 13, INRIA and CNAM

See <http://www-lipn.univ-paris13.fr/CerPAN/>

Type: ANR
Amount: 56.00 k€
Duration: 42 months
Scientific director for LRI:
J.-C. Filliâtre

This project aimed at developing and applying methods which allow to formally prove the soundness of programs coming from numerical analysis techniques. We were more precisely working on problems related to the verification of floating point algorithms.

FOST

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

See <http://fost.saclay.inria.fr>

Type: ANR
Amount: 56.64 k€
Duration: 36 months
Scientific director for LRI:
S. Boldo

The FOST (Formal prOofs of Scientific compuTation programs) 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.

Hiseo

Partners: CEA List (Saclay, project leader), INRIA Paris-Rocquencourt (Team Gallium).

See <http://hiseo.saclay.inria.fr>

Type: Digiteo
Amount: 106.32 k€
Duration: 36 months
Scientific director for LRI:
S. Boldo



Hiseo 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 (? , ?).

Data-Centric Languages

Typex

Partners: PPS (CNRS & University Paris Denis Diderot), INRIA Rhône-Alpes (team Tyrex).

See <http://typex.lri.fr/>

Type: ANR
Amount: 128.14 k€
Duration: 36 months
Scientific director for LRI:
V. Benzaken

The goal of this project is to produce a new generation of XML programming languages stemming from the synergy of integrating three approaches into a unique framework: a logical approach, a data-oriented approach and a programming language approach. Languages whose constructions are inspired by the latest results in the PL research; with precise and polymorphic type systems that merge PL typing techniques with logical-solver-based type inference; with efficient implementations issued by latest researches on tree automata and formally certified by latest theorem prover technologies; with optimizations directly issued from their types systems and the logical formalizations and whose efficiency will be formally guaranteed; with the capacity to specify and formally verify invariants, business rules, and data integrity. Languages with a direct and immediate impact on standardization processes.

Synchronous Programming

PARTOUT

Partners: INRIA Mimosa (project leader), CNAM, LRI.

See <http://www-sop.inria.fr/mimosa/PARTOUT>

Type: ANR
Amount: 71.24 k€
Duration: 48 months
Scientific director for LRI:
L. Mandel

The goal of the project PARTOUT is, from a programming language point of view, to study the impact on programming of the globalization of parallelism which now covers all the spectrum of informatics, ranging from multicore architectures and distributed systems, up to applications deployed on the Web.

SIESTA

Partners: AIRBUS, Turbomeca, Hispano-Suiza, Onera, CEA List, Esterel-Technology, EADS, LRI, LIG.

See <http://www.siesta-project.com>

Type: ANR
Amount: 26.35 k€
Duration: 36 months
Scientific director for LRI:
M. Pouzet

This project addresses the automated testing of embedded systems implemented in SCADE or Simulink. M. Pouzet is involved on the architecture of the SCADE 6 compiler to integrate verification techniques. The challenge is to take new programming constructs (e.g., hierarchical automata, reset and general forms of clocks) into account to improve verification techniques and modularity.

Synchronics

Partners: INRIA Rhône Alpes (co-leader), IRISA, VERIMAG

See <http://synchronics.inria.fr/>

Type: Action d'Envergure
Inria
Amount: 32.00 k€
Duration: 48 months
Scientific director for LRI:
M. Pouzet

The goal of the project is to propose new languages for the development of embedded systems allowing *from a unique source* to both simulate the system with its environment and

generate code. It capitalizes on recent extensions of data-flow synchronous languages (Lucid Synchronic, ReactiveML), a relaxed form of synchrony, and means to mix discrete and continuous systems inside the synchronous model of time.

The project focuses on language extensions to increase modularity, dedicated type systems to ensure safety properties, efficient compilation and the mix of discrete and continuous time.

GENCOD

Partners: Dassault-Aviation, Thales, Esterel-Technologies, TNI, Airbus

The GENCOD project aims at defining methods to certify the Esterel compiler for hardware (Norm. DO 254, the hardware version of DO 178 B used for critical software)

Type: Industriel
Amount: 79.36 k€
Duration: 24 months
Scientific director for LRI:
M. Pouzet

5/ Annexe 6: Realisations

Software Licensing and Distribution

Each software we produce is freely distributed under some open-source licence.

Program Verification

Why3 - The Why3 platform

<http://why3.lri.fr/>

Contact: J.-C. FILLIÂTRE

Why3 is a platform for deductive program verification. It provides a rich language for specification and programming, called WhyML, and relies on external theorem provers, both automated and interactive, to discharge verification conditions. Why3 comes with a standard library of logical theories (integer and real arithmetic, Boolean operations, sets and maps, etc.) and basic programming data structures (arrays, queues, hash tables, etc.). A user can write WhyML programs directly and get correct-by-construction OCaml programs through an automated extraction mechanism. WhyML is also used as an intermediate language for the verification of C, Java, or Ada programs.

Why3 is a complete reimplementaion of the former Why platform. Among the new features are: numerous extensions to the input language, a new architecture for calling external provers, and a well-designed API, allowing to use Why3 as a software library. An important emphasis is put on modularity and genericity, giving the end user a possibility to easily reuse Why3 formalizations or to add support for a new external prover if wanted.

Krakatoa and Jessie - Tools for Java and C Program Verification

<http://krakatoa.lri.fr>

Contact: C. MARCHÉ

Krakatoa and Jessie are two front-ends of the Why platform for deductive program verification. Krakatoa deals with Java programs annotated in a variant of the The Java Modeling Language. Jessie is a Frama-C plug-in that deals with C programs annotated in the ANSI/ISO C Specification Language (ACSL).

Frama-C - Framework for Modular Analysis of C codes

<http://frama-c.cea.fr/>

Contact: C. MARCHÉ



Frama-C is a tool suite dedicated to the analysis of source code of software written in C. Frama-C gathers several static analysis techniques in a single collaborative framework. The collaborative approach of Frama-C allows static analyzers to build upon the results already computed by other analyzers in the framework. Thanks to this approach, Frama-C provides sophisticated tools, such as a slicer and dependency analysis. The development of Frama-C is led by CEA-List.

CFML - a Characteristic Formula generator for ML

<http://arthur.chargueraud.org/softs/cfml/>

Contact: A. CHARGUÉRAUD

CFML can be used to verify Caml programs using the Coq proof assistant. It is based on the concept of characteristic formulae. CFML consists of two parts: (1) a generator that parses Caml code and produces characteristic formulae expressed as Coq axioms (the generator itself is implemented in Caml) and (2) a Coq library that provides tactics for manipulating characteristic formulae interactively.

Automated Deduction

Alt-Ergo - The Alt-Ergo theorem prover

<http://alt-ergo.lri.fr/>

Contact: S. CONCHON

Alt-Ergo is an open source automatic theorem prover dedicated to program verification. It is an SMT solver based on CC(X): a congruence closure algorithm parameterized by an equational theory X. Alt-Ergo is based on a home-made SAT-solver and implements an instantiation mechanism for quantified formulas. It is used internally in several major verification platforms: Caveat, Frama-C, SparkAda 2005, Spark2014, EasyCrypt.

CiME - CiME, a tool box for automated deduction.

<http://cime.lri.fr>

Contact: E. CONTEJEAN

CiME is a rewriting toolbox. CiME3 is the last generation of it, its main new feature being the production of traces for Coq. The development of CiME3 is now led by the CPR team at CNAM/ENSIIE. <http://www.ensie.fr/~a3pat/online/cime3.php>

CUBICLE - A parallel SMT-based model checker for parameterized systems

<http://cubicle.lri.fr/>

Contact: S. CONCHON

Cubicle is an open source model checker for verifying safety properties of array-based systems. This is a syntactically restricted class of parametrized transition systems with states represented as arrays indexed by an arbitrary number of processes. Cache coherence protocols and mutual exclusion algorithms are typical examples of such systems.

Cubicle model-checks by a symbolic backward reachability analysis on infinite sets of states represented by specific simple formulas, called cubes. Cubicle is based on ideas introduced by MCMT from which, in addition to revealing the implementation details, it differs in a more friendly input language and a concurrent architecture. Cubicle is written in OCaml. Its SMT solver is a tightly integrated, lightweight and enhanced version of Alt-Ergo; and its parallel implementation relies on the Functor library.

Gappa - A tool for certifying numerical applications

<http://gappa.gforge.inria.fr/>

Contact: G. MELQUIOND

Gappa is a tool intended to help verifying and formally proving properties on numerical programs dealing with floating-point or fixed-point arithmetic. It has been used to write robust floating-point filters for CGAL and it is used to certify elementary functions in CRLibm. While Gappa is intended to be used

directly, it can also act as a backend prover for the Why software verification platform or as an automatic tactic for the Coq proof assistant.

Synchronous Programming

ReactiveML - The ReactiveML language

<http://rml.inria.fr>

Contact: L. MANDEL

A programming language for implementing interactive systems. ReactiveML combines the temporal expressiveness of synchronous languages with the power of functional programming.

Lucid Synchrone - An experimental language for the implementation of reactive systems.

