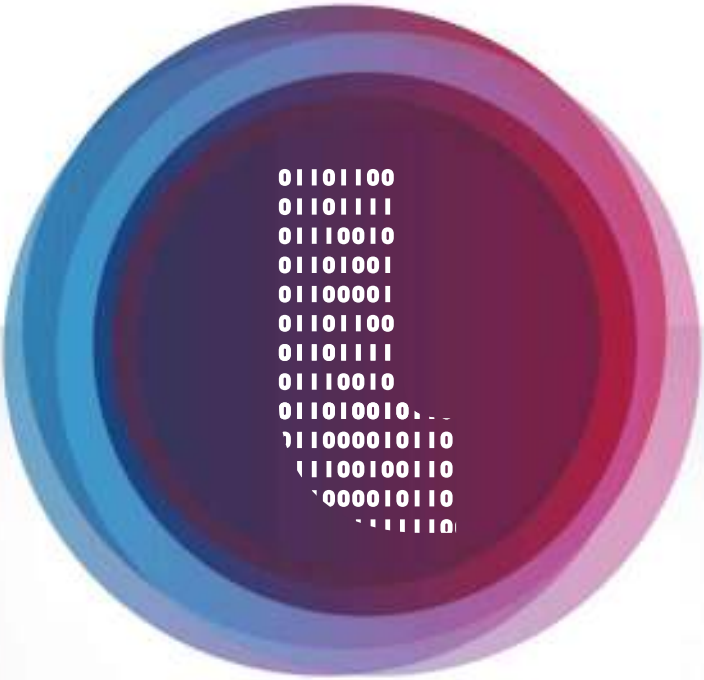
Loria
Laboratoire lorrain de recherche en informatique et ses applications

Lorraine Laboratory of
Research in Computer Science
and its Applications

ACTIVITY REPORT 2014



TEAM

Mosel

Proof-oriented development of computer-based systems

Research / Training / Transfer
in an international context

Table of contents

1. Team

Team leader

Dominique Méry [Professor, Université de Lorraine]

Faculty members

Marie Duflot-Kremer [Associate Professor, Université de Lorraine]
Didier Fass [Associate Professor, ICN]
Pascal Fontaine [Associate Professor, Université de Lorraine]
Denis Roegel [Associate Professor, Université de Lorraine]

Research scientist

Stephan Merz [Senior Researcher, Inria]

Post-doctoral researchers

Jingshu Chen [Airbus Foundation]
Anton Tarasyuk [Université de Lorraine and Région Lorraine, until 09/2014]

External Collaborator

Pierre Castéran [Associate Professor, LABRI Université de Bordeaux]
David Déharbe [Associate Professor, Univ. Federaldo Rio Grande de Norte, Brazil]

Visitors

Carlos Areces [Univ. Nacional de Córdoba, Argentina, 07/2014]
Luciana Benotti [Univ. Nacional de Córdoba, Argentina, 07/2014]
Richard Bonichon [Univ. Federal do Rio Grande do Norte, Brazil, 09/2014]
Raúl Fervari [Univ. Nacional de Córdoba, Argentina, 07/2014]
Guillaume Hoffmann [Univ. Nacional de Córdoba, Argentina, 07/2014]
Claudia Tavares [Univ. Federal do Rio Grande de Norte, Brazil, 09/2014]

PhD students

Manamiary Bruno Andriamiarina [Université de Lorraine, since 10/2010, ministery grant]
Haniel Barbosa [Université de Lorraine, since 12/2013, Inria, CORDI grant]
Pablo Federico Dobal [Université de Lorraine, since 09/2014, funded by ANR and Région Lorraine]
Souad Kherroubi [Université de Lorraine, since 12/2014, ANR IMPEX grant]
Rémi Nazin [Université de Lorraine, since 10/2014, DGA CNRS grant]
Hernán Vanzetto [Université de Lorraine, until 03/2014, funded by MSR-INRIA Joint Centre]

Student interns

Clément Herouard [ENS Rennes, 05–07/2014]
Ignacio Queralt Flores [Univ. Nacional de Córdoba, 04–09/2014]
Rémi Nazin [Master Sciences Cognitives, Université de Lorraine, 04-09/2014]
Rushikesh Sawan [Erasmus Mundus DESEM, Université de Lorraine, 03-06/2014]

Engineer

Pablo Federico Dobal [Inria, until 08/2014, funded by ADT veriT]

Administrative staff

Sophie Drouot [Assistant, Inria]
Delphine Hubert [Assistant, Université de Lorraine]
Martine Kuhlmann [Assistant, CNRS]

Note on the team. Most members of the Mosel team are part of the Inria project team VeriDis, which also includes members of the Automated Reasoning group of Max Planck Institute for Informatics in Saarbrücken, Germany. The VeriDis report for 2014 is available separately.

2. Overall Objectives

Proof-oriented system development focuses on formally describing and analyzing design models for computer-based systems. Because the descriptions are based on sound semantic models, they aim at ensuring higher levels of reliability and correctness. The Mosel research team develops such concepts, and applies them, focusing on reactive, real-time, distributed, and mobile systems that may contain both hardware and software components. Key concepts in the approach advocated by our group are *refinement* and *(de-)composition* that support the development of complex systems across several layers of abstraction. Our work is structured along the following lines of research:

Foundations and methodology. The basic theories underlying formal methods have been firmly established since several decades, and we refrain from developing completely new approaches. However, novel concepts of system design or novel application domains, including the security of computerized systems, asynchronous distributed and mobile systems or hardware/software codesign require extensions and adaptations of existing formalisms (B and TLA$^+$ are the two main frameworks used by our group). Moreover, formal methods need to be integrated in standard industrial development cycles, requiring serious attention to the methodology of their application. For example, specifications and proofs represent proper artefacts of system design, and we engage in work on their representation, management, and reuse, based on composition and genericity.

Techniques and tools for system verification. We study notations that aid system engineers in representing useful concepts, and that integrate different methods and tools of system design. We also engage in developing support tools or – whenever possible – in interfacing existing tools to facilitate their use or support their application in novel contexts. In particular, we contribute techniques and tools that support efficient deduction and bug finding, with a high degree of automation.

Applications. Industrial and academic case studies serve to validate our concepts and theories and lay the foundation for their transfer to use by practitioners in industry. They also force us to recognize deficiencies of our concepts, stimulating further theoretical advances and tool development. We are therefore maintaining active cooperations with partners in industry, such as ClearSy, Systerel or Microsoft Research, and academia, including neighboring disciplines such as control theory or circuit design. We also use our methods in the courses that we teach, which helps us evaluate their applicability.

3. Scientific Foundations

3.1. Foundations and Methodology

The Mosel team investigates methods to develop provably correct computer-based systems. The class of systems we are interested in includes reactive, distributed, embedded, and mobile systems. In contrast to classical sequential algorithms that can be characterized in terms of their input-output relation, the correctness of such systems is described in terms of their executions (traces). The choice of an adequate formal language depends on which properties are of interest for a given system. For example, methods based on pre- and postconditions suffice for expressing and proving safety properties, while temporal logics can also express liveness.

We are particularly interested in processes and methodologies that underly proof-based system *development*, as opposed to the verification of an existing system a posteriori. This view is formally reflected by the concept of *refinement*, which ensures that descriptions produced during later stages of system design preserve earlier, more abstract descriptions; in particular, all properties proved earlier remain valid for the refined model. In this way, the effort of verification is spread over the entire development process, and this helps us to achieve a significant degree of automation in our verification efforts. Crucially, errors can be detected early, when they are relatively inexpensive to correct. The formalisms that we are most familiar with are Abrial's (Event-)B

method [41, 42] and temporal logic [6], in particular the Temporal Logic of Actions and the TLA$^+$ language introduced by Lamport [46]. Members of Mosel have written tutorial presentations of these methods [3, 7].

The second cornerstone of system development is composition and decomposition [45]. Indeed, monolithic system development methods do not scale to realistic systems. Composition refers to the assembly of complex systems from independently developed, possibly pre-existing components. Dually, an entire system (or its specification) can be decomposed into separate subsystems that are then refined individually. Decomposition is a fundamental structuring principle of the Event-B method.

The contributions of the Mosel team to the foundations of this area concern extensions of the semantic models for particular types of systems such as distributed real-time, mobile or security-sensitive systems. We also study ways to make developments more easily reusable by focusing on generic theories and proofs that can later be instantiated for reuse.

3.2. Notation and tools

The development of provably correct systems [1] relies on languages with a precise, mathematically defined semantics. For all but toy systems, formal development methods generate a significant number of proof obligations, and highly automated tools become essential to successfully apply the methods. Whereas automated deduction has made substantial progress, each technique typically covers a restricted domain, and the combination of different tools is an active area of research.

Members of Mosel develop veriT [2], an SMT (Satisfiability Modulo Theories[43]) solver that combines decision procedures for different fragments of first-order logic and that integrates an automatic theorem prover for full first-order logic. The veriT solver is designed to produce detailed proofs; this makes it particularly suitable as a component of a robust cooperation of deduction tools.

We rely on interactive theorem provers for reasoning about specifications at a high level of abstraction. Members of Mosel have ample experience in the specification and subsequent machine-assisted, interactive verification of algorithms. In particular, we participate in a project at the joint MSR-INRIA Centre in Saclay on proof support for TLA$^+$[46] specifications. Our prover relies on an explicit, hierarchical proof language and includes different automatic backend provers [4].

4. Application Domains

Our work focuses on distributed algorithms and protocols. These are or will be found at all levels of computing infrastructure, from many-core processors and systems-on-chip to wide-area networks. We are particularly interested in novel paradigms, for example ad-hoc networks that underly mobile and low-power computing or overlay networks and peer-to-peer networking that provide services for telecommunication or cloud computing services. Distributed protocols underly computing infrastructure that must be highly available and mostly invisible to the end user, therefore correctness is important. One should note that standard problems of distributed computing such as consensus, group membership or leader election have to be reformulated for the dynamic context of these modern systems. We are not ourselves experts in the design of distributed algorithms, but work together with domain experts on the modeling and verification of these protocols. These cooperations help us focus on concrete algorithms and ensure that our work is relevant to the distributed algorithm community.

Formal verification techniques that we study can contribute to certify the correctness of systems. In particular, they help assert under which assumptions an algorithm or system functions as required. For example, the highest levels of the Common Criteria for Information Technology Security Evaluation require code analysis, based on mathematically precise foundations. While initially the requirements of certified development have mostly been restricted to safety-critical systems, they are becoming more and more common due to the cost associated with malfunctioning system components and software. We are in particular working on modeling and verifying medical devices that require closed-loop models of both the system and its environment.

5. Software

5.1. The veriT solver

Participants: Haniel Barbosa, David Déharbe, Pablo Federico Dobal, Pascal Fontaine [correspondent]..

The veriT solver is an SMT (Satisfiability Modulo Theories) solver developed in cooperation with David Déharbe from the Federal University of Rio Grande do Norte in Natal, Brazil. The solver can handle large quantifier-free formulas containing uninterpreted predicates and functions, and arithmetic over integers and reals. It features a very efficient decision procedure for uninterpreted symbols, as well as a simplex-based reasoner for linear arithmetic. It also has some support for user-defined theories, quantifiers, and lambda-expressions. This allows users to easily express properties about concepts involving sets, relations, etc. The prover can produce explicit proof traces when it is used as a decision procedure for quantifier-free formulas with uninterpreted symbols and arithmetic. To support the development of the tool, a regression platform using INRIA's grid infrastructure is used; it allows us to extensively test the solver on thousands of benchmarks in a few minutes. The veriT solver is available as open source under the BSD license at the veriT Web site.

Efforts in 2014 have been focused on efficiency and stability. The decision procedures for uninterpreted symbols and linear arithmetic have been further improved. There has also been some progress in the integration of the solver Redlog for non-linear arithmetic in the context of the SMArT project.

The veriT solver participated in the SMT competition SMT-COMP 2014, part of the Vienna Summer Of Logic Olympic Games, and received the gold medal for SMT. The success of the different solvers was measured as a combination of the number of benchmark problems solved in the various categories, the number of erroneous answers, and the time taken.

We target applications where validation of formulas is crucial, such as the validation of TLA$^+$ and B specifications, and work together with the developers of the respective verification platforms to make veriT even more useful in practice. The solver is available as a plugin for the Rodin platform for discharging proof obligations generated in Event-B [12]; on a large repository of industrial and academic cases, this SMT-based plugin decreased by 75% the number of proof obligations requiring human interactions, compared to the original B prover.

5.2. The TLA$^+$ proof system

Participants: Stephan Merz [correspondent], Hernán Pablo Vanzetto..

TLAPS, the TLA$^+$ proof system developed at the Joint MSR-INRIA Centre, is a platform for developing and mechanically verifying proofs about TLA$^+$ specifications. The TLA$^+$ proof language is hierarchical and explicit, allowing a user to decompose the overall proof into independent proof steps. TLAPS consists of a *proof manager* that interprets the proof language and generates a collection of proof obligations that are sent to *backend verifiers*. The current backends include the tableau-based prover Zenon for first-order logic, Isabelle/TLA$^+$, an encoding of TLA$^+$ as an object logic in the logical framework Isabelle, a generic SMT backend, and an interface to a decision procedure for propositional temporal logic.

The current version 1.3.2 of TLAPS was released in May 2014, it is distributed under a BSD-like license at http://tla.msr-inria.inria.fr/tlaps/content/Home.html. The prover fully handles the non-temporal part of TLA$^+$. The SMT backend, developed in Nancy, has been further improved in 2014, in particular through the development of an appropriate type synthesis procedure, and is now the default backend. A new interface with a decision procedure for propositional temporal logic has been developed in 2014, so that simple temporal proof obligations can now be discharged. It is based on a technique for "coalescing" first-order subformulas of temporal logic, described in section 6.3. The standard proof library has also been further developed, partly in response to the needs of the ADN4SE project on verifying a real-time micro-kernel system.

TLAPS was presented at tutorials at the TLA$^+$ community event organized during ABZ 2014 in Toulouse in June and at the SPES_XT summer school at the University of Twente (The Netherlands) in September.

6. New Results

6.1. Highlights of the year

The veriT solver (section 5.1) participated in the SMT competition 2014, part of the Vienna Summer Of Logic Olympic Games, and received the gold medal for SMT.

6.2. Proved development of algorithms and systems

6.2.1. Incremental development of distributed algorithms

Participants: Manamiary Andriamiarina, Dominique Méry..

Joint work with Mohammed Mosbah and Mohammed Tounsi from the LABRI laboratory in Bordeaux, France, and with Neeraj Kumar Singh from the Department of Computing and Software, McMaster University, Hamilton, Canada.

The development of distributed algorithms and, more generally, of distributed systems, is a complex, delicate, and challenging process. The approach based on refinement helps to gain formality by using a proof assistant, and proposes to apply a design methodology that starts from the most abstract model and leads, in an incremental way, to the most concrete model, for producing a distributed solution. Our work helps formalizing pre-existing algorithms, developing new algorithms, as well as developing models for distributed systems.