<http://www.di.ens.fr/~pouzet/lucid-synchron/>

Contact: M. POUZET

Lucid Synchron serves as an experimental language and environment for the implementation of reactive systems. It is based on the synchronous model of time as provided by Lustre combined with some features from ML languages. It is a strongly typed, higher-order functional language managing infinite sequences or streams as primitive values. These streams are used for representing input and output signals of reactive systems and are combined through the use of synchronous data-flow primitives à la Lustre. The language is founded on several type systems (e.g., type and clock inference, causality and initialization analysis) which statically guaranty safety properties on the generated code. Programs are compiled into sequential imperative OCaml code.

Data Centric Languages

CDuce - An XML centric Programmimg Language

<http://www.cduce.org>

Contact: V. BENZAKEN

CDuce is a modern XML-oriented functional language with innovative features. A compiler is available under the terms of an open-source license. CDuce is type-safe, efficient, and offers powerful constructions to work with XML documents. It is included in major Linux distributions. CDuce has a very wide range of applications such as those listed at URL <http://www.cduce.org/appli.html>.

Objective Caml libraries and tools

Bibtex2html - Generator of HTML files from BibTeX bibliographic databases

<http://www.lri.fr/~filliatr/bibtex2html/>

Contact: J.-C. FILLIÂTRE

bibtex2html is a collection of tools for translating from BibTeX to HTML. They allow to produce, from a set of bibliography files in BibTeX format, a bibliography in HTML format. Bibtex2html is distributed as a package in most Linux distributions. Package popularity contests show that it is among the 20% most often installed packages. We estimate that between 10000 and 100000 web pages have been generated using Bibtex2html.

ocamlgraph - Ocaml graph library

<http://ocamlgraph.lri.fr/>

Contact: J.-C. FILLIÂTRE



OCamlgraph is a graph library for Objective Caml. Its contribution is three-fold: (1) an easy-to-use graph data structure together with several operations and algorithms over graphs, (2) several other graph implementations for those not satisfied with the one above and (3) several classic operations and algorithms over graphs. Ocamlgraph is used internally by Frama-C, Why3, Alt-Ergo, etc.

Mlpost - Mlpost, an Objective Caml interface to Metapost

<http://mlpost.lri.fr/>

Contact: J.-C. FILLIÂTRE

Mlpost is an Objective Caml interface to Metapost. It permits the generation of pictures directly from an OCaml program.

Functory - A functor is a place where functional workers are manufacturing programs

<http://functory.lri.fr>

Contact: J.-C. FILLIÂTRE

Functory is a distributed computing library for Objective Caml which facilitates distributed execution of parallelizable computations in a seamless fashion. Further, it is polymorphic, incorporates a robust fault-tolerant mechanism and is already being deployed in real-world applications.

Coq Libraries

Coccinelle - Coccinelle

<http://www.lri.fr/~contejea/Coccinelle/coccinelle.html>

Contact: E. CONTEJEAN

A Coq library for term rewriting. Besides the usual definitions and theorems of term algebras, term rewriting and term orderings, it also models some of the algorithms implemented in the CiME toolbox, such a matching, matching modulo associativity-commutativity, computation of the one-step reducts of a term, RPO comparison between two terms, etc. The RPO algorithm can effectively be run inside Coq, and is used in the Color library (<http://color.inria.fr/>) as well as for certifying Spike implicit induction theorems in Coq.

ALEA - A library for reasoning on randomized algorithms in Coq

<http://www.lri.fr/~paulin/ALEA/>

Contact: C. PAULIN-MOHRING

This library forms a basis for reasoning on randomized algorithms in the Coq proof assistant. It is developed in the framework of the SCALP project on Security of Cryptographic ALgorithms with Probabilities. It is notably used within the CertiCrypt environment.

Flocq Library - A formalization of floating-point arithmetic in Coq

<http://flocq.gforge.inria.fr/>

Contact: S. BOLDO

Flocq (Floats for Coq) is a floating-point formalization for the Coq system. It provides a comprehensive library of theorems on a multi-radix multi-precision arithmetic. It also supports efficient numerical computations inside Coq. Notably it is used in the CompCert verified compiler project, for proving that compilation of floating-point expression preserves their semantics.

Coq.Interval - The Coq.Interval library for automatically proving bounds of real-valued expressions

<http://www.lri.fr/~melquion/soft/coq-interval/>

Contact: G. MELQUIOND

This library provides tactics for simplifying the proofs of inequalities on expressions of real numbers for the

Coq proof assistant.

The Coquelicot library - A user-friendly Coq library for real analysis

<http://coquelicot.saclay.inria.fr/>

Contact: S. BOLDO

An easier way of writing formulas and theorem statements is achieved by relying on total functions in place of dependent types for limits, derivatives, integrals, power series, and so on. To help with the proof process, the library comes with a comprehensive set of theorems that cover not only these notions, but also some extensions such as parametric integrals, two-dimensional differentiability, asymptotic behaviors. It also offers some automations for performing differentiability proofs. Moreover, Coquelicot is a conservative extension of Coq's standard library and we provide correspondence theorems between the two libraries. We have exercised the library on several use cases: in an exam at university entry level, for the definitions and properties of Bessel functions, and for the solution of the one-dimensional wave equation.

5/ Annexe 6: Realisations

Publications

Journal articles

Major international journals

- (1) J. B. Almeida, M. Barbosa, Jean-Christophe Filliâtre, J. S. Pinto, and B. Vieira. CAOverif: An open-source deductive verification platform for cryptographic software implementations. *Science of Computer Programming*, Oct. 2012. <http://www.sciencedirect.com/science/article/pii/S016764231200189X>.
- (2) P. Audebaud and Christine Paulin-Mohring. Proofs of randomized algorithms in Coq. *Science of Computer Programming*, 74(8):568–589, 2009.
- (3) M. Dumas and Guillaume Melquiond. Certification of bounds on expressions involving rounded operators. *Transactions on Mathematical Software*, 37(1), 2010.
- (4) F. de Dinechin, C. Lauter, and Guillaume Melquiond. Certifying the floating-point implementation of an elementary function using Gappa. *IEEE Transactions on Computers*, 60(2):242–253, Feb. 2011.
- (5) A. Frisch, G. Castagna, and Véronique Benzaken. Semantic subtyping: dealing set-theoretically with function, union, intersection and negation types. *Journal of the ACM* 2008, 55(4):1–64, 2008.
- (6) S. M. Rump, P. Zimmermann, Sylvie Boldo, and Guillaume Melquiond. Computing predecessor and successor in rounding to nearest. *BIT Numerical Mathematics*, 49(2):419–431, June 2009.
- (7) Guillaume Melquiond. Floating-point arithmetic in the Coq system. *Information and Computation*, 216:14–23, 2012.
- (8) Jean-Christophe Filliâtre. Deductive software verification. *International Journal on Software Tools for Technology Transfer (STTT)*, 13(5):397–403, Aug. 2011.
- (9) Sylvain Conchon, Évelyne Contejean, and Mohamed Iguernelala. Canonized rewriting and ground AC completion modulo Shostak theories : Design and implementation. *Logical Methods in Computer Science*, 8(3):1–29, Sept. 2012. Selected Papers of the Conference *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2011)*, Saarbrücken, Germany, 2011.
- (10) Sylvie Boldo, F. Clément, Jean-Christophe Filliâtre, M. Mayero, Guillaume Melquiond, and P. Weis. Wave equation numerical resolution: a comprehensive mechanized proof of a C program. *Journal of Automated Reasoning*, 50(4):423–456, Apr. 2013.



- (11) Sylvie Boldo, M. Daumas, and R.-C. Li. Formally verified argument reduction with a fused-multiply-add. *IEEE Transactions on Computers*, 58(8):1139–1145, 2009.
- (12) Sylvie Boldo and J.-M. Muller. Exact and Approximated error of the FMA. *IEEE Transactions on Computers*, 60(2):157–164, Feb. 2011.
- (13) Sylvie Boldo and Claude Marché. Formal verification of numerical programs: from C annotated programs to mechanical proofs. *Mathematics in Computer Science*, 5:377–393, 2011.
- (14) Sylvie Boldo and Guillaume Melquiond. Emulation of FMA and correctly-rounded sums: Proved algorithms using rounding to odd. *IEEE Transactions on Computers*, 57(4):462–471, 2008.
- (15) Véronique Benzaken, G. Castagna, D. Colazzo, and Kim Nguyen. Optimizing XML querying using type-based document projection. *ACM Transactions on Database Systems (TODS)*, 2013.
- (16) Yannick Moy and Claude Marché. Modular inference of subprogram contracts for safety checking. *Journal of Symbolic Computation*, 45:1184–1211, 2010.

- (17) Sylvie Boldo. Kahan’s algorithm for a correct discriminant computation at last formally proven. *IEEE Transactions on Computers*, 58(2):220–225, Feb. 2009.

Other journals

- (18) F. Durán, S. Lucas, J. Meseguer, Claude Marché, and X. Urbain. Proving operational termination of membership equational programs. *Higher-Order and Symbolic Computation*, 21(1–2):59–88, 2008.
- (19) Guillaume Melquiond, W. G. Nowak, and P. Zimmermann. Numerical approximation of the Maser-Gramain constant to four decimal digits: $\delta = 1.819\dots$ *Mathematics of Computation*, 2012.
- (20) Louis Mandel and Marc Pouzet. ReactiveML : un langage fonctionnel pour la programmation réactive. *Technique et Science Informatiques*, 27(9-10):1097–1128, 2008.
- (21) Marc Pouzet and P. Raymond. Modular Static Scheduling of Synchronous Data-flow Networks: An efficient symbolic representation. *Journal of Design Automation for Embedded Systems*, 14(3):165–192, Sept. 2010.
- (22) Sylvie Boldo and Thi Minh Tuyen Nguyen. Proofs of numerical programs when the compiler optimizes. *Innovations in Systems and Software Engineering*, 7:151–160, 2011.

Invited conferences

- (23) Sylvie Boldo. Formal verification of numerical programs: from C annotated programs to Coq proofs. In *Proceedings of the Third International Workshop on Numerical Software Verification*, Edinburgh, Scotland, July 2010.
- (24) Jean-Christophe Filliâtre. Using SMT solvers for deductive verification of C and Java programs. In C. Barrett and L. de Moura, editors, *SMT 2008: 6th International Workshop on Satisfiability Modulo*, Princeton, USA, 2008.
- (25) Jean-Christophe Filliâtre. Invited tutorial: Why — an intermediate language for deductive program verification. In H. Saïdi and N. Shankar, editors, *Automated Formal Methods (AFM09)*, Grenoble, France, 2009.
- (26) Jean-Christophe Filliâtre. Combining interactive and automated theorem proving in Why3 (invited talk). In K. Heljanko and H. Herbelin, editors, *Automation in Proof Assistants 2012*, Tallinn, Estonia, Apr. 2012.

- (27) Jean-Christophe Filliâtre. Combining interactive and automated theorem proving using Why3 (invited tutorial). In Z. Rakamarić, editor, *Second International Workshop on Intermediate Verification Languages (BOOGIE 2012)*, Berkeley, California, USA, July 2012.
- (28) Jean-Christophe Filliâtre. Deductive Program Verification. In N. Foster, P. Gardner, A. Schmitt, G. Smith, P. Thieman, and T. Wrigstad, editors, *Programming Languages Mentoring Workshop (PLMW 2013)*, Rome, Italy, January 2013.
- (29) Jean-Christophe Filliâtre. One logic to use them all. In *24th International Conference on Automated Deduction (CADE-24)*, volume 7898 of *Lecture Notes in Artificial Intelligence*, pages 1–20, Lake Placid, USA, June 2013. Springer.

Conference articles

Major international conferences and workshops

- (30) U. A. Acar, Arthur Charguéraud, and M. Rainey. Scheduling parallel programs by work stealing with private dequeues. In *Proceedings of the 18th ACM SIGPLAN symposium on Principles and practice of parallel programming*, PPOPP '13, pages 219–228, Feb. 2013.
- (31) G. Baudart, F. Jacquemard, Louis Mandel, and M. Pouzet. A synchronous embedding of Antescofo, a domain-specific language for interactive mixed music. In *Thirteen International Conference on Embedded Software (EMSOFT'13)*, Montreal, Canada, Sept. 2013.
- (32) A. Benveniste, B. Caillaud, and Marc Pouzet. The Fundamentals of Hybrid Systems Modelers. In *49th IEEE International Conference on Decision and Control (CDC)*, Atlanta, Georgia, USA, Dec. 2010.
- (33) J. C. Blanchette and Andrei Paskevich. TFF1: The TPTP typed first-order form with rank-1 polymorphism. In *24th International Conference on Automated Deduction (CADE-24)*, volume 7898 of *Lecture Notes in Artificial Intelligence*, Lake Placid, USA, June 2013. Springer.
- (34) P. Caspi, J.-L. Colaço, Léonard Gérard, Marc Pouzet, and P. Raymond. Synchronous objects with scheduling policies: Introducing safe shared memory in lustre. In *ACM International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES)*, Dublin, June 2009.
- (35) G. Castagna and Kim Nguyen. Typed iterators for XML. In *Proceedings of the 13th ACM SIGPLAN international conference on Functional programming*, pages 15–26, 2008.
- (36) A. Cimatti, A. Franzen, A. Griggio, Krishnamani Kalyanasundaram, and M. Roveri. Tighter integration of BDDs and SMT for predicate abstraction. In *Design, Automation & Test in Europe*, Dresden, Germany, Mar. 2010. IEEE.
- (37) A. Cohen, L. Mandel, F. Plateau, and M. Pouzet. Abstraction of Clocks in Synchronous Data-flow Systems. In *The Sixth ASIAN Symposium on Programming Languages and Systems (APLAS)*, volume 5356 of *Lecture Notes in computer Science*, pages 237–254, Bangalore, India, Dec. 2008.
- (38) G. Delaval, A. Girault, and Marc Pouzet. A Type System for the Automatic Distribution of Higher-order Synchronous Dataflow Programs. In *ACM International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES)*, Tucson, Arizona, June 2008.
- (39) W. Edmonson and Guillaume Melquiond. IEEE interval standard working group - P1788: current status. In J. D. Bruguera, M. Cornea, D. DasSarma, and J. Harrison, editors, *Proceedings of the 19th IEEE Symposium on Computer Arithmetic*, pages 231–234, Portland, OR, USA, 2009.
- (40) D. Ishii, Guillaume Melquiond, and S. Nakajima. Inductive verification of hybrid automata with strongest postcondition calculus. In E. B. Johnsen and L. Petre, editors, *Proceedings of the 10th Conference on Integrated Formal Methods*, volume 7940 of *Lecture Notes in Computer Science*, pages 139–153, Turku, Finland, 2013.
- (41) S. Maneth and Kim Nguyen. Xpath whole query optimization. In *36th International Conference on Very Large Data Bases (VLDB'2010)*, volume 3, pages 882–893, 2010.

- (42) Ali Ayad and Claude Marché. Multi-prover verification of floating-point programs. In J. Giesl and R. Hähnle, editors, *Fifth International Joint Conference on Automated Reasoning*, Lecture Notes in Artificial Intelligence, Edinburgh, Scotland, July 2010. Springer.
- (43) Arthur Charguéraud. Pretty-big-step semantics. In M. Felleisen and P. Gardner, editors, *Proceedings of the 22nd European Symposium on Programming*, volume 7792 of *Lecture Notes in Computer Science*, pages 41–60. Springer, Mar. 2013.
- (44) Claire Dross, Jean-Christophe Filliâtre, and Y. Moy. Correct Code Containing Containers. In *5th International Conference on Tests and Proofs (TAP'11)*, volume 6706 of *Lecture Notes in Computer Science*, pages 102–118, Zurich, June 2011. Springer.
- (45) Dariusz Biernacki, J.-L. Colaço, G. Hamon, and Marc Pouzet. Clock-directed Modular Code Generation of Synchronous Data-flow Languages. In *ACM International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES)*, Tucson, Arizona, June 2008.
- (46) Denis Cousineau, D. Doligez, L. Lamport, S. Merz, D. Ricketts, and H. Vanzetto. TLA+ proofs. In D. Giannakopoulou and D. Méry, editors, *18th International Symposium on Formal Methods*, volume 7436 of *Lecture Notes in Computer Science*, pages 147–154. Springer, 2012.
- (47) Denis Cousineau and O. Hermant. A semantic proof that reducibility candidates entail cut elimination. In A. Tiwari, editor, *23rd International Conference on Rewriting Techniques and Applications*, volume 15 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 133–148, Nagoya, Japan, 2012. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- (48) Évelyne Contejean, P. Courtieu, J. Forest, O. Pons, and X. Urbain. Automated Certified Proofs with CIME3. In M. Schmidt-Schauß, editor, *22nd International Conference on Rewriting Techniques and Applications (RTA 11)*, volume 10 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21–30, Novi Sad, Serbia, 2011. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- (49) Évelyne Contejean, P. Courtieu, J. Forest, Andrei Paskevich, O. Pons, and X. Urbain. A3PAT, an Approach for Certified Automated Termination Proofs. In *Partial Evaluation and Program Manipulation*, Madrid, Spain, Jan. 2010. ACM Press.
- (50) François Bobot and Andrei Paskevich. Expressing Polymorphic Types in a Many-Sorted Language. In C. Tinelli and V. Sofronie-Stokkermans, editors, *Frontiers of Combining Systems, 8th International Symposium, Proceedings*, volume 6989 of *Lecture Notes in Computer Science*, Saarbrücken, Germany, Oct. 2011.
- (51) François Bobot and Jean-Christophe Filliâtre. Separation predicates: a taste of separation logic in first-order logic. In *14th International Conference on Formal Engineering Methods (ICFEM)*, volume 7635 of *Lecture Notes in Computer Science*, Kyoto, Japan, Nov. 2012. Springer.
- (52) François Bobot, Jean-Christophe Filliâtre, Claude Marché, Guillaume Melquiond, and Andrei Paskevich. Preserving user proofs across specification changes. In E. Cohen and A. Rybalchenko, editors, *Verified Software: Theories, Tools, Experiments (5th International Conference VSTTE)*, Lecture Notes in Computer Science, Atherton, USA, May 2013. Springer.
- (53) François Bobot, Sylvain Conchon, Evelyne Contejean, Mohamed Iguernelala, A. Mahboubi, Alain Mebsout, and Guillaume Melquiond. A Simplex-based extension of Fourier-Motzkin for solving linear integer arithmetic. In B. Gramlich, D. Miller, and U. Sattler, editors, *IJCAR 2012: Proceedings of the 6th International Joint Conference on Automated Reasoning*, volume 7364 of *Lecture Notes in Computer Science*, pages 67–81, Manchester, UK, June 2012. Springer.
- (54) Jean-Christophe Filliâtre. Verifying two lines of C with Why3: an exercise in program verification. In R. Joshi, P. Müller, and A. Podelski, editors, *Verified Software: Theories, Tools, Experiments (4th International Conference VSTTE)*, volume 7152 of *Lecture Notes in Computer Science*, pages 83–97, Philadelphia, USA, Jan. 2012. Springer.
- (55) Jean-Christophe Filliâtre and Andrei Paskevich. Why3 — where programs meet provers. In M. Felleisen and P. Gardner, editors, *Proceedings of the 22nd European Symposium on Programming*, volume 7792 of *Lecture Notes in Computer Science*, pages 125–128. Springer, Mar. 2013.
- (56) Louis Mandel and L. Maranget. Programming in JoCaml (tool demonstration). In *17th European Symposium on Programming (ESOP'08)*, pages 108–111, Budapest, Hungary, Apr. 2008.