Our research was initially supported by the ANR project RIMEL (see http://rimel.loria.fr). More concretely, we aim at an integration of the correct-by-construction refinement-based approach into the *local computation* programming model underlying the VISIDIA toolkit developed at LABRI for designing distributed algorithms expressed as a set of rewriting rules over graph structures.

In particular, we show how state-based models can be developed for specific problems [16] and how they can be simply reused by controlling the composition of state-based models through the refinement relationship. Traditionally, distributed algorithms are supposed to run on a fixed network, whereas we consider a network with a changing topology.

The contribution is related to the development of proof-based patterns providing effective help to the developer of formal models of applications [17, 9, 31]. Our patterns simplify the development of distributed systems using refinement and temporal logic.

6.2.2. Modeling Medical Devices

Participants: Dominique Méry, Anton Tarasyuk..

Formal modelling techniques and tools [23] have attained sufficient maturity for formalizing highly critical systems in view of improving their quality and reliability, and the development of such methods has attracted the interest of industrial partners and academic research institutions. Building high quality and zero-defect medical software-based devices is a particular domain where formal modelling techniques can be applied effectively. Medical devices are very prone to showing unexpected system behaviour in operation when traditional methods are used for system testing. Device-related problems have been responsible for a large number of serious injuries. Officials of the US Food and Drug Administration (FDA) found that many deaths and injuries related to these devices are caused by flaws in product design and engineering. Cardiac pacemakers and

implantable cardioverter-defibrillators (ICDs) are among the most critical medical devices and require closed-loop modelling (integrated system and environment modelling) for verification purposes before obtaining a certificate from the certification bodies.

Clinical guidelines systematically assist practitioners in providing appropriate health care in specific clinical circumstances. Today, a significant number of guidelines and protocols are lacking in quality. Indeed, ambiguity and incompleteness are likely anomalies in medical practice. The analysis of guidelines using formal methods is a promising approach for improving them.

In [25], we give the semantics of refinement diagrams that are used in a refinement-based methodology for complex medical systems design, which possesses all the required key features. A refinement-based approach relying on formal verification, model validation using a model-checker, and refinement charts is proposed in this methodology for designing a high-confidence medical device. We show the effectiveness of this methodology for the design of a cardiac pacemaker system. Moreover, we organized a Dagstuhl seminar on the Pacemaker Challenge [14].

6.2.3. Analysis of real-time concurrent programs

Participants: Jingshu Chen, Marie Duflot-Kremer, Jorge Ibarra Delgado, Stephan Merz..

Joint work with Nadezhda Baklanova, Jan-Georg Smaus, Wilmer Ricciotti, and Martin Strecker at IRIT Toulouse, France, funded by the Airbus Foundation.

We investigate techniques for the formal verification of multi-threaded real-time programs. We assume that programs contain annotations that indicate the times for executing basic blocks, and that these annotations are enforced by the execution platform. Inspired by Safety-Critical Java [44], our partners in Toulouse developed a formal semantics for a fragment of Java in Isabelle/HOL. We designed techniques for formally ensuring the absence of concurrent accesses to shared resources in bounded-length executions of such programs. Specifically, we generate constraints that characterize the possible execution orders of the program, and then invoke an SMT solver in order to verify that no execution violates precedence constraints that ensure absence of conflicts. In the case where such an execution exists, we obtain a trace that exhibits the access conflict. Our technique has been implemented prototypically, and appears to scale much better than a previous analysis based on an encoding of programs as timed automata. The results have been published at AVoCS 2014 [11].

During his internship within the first year of the Erasmus Mundus master program on Dependable Software Systems, Jorge Ibarra Delgada investigated the possibility of adapting the JOP toolset for Safety-Critical Java, and in particular its Worst-Case Execution Time (WCET) analyzer, for obtaining suitable annotations for basic blocks.

6.2.4. Bounding message length in attacks against security protocols

Participant: Marie Duflot-Kremer..

Joint work with Myrto Arapinis from the University of Glasgow, UK.

Security protocols are short programs that describe communication between two or more parties in order to achieve security goals. Despite the apparent simplicity of such protocols, their verification is a difficult problem and has been shown to be undecidable in general. This undecidability comes from the fact that the set of executions to be considered is of infinite depth (an infinite number of protocol sessions can be run) and infinitely branching (the intruder can generate an unbounded number of distinct messages). Several attempts have been made to tackle each of these sources of undecidability. We have shown that, under a syntactic and reasonable condition of "well-formedness" on the protocol, we can get rid of the infinitely branching part. A journal version of this result, extending the set of security properties to which it is applicable and that particular includes authentication properties, has been published in Information and Computation [10].

6.2.5. Evaluating and verifying probabilistic systems

Participant: Marie Duflot-Kremer.

Joint work with colleagues at ENS Cachan and University Paris Est Créteil.

Since its introduction in the 1980s, model checking has become a prominent technique for the verification of complex systems. The aim was to decide whether or not a system fulfills its specification. With the rise of probabilistic systems, new techniques have been designed to verify this new type of systems, and appropriate logics have been proposed to describe more subtle properties to be verified. However, some characteristics of such systems fall outside the scope of model checking. In particular, it is often of interest not to tell wether a property is satisfied but how well the system performs with respect to a certain measure. We have designed a statistical tool for tackling both performance and verification issues. Following several conference talks, two journal papers have been submitted. The first one presents the approach in details with a few illustrative applications. The second one focuses on biological applications, and more precisely the use of statistical model checking to detect and measure several indicators of oscillating biological systems.

6.2.6. Modeling the "augmented human"

Participant: Didier Fass, Rémi Nazin..

Our work on "augmented human" is about researching scientific principles for the integration of humans and systems and aims at developing a modeling framework for the design of validated safety-critical systems with humans in the loop. This work started in 2003 as a pluridisciplinary Artem research project. It gathers theoretical biology, general systems theory, formal methods and virtual environments into an integrative epistemological framework.

In 2014, we have worked on two complementary research axes

1. Firstly, for improving the robustness of our theoretical framewok for describing human systems coupling and human systems integration we intitiated research on epistemology applied to human machine engenieering. That work was carried out in cooperation with Rémi Nazin during his internship for Cognitive Sciences Master. Rémi explored the question of what are suitable epistemological foundations for human machine. He continues as a PhD student in our team in collaboration with Christina Bastien (head of the Perseus team on Social and Ergonomic Psychology for User Experience of University of Lorraine). This PhD thesis is funded by the ministery of defense (Direction générale de l'armement).

2. Secondly, to gather human factors, behavioral health and performance, human machine and Cyber Physical Systems we introduced the concept of Human Machine Nature [22].

Human-Machine (HM) is a concept that integrates cyber-physical and biological systems. The scientific challenge is to design a theoretical framework dedicated to human-machine interaction and integration, its modeling, from epistemology to formal to empirical (experimental) methods. The practical challenge resides in the correct design for enhancement and reliable engineering of human systems integration, from human-machine interaction to sociotechnical system, their behavior and performance.

In this context, we cooperate with the Human Systems Integration Division of NASA Ames Research Center, more specifically with Brian Gore, Space Human Factors Engineering (SHFE) Portfolio Deputy Manager and Ames SHFE Lead.

International collaboration among the National Aeronautics and Space Administration (NASA), the French Aerospace Lab (ONERA) Salon de Provence Research Center, the Defense Advanced Research Project Agency (DARPA), and LORIA will provide opportunities to explore the complex unions of human and cyberphysical systems.

This collaboration project is supported and funded by Communauté Urbaine du Grand Nancy (CUGN).

Future work should:

- address questions related to the development of epistemological principles and their formal model related to augmented human engineering and their experimental validation,
- examine or discuss directions for designing and training *human systems integration*,
- research the (sensorimotory, cognitive and emotional) cognitive capabilities of individual operators and the team,
- develop a new approach to bioengineering that focuses on biological integration and incompatibilities,
- augment the respective Bio-Cyber-Physical Systems (Bio-CPS) portfolios by researching whether the "biologization" of artifacts (training, procedure and technical systems), and thereby reduce inherent variability brought to system performance by the human operator,
- increase educational opportunities through NASA and LORIA.

The domains of application of our research are aerospace, defense, forensic and health.

We have improved our definition and validation of a general isomorphic framework for describing biological and artefactual systems taking into account their structural elements, their shape and their dynamics for modeling their architecture and geometries, their behavior and analytical functions and their evolution and interactions.

Thus designing a human-artefact system consists in organizing the linkage of multimodal biological structures, sensorimotor elements at the hierarchical level of the living body, with the artificial interactive elements of the system, devices and patterns of stimulation. There exists a "transport" of functional interaction in the augmented space of both physiological and artifactual units, and thus a function may be viewed as the final result of a set of functional interactions that are hierarchically and functionally organized between the artificial and biological system elements.

6.2.7. Analysis and reconstruction of mathematical tables

Participant: Denis Roegel.

Our work on historical mathematical tables, from the multiple point of view of their accuracy, their historical context, their reconstruction, and their digital availability, began in 2009 and has already led to a large cluster of documents, essentially available on the LOCOMAT site (LORIA Collection of Mathematical Tables). There are now more than 3000 links to digitized mathematical and astronomical tables, and our growing census has already proven useful to many researchers in the history of mathematics. LOCOMAT has also contributed to the visibility of the LORIA, as a simple search on Google for terms such as "LORIA mathematics" will reveal.

In 2014, we have progressed in the analysis of the numerous tables produced by the Scottish mathematician Edward Sang (1805–1890). Due to our work on other reconstructions, the completion of this work has been delayed, and we hope to publish about Sang's endeavour in 2015. We have also started to work on the tables of the German astronomer Jean Peters (1869–1941), who has in particular produced extensive tables of logarithms of trigonometric functions to six, seven, eight and ten places. This work is also scheduled for publication in 2015.

In 2014, only one table was published, namely Arnaudeau's table of triangular numbers [**?**], computed around 1896, and only available as a manuscript at the École Polytechnique where we consulted it in 2013. This reconstruction complements our earlier reconstruction of a table of triangular numbers by de Joncourt.

6.2.8. 3D representation of complex data and objects

Participant: Denis Roegel.

In 2014, we have started to work on the interplay between science and art, in particular by seeking novel ways to represent certain data. Two simple examples have been the 3D representation of the cycles of Easter dates, both in the Julian and in the Gregorian calendar. In the latter, the task is to summarize 5700000 dates in a compact representation, and we have adopted a multilayered view by coiling together several subperiods [**?**]. A spin-off of this work has been the more artistic production of seemingly random walks on a sphere, based on long sequences of dates of Easter [**?**].

A perhaps more striking example was the representation of the duration of twilight as a function of the latitude of a place and of the longitude of the sun. Because twilight is not a universal phenomenon and because it is what is left of 24 hours when pure day and pure night are removed, each of which possibly non existent, the duration of twilight has a quite convoluted "shape", the result being what we have christened the "twilight flower" [**?**].

Finally, we have also worked on the use of a 3D representation to solve a little architectural "mystery." Many years ago, the mathematician Marcel Berger became interested in a 16th century winding staircase in Strasbourg, whose top seemed to display rings which looked like Villarceau circles. A careful examination of this staircase reveals that these rings are not planar, and can therefore not be Villarceau circles. Using a 3D model, we have suggested a more plausible explanation for these rings, and in particular for their number and for their coiling direction [**?**].

6.2.9. Historical mechanical calculators

Participant: Denis Roegel.

A long interest in mechanical computing, which led to the discovery of the currently oldest known key-driven calculating machine, as well as in the identification of the only known fragments of the prototype of Babbage's first difference engine, made us (re)discover several other machines, in particular an early modular mechanical counter [**?**], a specialized adding machine from the early 1850s [**?**] and several small adding machines [**?**] which we plan to describe in detail in upcoming articles.

6.3. Automated and Interactive Theorem Proving

6.3.1. Combination of satisfiability procedures

Participant: Pascal Fontaine.

Joint work with Christophe Ringeissen from the CASSIS project-team at Inria Nancy Grand-Est, and Paula Chocron, a student at the University of Buenos Aires.

A satisfiability problem is often expressed in a combination of theories, and a natural approach consists in solving the problem by combining the satisfiability procedures available for the component theories. This is the purpose of the combination method introduced by Nelson and Oppen. However, in its initial presentation, the Nelson-Oppen combination method requires the theories to be signature-disjoint and stably infinite (to ensure the existence of an infinite model). The design of a generic combination method for non-disjoint unions of theories is clearly a hard task but it is worth exploring simple non-disjoint combinations that appear frequently in verification. An example is the case of shared sets, where sets are represented by unary predicates. Another example is the case of bridging functions between data structures and a target theory (e.g. a fragment of arithmetic). In collaboration with Paula Chocron (Univ. Buenos Aires, former intern in Cassis) and Christophe Ringeissen (project-team Cassis), we have investigated both cases.

The notion of gentle theory has been introduced in the last few years as one solution to go beyond the restriction of stable infiniteness, in the case of disjoint theories. In [19, 32], we adapt the notion of gentle theory to the non-disjoint combination of theories sharing only unary predicates, constants, and equality. As in the disjoint case, combining two theories, one of them being gentle, requires some minor assumptions on the other one. We show that major classes of theories, i.e. Loewenheim and Bernays-Schoenfinkel-Ramsey, satisfy the appropriate notion of gentleness introduced for this particular non-disjoint combination framework.

We have also considered particular non-disjoint unions of theories connected via bridging functions [20]. We present a combination procedure which is proved correct for the theory of absolutely free data structures. We consider the problem of adapting the combination procedure to obtain a satisfiability procedure for the standard interpretations of the data structure. We present an enumeration procedure that allows us to revisit the case of lists with length.

6.3.2. Type synthesis for set-theoretic proof obligations

Participants: Stephan Merz, Hernán Pablo Vanzetto.

TLA$^+$ is a language for the formal specification of systems and algorithms whose first-order kernel is a variant of untyped Zermelo-Fraenkel set theory. Typical proof obligations that arise during the verification of TLA$^+$ specifications mix reasoning about sets, functions, arithmetic, tuples, and records. One of the challenges in designing an efficient encoding of TLA$^+$ proof obligations for the input languages of first-order automatic theorem provers or SMT solvers is to synthesize appropriate sorts for the terms appearing in a proof obligation, matching the type system of the target prover. We base this synthesis on the detection of "typing hypotheses" present in the proof obligations and then propagate this information throughout the entire formula. An initial type system[47] similar to the multi-sorted discipline underlying SMT-lib was not expressive enough for representing constraints such as domain conditions for function applications. We therefore developed a more expressive type system that includes dependent types, predicate types, and subtyping. Type synthesis in this system is no longer decidable but generates constraints that are submitted to SMT solvers during type reconstruction. When the constraints are valid, the translation of the formula becomes simpler, and checking it becomes correspondingly more efficient. When type construction does not succeed, the translator locally falls back to a sound, but inefficient "untyped" encoding where interpreted sorts such as integers are injected into the SMT sort representing TLA$^+$ values. In practice, this approach is found to behave significantly better than the original type system, and it extends easily to ATP proof backends. The results have been published at NFM 2014 [26], full details appear in Vanzetto's PhD thesis [8].

6.3.3. Syntactic Abstractions in First-Order Modal Logics

Participants: Stephan Merz.