- (57) Louis Mandel, C. Pasteur, and M. Pouzet. Time refinement in a functional synchronous language. In *Proceedings of 15th ACM SIGPLAN International Symposium on Principles and Practice of Declarative Programming (PPDP'13)*, Madrid, Spain, Sept. 2013.
- (58) Louis Mandel, Florence Plateau, and Marc Pouzet. Static scheduling of latency insensitive designs with *Lucy-n*. In *FMCAD 2011 - Formal Methods in Computer Aided Design*, Austin, TX, United States, 2011.
- (59) Marc Pouzet and P. Raymond. Modular static scheduling of synchronous data-flow networks: An efficient symbolic representation. In *ACM International Conference on Embedded Software (EMSOFT'09)*, Grenoble, France, Oct. 2009.
- (60) Matthieu Sozeau and N. Oury. First-class type classes. In S. Tahar, O. Ait-Mohamed, and C. Muñoz, editors, *21th International Conference on Theorem Proving in Higher Order Logics*, Lecture Notes in Computer Science. Springer, Aug. 2008.
- (61) Paolo Herms, Claude Marché, and B. Monate. A certified multi-prover verification condition generator. In R. Joshi, P. Müller, and A. Podelski, editors, *Verified Software: Theories, Tools, Experiments (4th International Conference VSTTE)*, volume 7152 of *Lecture Notes in Computer Science*, pages 2–17, Philadelphia, USA, Jan. 2012. Springer.
- (62) Stéphane Lescuyer and Sylvain Conchon. Improving Coq propositional reasoning using a lazy CNF conversion scheme. In S. Ghilardi and R. Sebastiani, editors, *Frontiers of Combining Systems, 7th International Symposium, Proceedings*, volume 5749 of *Lecture Notes in Computer Science*, pages 287–303, Trento, Italy, Sept. 2009. Springer.
- (63) Sylvain Conchon, Évelyne Contejean, and Mohamed Iguernelala. Ground Associative and Commutative Completion Modulo Shostak Theories. In A. Voronkov, editor, *LPAR, 17th International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, EasyChair Proceedings, Yogyakarta, Indonesia, Oct. 2010.
- (64) Sylvain Conchon, Évelyne Contejean, and Mohamed Iguernelala. Canonized Rewriting and Ground AC Completion Modulo Shostak Theories. In P. A. Abdulla and K. R. M. Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science, Saarbrücken, Germany, Apr. 2011. Springer.
- (65) Sylvain Conchon and Jean-Christophe Filliâtre. Semi-Persistent Data Structures. In *17th European Symposium on Programming (ESOP'08)*, Budapest, Hungary, Apr. 2008.
- (66) Sylvie Boldo. Floats & ropes: a case study for formal numerical program verification. In *36th International Colloquium on Automata, Languages and Programming*, volume 5556 of *Lecture Notes in Computer Science - ARCoSS*, pages 91–102, Rhodes, Greece, July 2009. Springer.
- (67) Sylvie Boldo. How to compute the area of a triangle: a formal revisit. In *Proceedings of the 21th IEEE Symposium on Computer Arithmetic*, Austin, Texas, USA, 2013.
- (68) Sylvie Boldo, F. Clément, Jean-Christophe Filliâtre, M. Mayero, Guillaume Melquiond, and P. Weis. Formal Proof of a Wave Equation Resolution Scheme: the Method Error. In M. Kaufmann and L. C. Paulson, editors, *Proceedings of the first Interactive Theorem Proving Conference*, volume 6172 of *LNCS*, pages 147–162, Edinburgh, Scotland, July 2010. Springer.
- (69) Sylvie Boldo, J.-H. Jourdan, X. Leroy, and Guillaume Melquiond. A formally-verified C compiler supporting floating-point arithmetic. In *Proceedings of the 21th IEEE Symposium on Computer Arithmetic*, Austin, Texas, USA, 2013.
- (70) Sylvie Boldo and Guillaume Melquiond. Flocq: A unified library for proving floating-point algorithms in Coq. In E. Antelo, D. Hough, and P. lenne, editors, *Proceedings of the 20th IEEE Symposium on Computer Arithmetic*, pages 243–252, Tübingen, Germany, 2011.
- (71) Sylvie Boldo and Thi Minh Tuyen Nguyen. Hardware-independent proofs of numerical programs. In C. Muñoz, editor, *Proceedings of the Second NASA Formal Methods Symposium*, NASA Conference Publication, pages 14–23, Washington D.C., USA, Apr. 2010.
- (72) Véronique Benzaken, G. Castagna, Kim Nguyen, and J. Siméon. Static and dynamic semantics of NoSQL languages. In R. Cousot, editor, *Proceedings of the 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Roma, Italy, Jan. 2013. ACM Press.

- (73) Yannick Moy. Sufficient preconditions for modular assertion checking. In F. Logozzo, D. Peled, and L. Zuck, editors, *9th International Conference on Verification, Model Checking, and Abstract Interpretation*, volume 4905 of *Lecture Notes in Computer Science*, pages 188–202, San Francisco, California, USA, Jan. 2008. Springer.

Major national conferences and workshops

- (74) Catherine Lelay and Guillaume Melquiond. Différentiabilité et intégrabilité en Coq. application à la formule de d’Alembert. In *Vingt-troisièmes Journées Francophones des Langages Applicatifs*, Carnac, France, Feb. 2012.
- (75) Claude Marché and Asma Tafat. Calcul de plus faible précondition, revisité en Why3. In *Vingt-quatrièmes Journées Francophones des Langages Applicatifs*, Aussois, France, Feb. 2013.
- (76) Filliâtre, Jean-Christophe and Kalyanasundaram, Krishnamani. Une bibliothèque de calcul distribué pour Objective Caml. In Sylvain Conchon, editor, *Vingt-deuxièmes Journées Francophones des Langages Applicatifs*, La Bresse, France, Jan. 2011. INRIA.
- (77) Jean-Christophe Filliâtre. Gagner en passant à la corde. In *Dix-neuvièmes Journées Francophones des Langages Applicatifs*, Étretat, France, Jan. 2008. INRIA.
- (78) Jean-Christophe Filliâtre and R. E. Sibaïe. Combine : une bibliothèque OCaml pour la combinatoire. In *Vingt-quatrièmes Journées Francophones des Langages Applicatifs*, Aussois, France, Feb. 2013.
- (79) Louis Mandel. Cours de ReactiveML. In *Vingt-et-unièmes Journées Francophones des Langages Applicatifs*, Vieux-Port La Ciotat, France, Jan. 2010. INRIA.
- (80) Louis Mandel and C. Pasteur. Réactivité des systèmes coopératifs : le cas de ReactiveML. In *Vingt-quatrièmes Journées Francophones des Langages Applicatifs*, Aussois, France, Feb. 2013.
- (81) Louis Mandel and Florence Plateau. Abstraction d’horloges dans les systèmes synchrones flot de données. In *Vingtièmes Journées Francophones des Langages Applicatifs*, Saint-Quentin sur Isère, Jan. 2009. INRIA.
- (82) Louis Mandel and Florence Plateau. Typage des horloges périodiques en Lucy-n. In Sylvain Conchon, editor, *Vingt-deuxièmes Journées Francophones des Langages Applicatifs*, La Bresse, France, Jan. 2011. INRIA.
- (83) Louis Mandel, Florence Plateau, and Marc Pouzet. Lucy-n : une extension n-synchrone de Lustre. In *Vingt-et-unièmes Journées Francophones des Langages Applicatifs*, Vieux-Port La Ciotat, France, Jan. 2010. INRIA.
- (84) Romain Bardou, Jean-Christophe Filliâtre, Johannes Kanig, and Stéphane Lescuyer. Faire bonne figure avec Mlpost. In *Vingtièmes Journées Francophones des Langages Applicatifs*, Saint-Quentin sur Isère, Jan. 2009. INRIA.
- (85) Romain Bardou and Marché Claude. Perle de preuve: les tableaux creux. In Sylvain Conchon, editor, *Vingt-deuxièmes Journées Francophones des Langages Applicatifs*, La Bresse, France, Jan. 2011. INRIA.
- (86) Sylvain Conchon, Alain Mebsout, and F. Zaïdi. Vérification de systèmes paramétrés avec Cubicle. In *Vingt-quatrièmes Journées Francophones des Langages Applicatifs*, Aussois, France, Feb. 2013.
- (87) Sylvain Conchon, Jean-Christophe Filliâtre, F. Le Fessant, J. Robert, and G. Von Tokarski. Observation temps-réel de programmes Caml. In *Vingt-et-unièmes Journées Francophones des Langages Applicatifs*, Vieux-Port La Ciotat, France, Jan. 2010. INRIA.
- (88) Sylvain Conchon, Johannes Kanig, and Stéphane Lescuyer. SAT-MICRO : petit mais costaud ! In *Dix-neuvièmes Journées Francophones des Langages Applicatifs*, Étretat, France, Jan. 2008. INRIA.