Joint work with Damien Doligez, Jael Kriener, Leslie Lamport, and Tomer Libal within the TLA$^+$ project at the MSR-INRIA Joint Centre.

TLA$^+$ proofs mix first-order and temporal logics, and few (semi-)automatic proof tools support such languages. Moreover, natural deduction and sequent calculi, which are standard underpinnings for reasoning in first-order logic, do not extend smoothly to modal or temporal logics, due to the presence of implicit parameters designating the current point of evaluation. We design a syntactic abstraction method for obtaining pure first-order, respectively propositional modal or temporal, formulas from proof obligations in first-order modal or temporal logic, and prove the soundness of this "coalescing" technique. The resulting formulas can be passed to existing automatic provers or decision procedures for first-order logic (possibly with theory support), respectively for propositional modal and temporal logic. The method is complete for proving safety properties of specifications. This work was presented at the workshop on Automated Reasoning in Quantified Non-Classical Logic organized as part of Vienna Summer of Logic [21], and it has been implemented within TLAPS (section

5.2).

6.3.4. Satisfiability of Propositional Modal Logics via SMT Solving

Participants: Pascal Fontaine, Stephan Merz.

Joint work with Carlos Areces from the National University of Córdoba, Argentina, and Clément Herouard, a student at ENS Rennes.

Modal logics extend classical propositional logic, and they are robustly decidable. Most existing decision procedures for modal logics are based on tableau constructions. Within our ongoing cooperation with members of the National University of Córdoba supported by the MEALS and MISMT projects, we are investigating the design of decision procedures based on adding custom instantiation rules to standard SAT and SMT solvers. Our constructions build upon the well-known standard translation of modal logics to the guarded fragment of first-order logic. The idea is to let the solver maintain an abstraction of the quantified formulas, together with corresponding models. The abstraction is refined by lazily instantiating quantifiers, until either it is found to be unsatisfiable or no new instantiations need to be considered. We prove the soundness, completeness, and termination of the procedure for basic modal logic and several extensions. In particular, a smooth extension to hybrid logic makes use of the decision procedures for equality built into SMT solvers, yielding surprisingly simple correctness proofs. A presentation of this work has been accepted for publication in 2015.

7. Collaborations and Contracts

7.1. National Projects

7.1.1. ANR Project IMPEX

Participants: Manamiary Bruno Andriamiarina, Pierre Castéran, Souad Kherroubi, Dominique Méry..

The ANR Project IMPEX is an INS ANR project that started in December 2013 for 4 years. The partners are LORIA as coordinator, IRIT/ENSEIHT, Systerel, Supelec and Telecom Sud Paris.

All software systems execute within an environment or context. Reasoning about the correct behavior of such systems is a ternary relation linking the requirements, system and context models. Formal methods are concerned with providing tool (automated) support for the synthesis and analysis of such models. These methods have quite successfully focused on binary relationships, for example: validation of a formal model against an informal one, verification of one formal model against another formal model, generation of code from a design, and generation of tests from requirements. The contexts of the systems in these cases are treated as second-class citizens: in general, the modeling is implicit and usually distributed between the requirements model and the system model. This project proposal is concerned with the explicit modeling of contexts as first-class citizens.

Several approaches aim at formalizing mathematical theories that are applicable in the formal developments of systems. These theories are helpful for building complex formalizations, expressing and reusing proof of properties. Usually, these theories are defined within contexts, that are imported and and/or instantiated. They usually represent the implicit semantics of the systems and are expressed by types, logics, algebras, etc. However, an implicit handling of contexts loses important information, and therefore is not expressive enough for ensuring that even a verified system is "correct". As a very simple example, take two formally developed systems that are composed to exchange currency data represented by a float. This system is no longer consistent if one system refers to Euros and the other to dollars. The objective of the IMPEX project is to build explicit formal models of contextual semantics and to extend proof-based techniques for handling such a stronger semantics [18].

7.1.2. ANR-DFG Project SMArT

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

The SMArT (Satisfiability Modulo Arithmetic Theories) project is funded by *ANR-DFG Programmes blancs 2013*, a program of the Agence Nationale de la Recherche and the (German) Deutsche Forschungsgemeinschaft DFG. It started in April 2014. The partners are Mosel, the Automation of Logic Group at Max-Planck Institute for Informatics in Saarbrücken, and the Systerel company. The objective of the SMArT project is to provide advanced techniques for arithmetic reasoning beyond linear arithmetic for formal system verification, and particularly for SMT. Arithmetic reasoning is one strong direction of research at MPI, and the results of the project will be validated by an integration of Redlog, mainly developed by Thomas Sturm, and veriT (section 5.1).

In September 2014, Pablo Federico Dobal was hired as a PhD student in joint supervision with Saarland University, co-funded by the SMArT project and the Région Lorraine. More information on the project can be found on http://smart.gforge.inria.fr/.

7.1.3. Project funded by the Airbus Foundation

Participants: Jingshu Chen, Marie Duflot-Kremer, Pascal Fontaine, Stephan Merz.

This two-year project (2013/2014) funds our work on the analysis of real-time concurrent programs described in section 6.2, and in particular part of the salary of Jingshu Chen as a post-doctoral researcher. It is complemented by funds granted by Région Lorraine.

7.1.4. Project at MSR-INRIA Centre

Participants: Stephan Merz, Hernán-Pablo Vanzetto.

We participate in the project on Tools and Methodologies for Formal Specifications and for Proofs at the MSR-INRIA Joint Centre. The objective of the project is to develop a proof environment for verifying distributed algorithms in TLA$^+$ (see also sections 5.2 and 6.3). In particular, the project funds the PhD thesis of Hernán Vanzetto.

7.1.5. Project ADN4SE

Participant: Stephan Merz.

Joint work with Damien Doligez of Inria Paris Rocquencourt and Jael Kriener and Tomer Libal at the Joint MSR-INRIA Centre.

The ADN4SE project started in 2013 within *Programme d'Investissements d'Avenir: Briques Génériques du Logiciel Embarqué*. The objective of this project is to develop and commercialize the PharOS real-time micro-kernel operating system. In cooperation with researchers at CEA-List, we are contributing to the project by verifying key properties (in particular, determinism) of a high-level model of the system written in TLA$^+$.

7.1.6. Regional Funding

Participants: Jingshu Chen, Pablo Federico Dobal, Pascal Fontaine, Stephan Merz.

The PhD thesis of Pablo Federico Dobal benefits from joint funding by Région Lorraine since September 2014, complementing funding through the ANR-DFG project SMArT. The post-doctoral research of Jingshu

Chen is jointly funded by Région Lorraine and the Airbus Foundation.

7.1.7. Inria Development Action VeriT

Participants: Pablo Dobal, Pascal Fontaine.

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

7.2. Participation In International Programs

7.2.1. FP7 project MEALS

Participants: Haniel Barbosa, Pablo Federico Dobal, Pascal Fontaine, Stephan Merz.

MEALS is a Marie Curie IRSES project (October 2011 – September 2015) for exchanging scientists between Europe and Argentina. It is coordinated by Holger Hermanns from Saarland University (Germany) and involves partners from Germany (RWTH Aachen, TU Dresden), the UK (Imperial College, Univ. of Leicester), the Netherlands (TU Eindhoven) and France (Inria) on the European side and Universidad de Buenos Aires, Universidad Nacional de Córdoba, Universidad Nacional de Rio Cuarto, and Instituto Teconológico Buenos Aires in Argentina. It is structured in five work packages (Quantitative Analysis of Concurrent Program Behaviour, Reasoning Tasks for Specification and Verification, Security and Information Flow Properties, Synthesis in Model-based Systems Engineering, Foundations for the Elaboration and Analysis of Requirements Specifications). Our team mainly cooperates with the group led by Carlos Areces in Córdoba within work package 2. In 2014, the project funded visits by Stephan Merz to Córdoba and by Carlos Areces, Luciana Benotti, Raúl Fervari, and Guillaume Hoffmann to Nancy.