Other conferences and workshops

- (89) M. Barbosa, Jean-Christophe Filliâtre, J. S. Pinto, and B. Vieira. A Deductive Verification Platform for Cryptographic Software. In *4th International Workshop on Foundations and Techniques for Open Source Software Certification (OpenCert 2010)*, volume 33, Pisa, Italy, Sept. 2010. Electronic Communications of the EASST.
- (90) G. Baudart, Louis Mandel, and M. Pouzet. Programming mixed music in ReactiveML. In *ACM SIGPLAN Workshop on Functional Art, Music, Modeling and Design (FARM'13)*, Boston, USA, Sept. 2013.
- (91) T. Bormer, M. Brockschmidt, D. Distefano, G. Ernst, Jean-Christophe Filliâtre, R. Grigore, M. Huisman, V. Klebanov, Claude Marché, R. Monahan, W. Mostowski, N. Polikarpova, C. Scheben, G. Schellhorn, B. Tofan, J. Tschannen, and M. Ulbrich. The COST IC0701 verification competition 2011. In B. Beckert, F. Damiani, and D. Gurov, editors, *Formal Verification of Object-Oriented Software, Revised Selected Papers Presented at the International Conference, FoVeOOS 2011*, volume 7421 of *Lecture Notes in Computer Science*. Springer, 2012.
- (92) E. Contejean. Coccinelle, a Coq library for rewriting. In *Types*, Torino, Italy, Mar. 2008.
- (93) C. Hurlin, François Bobot, and A. J. Summers. Size does matter : Two certified abstractions to disprove entailment in intuitionistic and classical separation logic. In *International Workshop on Aliasing, Confinement and Ownership in object-oriented programming (IWACO'09)*, July 2009. Coq proofs: <http://www-sop.inria.fr/everest/Clement.Hurlin/disprove.tgz>.
- (94) J. Kanig, E. Schonberg, and Claire Dross. Hi-Lite: the convergence of compiler technology and program verification. In B. Brosgol, J. Boleng, and S. T. Taft, editors, *Proceedings of the 2012 ACM Conference on High Integrity Language Technology, HILT '12*, pages 27–34, Boston, USA, 2012.
- (95) D. Mentré, Claude Marché, Jean-Christophe Filliâtre, and M. Asuka. Discharging proof obligations from Atelier B using multiple automated provers. In S. Reeves and E. Riccobene, editors, *ABZ'2012 - 3rd International Conference on Abstract State Machines, Alloy, B and Z*, volume 7316 of *Lecture Notes in Computer Science*, pages 238–251, Pisa, Italy, June 2012. Springer. <http://hal.inria.fr/hal-00681781/en/>.
- (96) M. Pereira, Jean-Christophe Filliâtre, and S. M. de Sousa. ARMY: a deductive verification platform for ARM programs using Why3. In *INForum 2012*, Sept. 2012.
- (97) E. Tushkanova, A. Giorgetti, Claude Marché, and O. Kouchnarenko. Specifying generic Java programs: two case studies. In C. Brabrand and P.-E. Moreau, editors, *Tenth Workshop on Language Descriptions, Tools and Applications*. ACM Press, 2010.
- (98) Asma Tafat, S. Boulmé, and Claude Marché. A refinement methodology for object-oriented programs. In B. Beckert and C. Marché, editors, *Formal Verification of Object-Oriented Software, Papers Presented at the International Conference, Karlsruhe Reports in Informatics*, pages 143–159, Paris, France, June 2010.
- (99) Asma Tafat, S. Boulmé, and Claude Marché. A refinement methodology for object-oriented programs. In B. Beckert and C. Marché, editors, *Formal Verification of Object-Oriented Software, Revised Selected Papers Presented at the International Conference, FoVeOOS 2010*, volume 6528 of *Lecture Notes in Computer Science*, pages 153–167. Springer, Jan. 2011.
- (100) Claire Dross, Sylvain Conchon, J. Kanig, and Andrei Paskevich. Reasoning with triggers. In P. Fontaine and A. Goel, editors, *SMT workshop*, Manchester, UK, 2012. LORIA.
- (101) David Baelde, R. Beauxis, and S. Mimram. Liquidsoap: A high-level programming language for multimedia streaming. In I. Cerná, T. Gyimóthy, J. Hromkovic, K. G. Jeffery, R. Královic, M. Vukolic, and S. Wolf, editors, *37th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'11)*, volume 6543 of *Lecture Notes in Computer Science*, Nový Smokovec, Slovakia, Jan. 2011. Springer.
- (102) Évelyne Contejean, P. Courtieu, J. Forest, Andrei Paskevich, O. Pons, and X. Urbain. A3PAT, an Approach for Certified Automated Termination Proofs. In E. Cariou, L. Duchien, and Y. Ledru, editors, *Journées nationales du GDR-GPL*, Pau, France, Mar. 2010. GDR GPL.
- (103) François Bobot, Jean-Christophe Filliâtre, Claude Marché, and Andrei Paskevich. Why3: Shepherd your herd of provers. In *Boogie 2011: First International Workshop on Intermediate Verification Languages*, Wrocław, Poland, Aug. 2011.