7.2.2. Cooperation with NASA Ames Research Center, U.S.A.

Participants: Didier Fass, Dominique Méry..

Didier Fass and Dominique Méry have started a close working relationship with NASA Ames Reseach Center, Human Systems Integration Division (HSI) and more particularly with Dr. Brian Gore. It is anticipated that collaboration among the researchers at NASA Ames and LORIA will lead to more formal understanding of the methods required to optimize human-systems integration issues in the design of complex human-automation systems. This increase in collaborative research will lead to knowledge increases that will in turn reduce gaps and improve the risk profile of both NASA and LORIA.

7.2.3. Cooperation with NUI Maynooth, Ireland

Participant: Dominique Méry..

The project *Building Reliable Systems: Software Refinement meets Software Verification* was a one-year project funded by PHC Ulysses. The academic Irish partner is Rosemary Monahan of NUI Maynooth. The

verification of software requires the specification of preconditions and postconditions as well as other properties of the code. These properties are expressed as annotations and provide a detailed understanding of how the software is implemented. In program verification, the annotation process is often done *a posteriori*, with verification tools used to check that annotations are sound according to the semantics of the program. Determining the correct annotations to provide a complete specification is difficult, especially when specifying invariant properties of the code. *A priori* techniques for developing correct software are based on the correct-by-construction paradigm. The refinement-based approach is such a technique, providing for the construction of a correct program through the step-by-step refinement of an initial high-level model of the software. In this way, the program specification is developed alongside the code, discharging the conditions that need to be proved. We focus on combining these two software engineering techniques, to benefit from the strengths of both. We have proposed a framework for integrating the *a posteriori* paradigm Spec# and the *a priori* paradigm Event-B. This integration induces a methodology that bridges the gap between software modeling and program verification in the software development life cycle. During this year, we have designed the Rodin plugin EB2RC that implements transformations of Event-B models into algorithms.

7.2.4. STIC AmSud MISMT

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

VeriDis has a close working relationship with two South American teams at Universidade Federal do Rio Grande de Norte (UFRN), Brazil (more specifically with Prof. David Déharbe), and at Universidad Nacional de Córdoba, Argentina (more specifically with Prof. Carlos Areces). The STIC AmSud MISMT project, including both teams and Mosel, started in 2014. It complements the MEALS project and extends it to cooperation with UFRN.

The project is centered around Satisfiability Modulo Theories, with a focus on applications to Modal Logic. Notably, the project sustains the development of the veriT solver (section 5.1), of which David Déharbe and Pascal Fontaine are the main developers. First results on using SMT for modal logic have been accepted for publication.

In February, Stephan Merz spent three weeks in Córdoba. David Déharbe stayed in Nancy until July, on a sabbatical from UFRN. A workshop with many participants from the project took place in Nancy in early July. Richard Bonichon and Claudia Tavares visited Nancy in September. At the end of the year, Haniel Barbosa (VeriDis PhD student in co-tutelle with Natal) spent three months in Natal and visited Córdoba for two weeks.

More information on the STIC AmSud MISMT project is available on http://mismt.gforge.inria.fr/.

7.3. Visits of International Scientists

David Déharbe from Universidade Federal do Rio Grande do Norte (Natal, Brazil) spent a sabbatical year with the VeriDis team in Nancy from August, 2013 to July, 2014.

Carlos Areces, Luciana Benotti, Raúl Fervari, and Guillaume Hoffmann from Universidad Nacional de Córdoba, Argentina visited Mosel for a research stay in July, 2014. Richard Bonichon and Claudia Tavares from Universidade Federal do Rio Grande do Norte visited Mosel in September, 2014.

7.4. Internships

Ignacio Queralt Flores from Universidad Nacional de Córdoba (Argentina) visited Mosel within the Inria International Internship program from April to September, 2014. He worked on symbolic techniques for transition checking in TLA$^+$.

During his internship between May and July, 2014, Clément Herouard from ENS Rennes (France) worked on SMT techniques for modal logics and their extensions.

8. Dissemination

8.1. Scientific Animation

- Didier Fass is
  - an expert for the French Agence Nationale de la Recherche (ANR),
  - Member of the board and of the scientific committee of Association francophone des spécialistes de l'investigation numérique,
  - member of the selection committee, Young Innovators Competition, International Telecommunication Union, Geneva,
  - Member of the scientific committee of think tank Renaissance Numérique,
  - Member of Espace lorrain d'éthique pour la santé
- Pascal Fontaine
  - co-organized the SAT/SMT Summer School 2014, affiliated with Vienna Summer of Logic, in Semmering, Austria,
  - served on the program committees of the the International Joint Conference on Automated Reasoning (IJCAR) and of the workshops PAAR and SMT,
  - was an elected member of the SMT Steering Committee (2012–2014), and is one of three SMT-LIB managers,
  - has been an elected CADE trustee since October 2014.
- Dominique Méry is
  - a member of the IFIP Working Group 1.3 on *Foundations of System Specification*,
  - head of the Doctoral School IAEM Lorraine for the University of Lorraine,
  - head of the Formal Methods department of the LORIA laboratory,
  - an expert for the French Ministry of Education (DS9),
  - an expert for the French Agence Nationale de la Recherche (ANR) and AERES.
  - He co-chaired the program committees of the 11th International Colloquium on Theoretical Aspects of Computing, held in Bucharest, Romania in September, and of the First Workshop on Formal Integrated Development Environments, a satellite of ETAPS in Grenoble, France, in April.
  - He served on the program committees of ABZ, AFADL, CSDM, MedicalCPS, FHIES, FM, ICFEM, iFM, and FACS.
- Stephan Merz is
  - a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*,
  - the INRIA representative in the Scientific Directorate of the International Computer Science Meeting Center in Dagstuhl,
  - the delegate for the organization of conferences at INRIA Nancy Grand-Est,
  - co-head of the PhD committee for computer science in Lorraine,
  - co-organizer of the VTSA summer school between Nancy, Saarbrücken, Luxembourg, and Liège,
  - guest editor (together with Gerald Lüttgen of University of Bamberg) of a special issue of Science of Computer Programming on the Automated Verification of Critical Systems,

- co-chair of the program committee of the 16th International Conference on Formal Engineering Methods, held in Luxembourg in November, of the First International Workshop on Formal Reasoning in Distributed Algorithms (FRIDA) in July, as part of Vienna Summer of Logic, and of the TLA$^+$community meeting in Toulouse,
- a member of the program committees of ABZ, IJCAR, SAC, SEFM, SSS, and of the workshops AVoCS, GRSRD, SETS, and VERIFY,
- a member of the hiring committee for an assistant professor at University Toulouse 3,
- an expert for the French Agence Nationale de la Recherche (ANR), Haut Conseil de l'Evaluation de la Recherche et de l'Enseignement Supérieur (HCERES), for the German DFG, the Dutch NWO, and the European Research Council (ERC).
- He was invited for a keynote talk at *Groupe de Travail Vérification* of *GDR IM* in Paris.

8.2. Teaching

The university employees of Mosel have significant teaching obligations. We indicate the graduate courses they have been teaching this year, as well as significant pedagogical responsibilities.

- Marie Duflot-Kremer taught a course on Introduction to Algorithmic Verification (first-year master level at Université de Lorraine). She and Stephan Merz also taught a course on Algorithmic Verification in the second year of master and for students of Erasmus Mundus Dependable Software Systems.
- Pascal Fontaine is head of the Master MIAGE (Business Informatics) at Université de Lorraine since September 2014.
- Dominique Méry gave courses in the Master program in Nancy on formal system engineering, modeling and verification of systems, theoretical computer science, development of software systems, distributed algorithms.
- Stephan Merz taught a course on formal specification using TLA$^+$ at the SPES_XT summer school on model-based development of embedded systems at the University of Twente (The Netherlands) in September.

8.3. Supervision

- PhD: Hernán Pablo Vanzetto, Proof Automation and Type Synthesis for Set Theory in the Context of TLA$^+$, Université de Lorraine. Supervised by Kaustuv Chaudhuri and Stephan Merz, defended on December 8, 2014.
- PhD in progress: Manamiary Andriamiarina, Refinement Techniques for Distributed Algorithms, since 10/2010, supervised by Dominique Méry;
- PhD in progress: Noran Azmy, On the Automation of Proofs in TLAPS, Saarland University. Supervised by Stephan Merz and Christoph Weidenbach, since 11/2012.
- PhD in progress: Haniel Barbosa, Refutational Completeness in Satisfiability Modulo Theories, Université de Lorraine and UFRN (Natal, Brazil). Supervised by David Déharbe, Pascal Fontaine, and Stephan Merz, since 12/2013.
- PhD in progress: Pablo Federico Dobal, Satisfiability Modulo Arithmetic Theories, Université de Lorraine and Saarland University. Supervised by Pascal Fontaine, Stephan Merz, and Thomas Sturm, since 09/2014.

8.4. Juries

Stephan Merz served as a reviewer for the PhD theses of Nadezhda Baklanova (Univ. Toulouse 3), Claire Dross (Univ. Paris Sud), and Giuliano Losa (EPFL Lausanne).

8.5. Popularization

Marie Duflot-Kremer took part in various popularization activities, with a public ranging from primary school kids (with unplugged activities concerning sorting, programming, error detection) to non-scientific staff of the Inria center. She is also a member of the steering committee preparing an itinerant exposition intended for explaining computer science to high-school students and took part in an event of the European Code Week in Paris.

Pascal Fontaine and Stephan Merz illustrated some subjects and techniques that underly formal verification of protocols and algorithms at events like "Fête de la Science". Using wooden puzzles and Sudoku sheets, they explained how real-life problems can be represented in logical form and then solved using automated tools based on formal logic.

9. Bibliography

Major publications in recent years

[1] JEAN-RAYMOND ABRIAL, DOMINIQUE CANSELL, AND DOMINIQUE MÉRY. Refinement and reachability in Event-B. In *ZB*, pages 222–241, 2005.

[2] THOMAS BOUTON, DIEGO CAMINHA B. DE OLIVEIRA, DAVID DÉHARBE, AND PASCAL FONTAINE. veriT: an open, trustable and efficient SMT-solver. In Renate Schmidt, editor, *Proc. Conference on Automated Deduction (CADE)*, volume 5663 of *Lecture Notes in Computer Science*, pages 151–156, Montreal, Canada, 2009. Springer.

[3] DOMINIQUE CANSELL AND DOMINIQUE MÉRY. The Event-B modelling method: Concepts and case studies. In Dines Bjørner and Martin C. Henson, editors, *Logics of Specification Languages*, Monographs in Theoretical Computer Science, pages 47–152. Springer, Berlin-Heidelberg, 2008.

[4] DENIS COUSINEAU, DAMIEN DOLIGEZ, LESLIE LAMPORT, STEPHAN MERZ, DANIEL RICKETTS, AND HERNÁN VANZETTO. TLA+ Proofs. In Dimitra Giannakopoulou and Dominique Méry, editors, *18th International Symposium On Formal Methods - FM 2012*, volume 7436 of *Lecture Notes in Computer Science*, pages 147–154, Paris, France, 2012. Springer.

[5] DAVID DÉHARBE, PASCAL FONTAINE, STEPHAN MERZ, AND BRUNO WOLTZENLOGEL PALEO. Exploiting symmetry in SMT problems. In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *23rd Intl. Conf. Automated Deduction (CADE 2011)*, volume 6803 of *LNCS*, pages 222–236, Wroclaw, Poland, 2011. Springer.

[6] FRED KRÖGER AND STEPHAN MERZ. *Temporal Logic and State Systems*. Texts in Theoretical Computer Science. Springer, 2008.

[7] STEPHAN MERZ. The specification language TLA$^+$. In Dines Bjørner and Martin C. Henson, editors, *Logics of Specification Languages*, Monographs in Theoretical Computer Science, pages 401–451. Springer, Berlin-Heidelberg, 2008.

Year publications

Doctoral Dissertations and Habilitation Theses

[8] H. VANZETTO, *Proof automation and type synthesis for set theory in the context of TLA+*, Theses, Université de Lorraine, December 2014, https://hal.inria.fr/tel-01096518.

Articles in International Peer-Reviewed Journal

[9] M. B. ANDRIAMIARINA, D. MÉRY, N. K. SINGH, "Revisiting Snapshot Algorithms by Refinement-based Techniques (Extended Version)", *Computer Science and Information Systems 11*, 1, January 2014, p. 251–270, https://hal.inria.fr/hal-00924525.

[10] M. ARAPINIS, M. DUFLOT, "Bounding messages for free in security protocols – extension to various security properties", *Information and Computation*, 2014, p. 34, https://hal.inria.fr/hal-01083657.

[11] J. CHEN, M. DUFLOT, S. MERZ, "Analyzing Conflict Freedom For Multi-threaded Programs With Time Annotations", *Electronic Communications of the EASST 70*, December 2014, p. 14, https://hal.inria.fr/hal-01087871.

[12] D. DÉHARBE, P. FONTAINE, L. VOISIN, Y. GUYOT, " Integrating SMT solvers in Rodin", *Science of Computer Programming 94*, November 2014, p. 14, https://hal.inria.fr/hal-01094999.

[13] G. LÜTTGEN, S. MERZ, "Editorial: Special Issue of Automated Verification of Critical Systems", *Science of Computer Programming 96*, 3, December 2014, p. 277–278, https://hal.inria.fr/hal-01084232.

[14] D. MÉRY, B. SCHÄTZ, A. WASSYNG, "The Pacemaker Challenge: Developing Certifiable Medical Devices (Dagstuhl Seminar 14062)", *Dagstuhl Reports 4*, 2, 2014, p. 17–37, https://hal.inria.fr/hal-01097629.

Invited Conferences

[15] C. BARRETT, L. DE MOURA, P. FONTAINE, " Proofs in satisfiability modulo theories", *in : APPA (All about Proofs, Proofs for All)*, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01095009.

[16] D. MÉRY, "Playing with State-Based Models for Designing Better Algorithms", *in : Model and Data Engineering - 4th International Conference, MEDI 2014*, Y. A. Ameur, L. Bellatreche, G. A. Papadopoulos (editors), *Lecture Notes in Computer Science*, *8748*, Springer, p. 1–3, Larnaca, Greece, September 2014, https://hal.inria.fr/hal-01097625.

International Peer-Reviewed Conference/Proceedings

[17] M. B. ANDRIAMIARINA, D. MÉRY, N. K. SINGH, "Analysis of Self-* and P2P Systems using Refinement", *in : ABZ 2014 - 4th International ABZ 2014 Conference ASM, Alloy, B, TLA, VDM, Z*, Y. A. Ameur, K.-D. Schewe (editors), *LNCS*, *8477*, Springer, p. 117–123, Toulouse, France, June 2014, https://hal.inria.fr/hal-01018125.