- (104) François Bobot, Sylvain Conchon, Evelyne Contejean, and Stéphane Lescuyer. Implementing Polymorphism in SMT solvers. In C. Barrett and L. de Moura, editors, *SMT 2008: 6th International Workshop on Satisfiability Modulo*, 2008.
- (105) Jean-Christophe Filliâtre, Andrei Paskevich, and A. Stump. The 2nd verified software competition: Experience report. In V. Klebanov and S. Grebing, editors, *COMPARE2012: 1st International Workshop on Comparative Empirical Evaluation of Reasoning Systems*, Manchester, UK, June 2012. Easy-Chair.
- (106) Jean-Christophe Filliâtre and K. Kalyanasundaram. Functory: A distributed computing library for Objective Caml. In *Trends in Functional Programming*, Madrid, Spain, May 2011.
- (107) Johannes Kanig and Jean-Christophe Filliâtre. Who: A verifier for effectful higher-order programs. In *ACM SIGPLAN Workshop on ML*, Edinburgh, Scotland, UK, Aug. 2009.
- (108) Louis Mandel and F. Plateau. Scheduling and buffer sizing of n-synchronous systems: Typing of ultimately periodic clocks in Lucy-n. In *Eleventh International Conference on Mathematics of Program Construction (MPC'12)*, Madrid, Spain, June 2012.
- (109) Louis Mandel and Florence Plateau. Interactive programming of reactive systems. In *Proceedings of Model-driven High-level Programming of Embedded Systems (SLA++P'08)*, Electronic Notes in Computer Science, pages 44–59, Budapest, Hungary, Apr. 2008. Elsevier Science Publishers. to appear.
- (110) Louis Mandel, Florence Plateau, and Marc Pouzet. Clock typing of n-synchronous programs. In *Designing Correct Circuits (DCC 2010)*, Paphos, Cyprus, Mar. 2010.
- (111) Louis Mandel, Florence Plateau, and Marc Pouzet. Lucy-n : une extension n-synchrone de Lustre. In E. Cariou, L. Duchien, and Y. Ledru, editors, *Journées nationales du GDR-GPL*, Pau, France, Mar. 2010. GDR GPL.
- (112) Louis Mandel, Florence Plateau, and Marc Pouzet. Lucy-n: a n-synchronous extension of Lustre. In *Tenth International Conference on Mathematics of Program Construction (MPC 2010)*, Québec, Canada, June 2010.
- (113) Paolo Herms. Certification of a chain for deductive program verification. In Y. Bertot, editor, *2nd Coq Workshop, satellite of ITP'10*, 2010.
- (114) Romain Bardou. Ownership, pointer arithmetic and memory separation. In *Formal Techniques for Java-like Programs (FTJP'08)*, Paphos, Cyprus, July 2008.
- (115) Sylvain Conchon, Evelyne Contejean, Johannes Kanig, and Stéphane Lescuyer. CC(X): Semantical Combination of Congruence Closure with Solvable Theories. In *Proceedings of the 5th International Workshop on Satisfiability Modulo Theories (SMT 2007)*, volume 192 of *Electronic Notes in Computer Science*, pages 51–69. Elsevier Science Publishers, 2008.
- (116) Sylvain Conchon, Guillaume Melquiond, Cody Roux, and Mohamed Iguernelala. Built-in treatment of an axiomatic floating-point theory for SMT solvers. In P. Fontaine and A. Goel, editors, *SMT workshop*, pages 12–21, Manchester, UK, 2012. LORIA.
- (117) Sylvain Conchon, Jean-Christophe Filliâtre, and J. Signoles. Designing a generic graph library using ML functors. In M. Morazán, editor, *Trends in Functional Programming*, volume 8. Intellect, 2008.
- (118) Sylvie Boldo, M. Daumas, and P. Giorgi. Formal proof for delayed finite field arithmetic using floating point operators. In *Proceedings of the 8th Conference on Real Numbers and Computers*, Santiago de Compostela, Spain, July 2008.
- (119) Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Improving real analysis in Coq: a user-friendly approach to integrals and derivatives. In C. Hawblitzel and D. Miller, editors, *Proceedings of the Second International Conference on Certified Programs and Proofs*, volume 7679 of *Lecture Notes in Computer Science*, pages 289–304, Kyoto, Japan, Dec. 2012.
- (120) Sylvie Boldo, Jean-Christophe Filliâtre, and Guillaume Melquiond. Combining Coq and Gappa for certifying floating-point programs. In *16th Symposium on the Integration of Symbolic Computation and Mechanised Reasoning*, volume 5625 of *Lecture Notes in Artificial Intelligence*, pages 59–74, Grand Bend, Canada, July 2009. Springer.
- (121) Thi Minh Tuyen Nguyen and Claude Marché. Hardware-dependent proofs of numerical programs. In J.-P. Jouannaud and Z. Shao, editors, *Certified Programs and Proofs*, Lecture Notes in Computer Science. Springer, Dec. 2011.

Books and book chapters

- (122) J.-M. Muller, N. Brisebarre, F. de Dinechin, C.-P. Jeannerod, V. Lefèvre, Guillaume Melquiond, N. Revol, D. Stehlé, and S. Torres. *Handbook of Floating-Point Arithmetic*. Birkhäuser, 2010.
- (123) Véronique Benzaken, G. Castagna, H. Hosoya, B. C. Pierce, and S. Vansummen. XML typechecking. In *Encyclopedia of Database Systems*, pages 3646–3650. Springer US, 2009.
- (124) Christine Paulin-Mohring. *From Semantics and Computer Science: Essays in Honor of Gilles Kahn*, chapter A constructive denotational semantics for Kahn networks in Coq. Cambridge University Press, 2008.
- (125) Christine Paulin-Mohring. Tools for practical software verification (international summer school, LASER 2011, revised tutorial lectures). volume 7682 of *Lecture Notes in Computer Science*, chapter Introduction to the Coq proof-assistant for practical software verification. Springer, 2012.
- (126) Sylvie Boldo and Guillaume Melquiond. *Informatique Mathématique, une photographie en 2013*, chapter Arithmétique des ordinateurs et preuves formelles, pages 189–220. Presses Universitaires de Perpignan, Perpignan, France, 2013.
- (127) Sylvie Boldo and T. Viéville. Représentation numérique de l’information. In G. Dowek, editor, *Introduction à la science informatique*, Repères pour agir, pages 23–72. CRDP Académie de Paris, July 2011.
- (128) Sylvie Boldo and T. Viéville. Structuration et contrôle de l’information. In G. Dowek, editor, *Introduction à la science informatique*, Repères pour agir, pages 281–308. CRDP Académie de Paris, July 2011.
- (129) B. Wack, Sylvain Conchon, J. Courant, M. de Falco, G. Dowek, Jean-Christophe Filliâtre, and S. Gonnord. *Informatique pour tous en classes préparatoires aux grandes écoles : Manuel d’algorithmique et programmation structurée avec Python*. Eyrolles, Aug. 2013.

Edited books

- (130) P. Audebaud and Christine Paulin-Mohring, editors. *Science of Computer Programming. Special issue on the Mathematics of Program Construction (MPC 2008)*, volume 76. Elsevier Science Publishers, 2011.
- (131) P. Audebaud and Christine Paulin-Mohring, editors. *Mathematics of Program Construction, MPC 2008, Marseille, July 15-18, 2008*, volume 5133 of *Lecture Notes in Computer Science*. Springer, 2008.
- (132) B. Beckert and Claude Marché, editors. *Formal Verification of Object-Oriented Software, Revised Selected Papers Presented at the International Conference, FoVeOOS 2010*, volume 6528 of *Lecture Notes in Computer Science*. Springer, Jan. 2011.

Dissemination

- (133) Jean-Christophe Filliâtre. Deductive program verification with Why3. <https://www.lri.fr/~marche/DigiCosmeSchool/filliatre.html>, 2013.



- (134) Claude Marché. The krakatoa tool for deductive verification of java programs. Winter School on Object-Oriented Verification, Viinistu, Estonia, Jan. 2009. <http://krakatoa.lri.fr/ws/>.
- (135) Jean-Christophe Filliâtre. *Course notes EJCP 2012*, chapter Vérification déductive de programmes avec Why3. June 2012.
- (136) Sylvie Boldo. Demandez le programme! Interstices, Feb. 2009.
- (137) Sylvie Boldo. C'est la faute à l'ordinateur! Interstices – Idée reçue, Feb. 2010.
- (138) Sylvie Boldo. L'informatique. Universcience web television, Apr. 2010.
- (139) Sylvie Boldo. Un algorithme de découpe de gâteau. Interstices, July 2010.
- (140) Sylvie Boldo and Guillaume Melquiond. Arithmétique des ordinateurs et preuves formelles. In V. Berthé, C. Frougny, N. Portier, M.-F. Roy, and A. Siegel, editors, *École des Jeunes Chercheurs en Informatique Mathématique*, pages 1–30. Rennes, France, Mar. 2012.

Other publications

- (141) P. Attar, F. Boussinot, Louis Mandel, and J.-F. Susini. Proposal for a Dynamic Synchronous Language. PARTOUT, May 2011.
- (142) P. Baudin, Jean-Christophe Filliâtre, Claude Marché, B. Monate, Yannick Moy, and V. Prevosto. *ACSL: ANSI/ISO C Specification Language*, 2008. <http://www.frama-c.cea.fr/acsl.html>.
- (143) P. Baudin, Jean-Christophe Filliâtre, Claude Marché, B. Monate, Yannick Moy, and V. Prevosto. *ACSL: ANSI/ISO C Specification Language, version 1.4*, 2009. <http://frama-c.cea.fr/acsl.html>.
- (144) J. C. Blanchette and A. Paskevich. TFF1: The TPTP typed first-order form with rank-1 polymorphism. Technical report, Tech. Univ. Munich, 2012. <http://www21.in.tum.de/~blanchet/tff1spec.pdf>.
- (145) E. Martin-Dorel, Guillaume Melquiond, and J.-M. Muller. Some issues related to double roundings. Technical report, Nov. 2011.
- (146) Y. Moy and Claude Marché. *The Jessie plugin for Deduction Verification in Frama-C — Tutorial and Reference Manual*. INRIA & LRI, 2011. <http://krakatoa.lri.fr/>.
- (147) A. Rousseau, A. Darnaud, B. Goglin, C. Acharian, C. Leininger, C. Godin, C. Holik, C. Kirchner, D. Rives, E. Darquie, E. Kerrien, F. Neyret, F. Maseglia, F. Dufour, G. Berry, G. Dowek, H. Robak, H. Xypas, I. Illina, I. Gnaedig, J. Jongwane, J. Ehrel, L. Viennot, L. Guion, L. Calderan, L. Kovacic, M. Collin, M.-A. Enard, M.-H. Comte, M. Quinson, M. Olivi, M. Giraud, M. Dorémus, M. Ogouchi, M. Droin, N. Lacaux, N. Rougier, N. Roussel, P. Guitton, P. Peterlongo, R.-M. Cornus, S. Vandermeersch, S. Maheo, S. Lefebvre, Sylvie Boldo, T. Viéville, V. Poirel, A. Chabreuil, A. Fischer, C. Farge, C. Vadel, I. Astic, J.-P. Dumont, L. Féjoz, P. Rambert, P. Paradinas, S. De Quatrebarbes, and S. Laurent. Médiation scientifique : une facette de nos métiers de la recherche. Interne, Inria, Mar. 2013.
- (148) V. Saraswat, D. Cunningham, L. Hadarean, Louis Mandel, A. Shinnar, and O. Tardieu. Constrained types - future directions. In *18th International Conference on Principles and Practice of Constraint Programming*, Québec City, Canada, Oct. 2012. Position Paper.
- (149) E. Tushkanova, A. Giorgetti, Claude Marché, and O. Kouchnarenko. Modular specification of java programs. Technical Report RR-7097, INRIA, 2009.
- (150) Ali Ayad. On formal methods for certifying floating-point C programs. Research Report RR-6927, INRIA, 2009.
- (151) Ali Ayad and Claude Marché. Behavioral properties of floating-point programs. Hisseo publications, 2009. <http://hisseo.saclay.inria.fr/ayad09.pdf>.

- (152) Andrei Paskevich. Algebraic types and pattern matching in the logical language of the why verification platform. Technical Report RR-7128, INRIA, 2009.
- (153) Andrei Paskevich. Algebraic types and pattern matching in the logical language of the Why verification platform (version 2). Technical Report 7128, INRIA, 2010.
- (154) Arthur Milchior. Algorithme de matching, modulo. Rapport de stage L3, 2009.
- (155) Asma Tafat. Invariants et raffinements en présence de partage. Master's thesis, Université Paris 6, 2009.
- (156) Asma Tafat, S. Boulmé, and Claude Marché. A refinement approach for correct-by-construction object-oriented programs. Technical Report 7310, INRIA, 2010.
- (157) Asma Tafat and Claude Marché. Binary Heaps Formally Verified in Why3. Research Report RR-7780, INRIA, Oct. 2011.
- (158) Catherine Lelay. étude de la différentiabilité et de l'intégrabilité en Coq : Application à la formule de d'Alembert pour l'équation des ondes. Master's thesis, Université Paris 7, 2011.
- (159) Claire Dross, Sylvain Conchon, J. Kanig, and Andrei Paskevich. Reasoning with triggers. Research Report RR-7986, INRIA, June 2012.
- (160) Claude Marché and Asma Tafat. Weakest precondition calculus, revisited using Why3. Research Report RR-8185, INRIA, Dec. 2012.
- (161) Évelyne Contejean, P. Courtieu, J. Forest, O. Pons, and X. Urbain. Automated Certified Proofs with CiME3. Technical Report 2044, Cédric laboratory, CNAM Paris, France, 2011.
- (162) François Bobot and Andrei Paskevich. Expressing Polymorphic Types in a Many-Sorted Language. Research report, 2011.
- (163) François Bobot, Jean-Christophe Filliâtre, Claude Marché, and Andrei Paskevich. *The Why3 platform, version 0.71*. LRI, CNRS & Univ. Paris-Sud & INRIA Saclay, version 0.71 edition, Oct. 2011.
- (164) François Bobot, Jean-Christophe Filliâtre, Claude Marché, Guillaume Melquiond, and Andrei Paskevich. *The Why3 platform, version 0.72*. LRI, CNRS & Univ. Paris-Sud & INRIA Saclay, version 0.72 edition, May 2012.
- (165) François Bobot, Jean-Christophe Filliâtre, Claude Marché, Guillaume Melquiond, and Andrei Paskevich. *The Why3 platform, version 0.73*. LRI, CNRS & Univ. Paris-Sud & INRIA Saclay, version 0.73 edition, July 2012.
- (166) François Bobot, Jean-Christophe Filliâtre, Claude Marché, Guillaume Melquiond, and Andrei Paskevich. *The Why3 platform, version 0.80*. LRI, CNRS & Univ. Paris-Sud & INRIA Saclay, version 0.80 edition, Oct. 2012. <https://gforge.inria.fr/docman/view.php/2990/8186/manual-0.80.pdf>.
- (167) François Bobot, Jean-Christophe Filliâtre, Claude Marché, Guillaume Melquiond, and Andrei Paskevich. *The Why3 platform, version 0.81*. LRI, CNRS & Univ. Paris-Sud & INRIA Saclay, version 0.81 edition, Mar. 2013.
- (168) Kalyanasundaram, Krishnamani and Claude Marché. Automated Generation of Loop Invariants using Predicate Abstraction. Research Report RR-7714, INRIA, Aug. 2011.
- (169) Lelay, Catherine and Guillaume Melquiond. Différentiabilité et intégrabilité en Coq. application à la formule de d'Alembert. 2011.
- (170) Matthieu Sozeau. *The Coq Proof Assistant Reference Manual – Version V8.2*, chapter User defined equalities and relations. <http://coq.inria.fr/>, 2008.
- (171) Matthieu Sozeau. *The Coq Proof Assistant Reference Manual – Version V8.2*. <http://coq.inria.fr/>, 2008.
- (172) Mohamed Iguernelala. Extension modulo Associativité-Commutativité de l'algorithme de clôture par congruence CC(X). Master's thesis, Université Paris-Sud, 2009.
- (173) Nuno Gaspar. Mechanized semantics into concurrent program verification. <http://www.lri.fr/~gaspar/rgcoq.html>, Sept. 2011.

- (174) Paolo Herms, Claude Marché, and B. Monate. A Certified Multi-prover Verification Condition Generator. Research Report RR-7793, INRIA, Nov. 2011.
- (175) Romain Bardou and Claude Marché. Regions and permissions for verifying data invariants. Research Report 7412, INRIA, 2010.
- (176) Sylvain Conchon and Evelyne Contejean. The Alt-Ergo automatic theorem prover, 2008. <http://alt-ergo.lri.fr/>.
- (177) Sylvain Conchon, Évelyne Contejean, and Mohamed Iguernelala. Canonized Rewriting and Ground AC Completion Modulo Shostak Theories. Research Report 1538, LRI, Université Paris Sud, Dec. 2010.
- (178) Sylvie Boldo, F. Clément, Jean-Christophe Filliâtre, M. Mayero, Guillaume Melquiond, and P. Weis. Wave Equation Numerical Resolution: Mathematics and Program. Research Report RR-7826, INRIA, Dec. 2011.
- (179) Sylvie Boldo and Thi Minh Tuyen Nguyen. Hardware-independent proofs of numerical programs. Hisseo publications, 2009. <http://hisseo.saclay.inria.fr/tuyen09.pdf>.
- (180) Thi Minh Tuyen Nguyen and Claude Marché. Proving floating-point numerical programs by analysis of their assembly code. Research Report RR-7655, INRIA, June 2011. Digiteo Hisseo.
- (181) Yannick Moy and Claude Marché. *Jessie Plugin Tutorial*, Beryllium version. INRIA, 2009. <http://www.frama-c.cea.fr/jessie.html>.
- (182) W. Urribarrí and Christine Paulin-Mohring. Modules and refinement in Why. Oct. 2009.

Theses and habilitations

- (183) Cédric Auger. *Compilation Certifiée de SCADE/LUSTRE*. Thèse de doctorat, Université Paris-Sud, 2013. <http://tel.archives-ouvertes.fr/tel-00818169/>.
- (184) Florence Plateau. *Modèle n-synchrone pour la programmation de réseaux de Kahn à mémoire bornée*. Thèse de doctorat, Université Paris-Sud, 2010.
- (185) François Bobot. *Logique de séparation et vérification déductive*. These, Université Paris Sud - Paris XI, Dec. 2011. <http://tel.archives-ouvertes.fr/tel-00652508>.
- (186) Jean-Christophe Filliâtre. *Deductive Program Verification*. Thèse d'habilitation, Université Paris-Sud, Dec. 2011.
- (187) Johannes Kanig. *Spécification et preuve de programmes d'ordre supérieur*. Thèse de doctorat, Université Paris-Sud, 2010.
- (188) Matthieu Sozeau. *Un environnement pour la programmation avec types dépendants*. Thèse de doctorat, Université Paris-Sud, Dec. 2008.
- (189) Mohamed Iguernelala. *Strengthening the Heart of an SMT-Solver: Design and Implementation of Efficient Decision Procedures*. Thèse de doctorat, Université Paris-Sud, June 2013. <http://tel.archives-ouvertes.fr/tel-00842555>.
- (190) Nicolas Rousset. *Automatisation de la Spécification et de la Vérification d'applications Java Card*. Thèse de doctorat, Université Paris-Sud, June 2008.
- (191) Paolo Herms. *Certification of a Tool Chain for Deductive Program Verification*. Thèse de doctorat, Université Paris-Sud, Jan. 2013. <http://tel.archives-ouvertes.fr/tel-00789543>.
- (192) Romain Bardou. *Verification of Pointer Programs Using Regions and Permissions*. Thèse de doctorat, Université Paris-Sud, Oct. 2011. <http://tel.archives-ouvertes.fr/tel-00647331>.
- (193) Stéphane Lescuyer. *Formalisation et développement d'une tactique réflexive pour la démonstration automatique en Coq*. Thèse de doctorat, Université Paris-Sud, Jan. 2011.