[18] Y. AÏT AMEUR, J. P. GIBSON, D. MÉRY, "On Implicit and Explicit Semantics: Integration Issues in Proof-Based Development of Systems", *in : Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications - 6th International Symposium,*, T. Margaria, B. Steffen (editors), *Lectures Notes in Computer Science*, *8803*, Springer, p. 604–618, Corfu, Greece, October 2014, https://hal.inria.fr/hal-01097624.

[19] P. CHOCRON, P. FONTAINE, C. RINGEISSEN, "A Gentle Non-Disjoint Combination of Satisfiability Procedures", *in : Automated Reasoning - 7th International Joint Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic*, *Lecture Notes in Computer Science*, *8562*, Springer, p. 122–136, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087162.

[20] P. CHOCRON, P. FONTAINE, C. RINGEISSEN, "Satisfiability Modulo Non-Disjoint Combinations of Theories Connected via Bridging Functions", *in : Workshop on Automated Deduction: Decidability, Complexity, Tractability, ADDCT 2014. Held as Part of the Vienna Summer of Logic, affiliated with IJCAR 2014 and RTA 2014*, Silvio Ghilardi, Ulrike Sattler, Viorica Sofronie-Stokkermans, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01087218.

[21] D. DOLIGEZ, J. KRIENER, L. LAMPORT, T. LIBAL, S. MERZ, "Coalescing: Syntactic Abstraction for Reasoning in First-Order Modal Logics", *in : ARQNL 2014 - Automated Reasoning in Quantified Non-Classical Logics*, Vienna, Austria, July 2014, https://hal.inria.fr/hal-01063512.

[22] D. FASS, "Reclaiming human machine nature", *in : HCI International 2014*, V. G. Duffy (editor), *8529*, Springer, p. 588–589, Heraklion, Greece, June 2014, https://hal.archives-ouvertes.fr/hal-01069481.

[23] D. MÉRY, N. K. SINGH, "Formal Evaluation of Landing Gear System", *in : SoICT 2014 Fifth Symposium on Information and Communication Technology,*, N. H. Son, Y. Deville, M. Bui (editors), ACM, Hanoi, Vietnam, December 2014, https://hal.inria.fr/hal-01097645.

[24] D. MÉRY, N. K. SINGH, "Modeling an Aircraft Landing System in Event-B", *in : ABZ 2014 Case Study Track*, F. Boniol (editor), *CCIS*, *433*, Springer, p. 154–159, Toulouse, France, June 2014, https://hal.inria.fr/hal-00985010.

[25] D. MÉRY, N. K. SINGH, "The Semantics of Refinement Chart", *in : HCI International*, V. G. Duffy (editor), *Lecture Notes in Computer Science*, *8529*, Springer, p. 415–426, Heraklion, Greece, June 2014, https://hal.inria.fr/hal-00995176.

[26] S. MERZ, H. VANZETTO, "Refinement Types for TLA+", *in : NASA Formal Methods - 6th International Symposium*, J. M. Badger, K. Y. Rozier (editors), *LNCS*, *8430*, Springer, p. 143–157, Houston, Texas, United States, 2014, https://hal.inria.fr/hal-01063516.

Books or Proceedings Editing

[27] G. CIOBANU, D. MÉRY (editors), *Theoretical Aspects of Computing – ICTAC 2014*, *Lecture Notes in Computer Science*, *8687*, Gabriel Ciobanu, Bucharest, Romania, Springer, September 2014, https://hal.inria.fr/hal-01097627.

[28] C. DUBOIS, D. GIANNAKOPOULOU, D. MÉRY (editors), *Proceedings 1st Workshop on Formal Integrated Development Environment*, *Electronic Proceedings in Theoretical Computer Science*, *149*, France, EPTCS, April 2014, 105p., https://hal.inria.fr/hal-00987531.

[29] G. LÜTTGEN, S. MERZ (editors), *Science of Computer Programming Special Issue: Automated Verification of Critical Systems*, *Science of Computer Programming*, *96*, 3, Elsevier, December 2014, https://hal.inria.fr/hal-01084228.

[30] S. MERZ, J. PANG (editors), *Formal Methods and Software Engineering – 16th International Conference on Formal Engineering Methods (ICFEM 2014)*, *Lecture Notes in Computer Science*, *8829*, Springer, November 2014, 460p., https://hal.inria.fr/hal-01098238.

Research Reports

[31] M. B. ANDRIAMIARINA, D. MÉRY, N. K. SINGH, "Analysis of Self-* and P2P Systems using Refinement (Full Report)", *Research report*, 2014, https://hal.inria.fr/hal-01018162.

[32] P. CHOCRON, P. FONTAINE, C. RINGEISSEN, "A Gentle Non-Disjoint Combination of Satisfiability Procedures (Extended Version)", *Research Report number RR-8529*, April 2014, https://hal.inria.fr/hal-00985135.

[33] D. ROEGEL, "A reconstruction of Arnaudeau's table of triangular numbers (ca. 1896)", *Research report*, LORIA - Université de Lorraine, December 2014, https://hal.inria.fr/hal-01098344.

[34] D. ROEGEL, "Easter-based walks on a sphere", *Research report*, 2014, https://hal.inria.fr/hal-01009458.

[35] D. ROEGEL, "Easter bracelets for 5700000 years", *Research report*, 2014, https://hal.inria.fr/hal-01009457.

[36] D. ROEGEL, "The strange beauty of the twilight flower", *Research report*, 2014, https://hal.inria.fr/hal-00978237.

[37] D. ROEGEL, "The "Villarceau circles" in Uhlberger's staircase (ca. 1580)", *Research report*, 2014, https://hal.inria.fr/hal-00941465.

Other Publications

[38] D. ROEGEL, "The (re)discovery of an early specialized mechanical calculating machine (ca. 1850)", December 2014, https://hal.inria.fr/hal-01096153.

[39] D. ROEGEL, "The (re)discovery of one of the oldest modular digital mechanical counters (1844)", December 2014, https://hal.inria.fr/hal-01096151.

[40] D. ROEGEL, "The (re)discovery of some of the oldest key-driven adding machines (1844)", December 2014, https://hal.inria.fr/hal-01096468.

References in notes

[41] JEAN-RAYMOND ABRIAL. *The B-Book: Assigning Programs to Meanings*. Cambridge University Press, 1996.

[42] JEAN-RAYMOND ABRIAL. *Modeling in Event-B: System and Software Engineering*. Cambridge University Press, 2010.

[43] CLARK BARRETT, ROBERTO SEBASTIANI, SANJIT A. SESHIA, AND CESARE TINELLI. Satisfiability modulo theories. In Armin Biere, Marijn J. H. Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, chapter 26, pages 825–885. IOS Press, February 2009.

[44] T. BØGHOLM, H. KRAGH-HANSEN, P. OLSEN, B. THOMSEN, AND K. G. LARSEN. Model-based schedulability analysis of safety critical hard real-time Java programs. In G. Bollella and C. D. Locke, editors, *Workshop on Java Technologies for Real-time and Embedded Systems (JTRES)*, pages 106–114. ACM, 2008.

[45] W.-P. de Roever, H. Langmaack, and A. Pnueli, editors. *Compositionality: The Significant Difference*, volume 1536 of *Lecture Notes in Computer Science*. Springer-Verlag, 1998.

[46] LESLIE LAMPORT. *Specifying Systems*. Addison-Wesley, Boston, Mass., 2002.

[47] STEPHAN MERZ AND HERNÁN VANZETTO. Harnessing SMT Solvers for TLA+ Proofs. In Gerald Lüttgen and Stephan Merz, editors, *12th International Workshop on Automated Verification of Critical Systems (AVoCS 2012)*, volume 53 of *ECEASST*, Bamberg, Germany, December 2012. EASST.