- (194) Sylvain Conchon. *SMT Techniques and their Applications: from Alt-Ergo to Cubicle*. Thèse d'habilitation, Université Paris-Sud, Dec. 2012. In English, <http://www.lri.fr/~conchon/publis/conchonHDR.pdf>.
- (195) Thi Minh Tuyen Nguyen. *Taking architecture and compiler into account in formal proofs of numerical programs*. Thèse de doctorat, Université Paris-Sud, June 2012. <http://tel.archives-ouvertes.fr/tel-00710193>.
- (196) Thierry Hubert. *Analyse Statique et preuve de Programmes Industriels Critiques*. Thèse de doctorat, Université Paris-Sud, June 2008.
- (197) Yannick Moy. *Automatic Modular Static Safety Checking for C Programs*. PhD thesis, Université Paris-Sud, Jan. 2009.
- (198) X. Urbain. *Preuve automatique : techniques, outils et certification*. Thèse d'habilitation, Université Paris-Sud 11, Nov. 2010.

Shared publications

Conference articles

Major international conferences and workshops

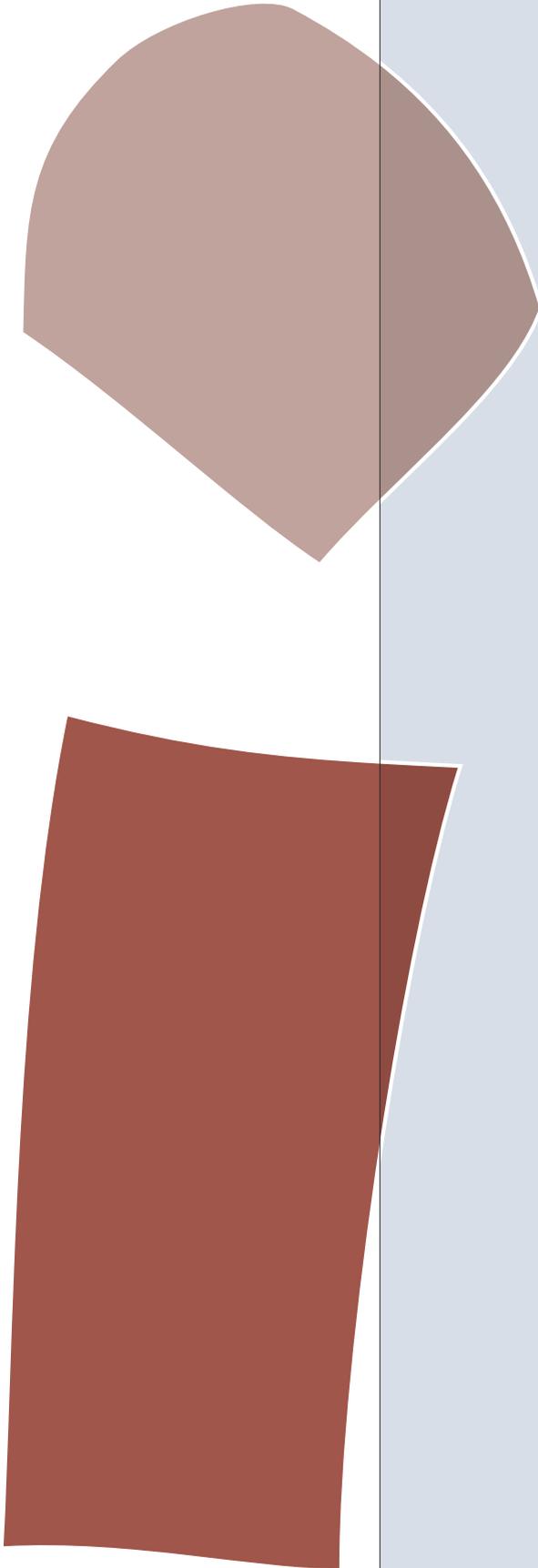
- (1) David Baelde, Pierre Courtieu, David Gross-Amblard, and Christine Paulin-Mohring. Towards Provably Robust Watermarking. In *ITP 2012*, volume 7406 of *Lecture Notes in Computer Science*, Aug. 2012.
- (2) Sylvain Conchon, A. Goel, S. Krstić, Alain Mebsout, and Fatiha Zaïdi. Cubicle: A parallel SMT-based model checker for parameterized systems. In M. Parthasarathy and S. A. Seshia, editors, *CAV 2012: Proceedings of the 24th International Conference on Computer Aided Verification*, volume 7358 of *Lecture Notes in Computer Science*, Berkeley, California, USA, July 2012. Springer.
- (3) Véronique Benzaken, G. Castagna, Dario Colazzo, and C. Miachon. Pattern by example: Type-driven visual programming of XML queries. In *10th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming*, Valencia, Spain, July 2008.
- (4) Véronique Benzaken, Jean-Daniel Fekete, Pierre-Luc Hémyery, Wael Khemiri, and Ioana Manolescu. EdiFlow: data-intensive interactive workflows for visual analytics. In S. Abiteboul, C. Koch, and T. K. Lee, editors, *International Conference on Data Engineering (ICDE)*. IEEE Comp. Soc. Press, Apr. 2011.

Other conferences and workshops

- (5) Albert Cohen, Louis Mandel, Florence Plateau, and Marc Pouzet. Relaxing synchronous composition with clock abstraction. In *Hardware Design using Functional languages*, pages 35–52, York, UK, Mar. 2009.
- (6) Manolescu, Ioana, Khemiri, Wael, Benzaken, Veronique, and Fekete, Jean-Daniel. Reactive workflows for visual analytics. In B. Amann, editor, *Journées Bases de Données Avancées*, Belgique Namur, 2009.
- (7) Véronique Benzaken, Jean-Daniel Fekete, Wael Khemiri, and Ioana Manolescu. Ediflow: data-intensive interactive workflows for visual analytics. In *Journées Bases de Données Avancées*, Toulouse France, Oct. 2010.

Other publications

- (8) N. Lupinski, Joël Falcou, and Christine Paulin-Mohring. Sémantiques d'un langage de squelettes. <http://www.lri.fr/~paulin/Skel>, 2012.



6/ Annexe 7: Thèses

Annexe 7: Thèses

Toccatà

6/ Annexe 7: Thèses

Thesis

Defended thesis				
<i>Name</i>	<i>Start</i>	<i>Defense</i>	<i>Funding</i>	<i>Advisor</i>
Cédric AUGER	01.09.2008	07.02.2013	Alloc. Ministère	POUZET
Romain BARDOU	01.09.2007	14.10.2011	Alloc. Ministère	MARCHÉ
François BOBOT	01.10.2008	12.12.2011	Alloc. Ministère	FILLIÂTRE
Paolo HERMS	01.10.2009	14.01.2013	CEA-List	MARCHÉ
Thierry HUBERT	01.10.2004	20.06.2008	CIFRE Dassault-Aviation	MARCHÉ
Mohamed IGUERNE LALA	01.10.2009	10.06.2013	Alloc. Ministère	CONCHON, CONTEJEAN
Johannes KANIG	01.09.2007	26.11.2010	CDD sur contrat INRIA	PAULIN-MOHRING, FILLIÂTRE
Stéphane LESCUYER	16.07.2007	04.01.2011	CDD sur contrat INRIA	CONTEJEAN, CONCHON
Yannick MOY	01.12.2005	15.01.2009	CIFRE France Telecom	MARCHÉ
Thi Minh Tuyen NGUYEN	01.02.2009	11.06.2012	Contrat Digiteo-Inria	MARCHÉ, BOLDO
Florence PLATEAU	01.10.2005	06.01.2010	Alloc. Ministère	POUZET, MANDEL
Nicolas ROUSSET	01.10.2004	30.06.2008	CIFRE Gemalto	MARCHÉ
Matthieu SOZEAU	01.10.2005	08.12.2008	Alloc. Ministère	PAULIN-MOHRING
Asma TAFAT-BOUZID	01.10.2009	06.09.2013	Alloc. Ministère	MARCHÉ

Habilitation à Diriger des Recherches	
<i>Name</i>	<i>Defense</i>
Sylvain CONCHON	12.2012
Jean-Christophe FILLIÂTRE	12.2011
Xavier URBAIN	11.2010

Thesis in progress			
<i>Name</i>	<i>Start</i>	<i>Funding</i>	<i>Advisor</i>
Martin CLOCHARD	14.09.2013	E.N.S. Paris	MARCHÉ
Claire DROSS	01.01.2011	CIFRE AdaCore	MARCHÉ, PASKEVICH
Stefania DUMBRAVA	01.10.2012	Alloc. Ministère	BENZAKEN, CONTEJEAN
Léon GONDELMAN	01.10.2013	Contrat ANR BWare	FILLIÂTRE, PASKEVICH
Catherine LELAY	03.10.2011	contrat Digiteo-Inria	BOLDO, MELQUIOND
Alain MEBSOUT	01.10.2011	Alloc. Ministère	CONCHON