INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Mosel

Proof-oriented development of computer-based systems

Nancy - Grand Est

THEME SYM

Table of contents

1. Team

Head of project team

Dominique Méry [Professor, University Henri Poincaré Nancy 1, HdR]

Administrative assistant

Josiane Reffort [Administrative assistant, University Henri Poincaré Nancy 1, until September 2007]
Caroline Suter [Administrative assistant, since October 2007]

Permanent researcher

Stephan Merz [Research Director, INRIA, HdR]

Faculty members

Dominique Cansell [Assistant Professor, University of Metz, on secondment at INRIA since September 2007, HdR]
Pascal Fontaine [Assistant Professor, University Nancy 2]
Jacques Jaray [Professor, Institut National Polytechnique de Lorraine and École des Mines de Nancy, HdR]
Leonor Prensa Nieto [Assistant Professor, Institut National Polytechnique de Lorraine and École Nationale Supérieure d'Electricité et de Mécanique, on sabbatical leave since September 2007]
Denis Roegel [Assistant Professor, University Nancy 2]

Junior technical staff

Thomas Bouton [since September 1, 2007]

Ph. D. Students

Nazim Benaïssa [University Henri Poincaré Nancy 1, supported by a grant from the government of Algeria and the Lorraine Region, defense planned for 2009]
Diego Caminha Barbosa de Oliveira [University Nancy 2, supported by CORDI-S contract, since December 1, 2007, defense planned for 2010]
Loïc Fejoz [University Henri Poincaré Nancy 1, supported by Microsoft ERO grant, defense planned for 2008]
Houda Fekih [joint supervision, University of Tunis and Institut National Polytechnique de Lorraine, defense planned for 2008]
Eun Young Kang [University Henri Poincaré Nancy 1, defense on November 8, 2007]
Olfa Mosbahi [joint supervision, University of Tunis and Institut National Polytechnique de Lorraine, research and teaching assistantship at INPL, defense planned for 2008]
Joris Rehm [University Henri Poincaré Nancy 1, grant of French ministery of Higher Education and Research, defense planned for 2009]
Mouna Saad [joint supervision, University of Tunis and Institut National Polytechnique de Lorraine, since September 2007, defense planned for 2010]

Internships

Damián Barsotti [Univ. Córdoba, Argentina, April – June, 2007]
Diego Caminha Barbosa de Oliveira [Federal University of Rio Grande do Norte, Natal, Brazil, April – September, 2007]
Sebti Mouelhi [Master Nancy, February – August, 2007]
Mauricio Notti [Univ. Rosario, Argentina, May – July, 2007]

External collaborators

Dines Bjørner [Technical University of Denmark, Copenhagen, invited professor, October – December, 2007]
Paul Gibson [Institut National des Télécommunications Evry]

2. Overall Objectives

2.1. Introduction

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 theoretical underpinnings of 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, 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.

Notation and tools. We are studying notations that aid system engineers for representing their concepts, and that integrate different methods and tools of system design. Where necessary, 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.

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 and academia, including neighboring disciplines such as circuit design. We also use our methods in the courses we teach to evaluate their applicability.

The cooperation with research groups within France and elsewhere helps us to clarify and promote our ideas. We are actively participating in the SSS (*Sûreté et Sécurité des Systèmes*) theme of research within the regional competence center on digital modeling of computer-based systems.

2.2. Highlights of the year

A very interesting collaboration started in 2007 within the project RIMEL for the proof-based development of distributed algorithms (see section 8.1). We have obtained new insights into existing algorithms, such as Mazurkiewicz's algorithm, and plan to address self-healing systems.

3. Scientific Foundations

3.1. Foundations and Methodology

Keywords: *abstraction*, *composition*, *concurrency*, *distributed systems*, *formal methods*, *reactive systems*, *refinement*.

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 system *development*, as opposed to the verification of an existing system a posteriori. This view is formally reflected by the notion of *refinement*, which ensures that descriptions produced in later stages of system design preserve earlier, more abstract descriptions; in particular, all properties proven 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 automatisation in our verification efforts. Crucially, errors can be detected very early, when they are relatively cheap to correct. The formalisms that we are most familiar with are the B method due to Abrial [41], [40] and the Temporal Logic of Actions and the TLA$^+$ language introduced by Lamport [43]. Members of MOSEL have been invited to write tutorials on these methods [3], [6].

The second cornerstone of system development is composition and decomposition [39]. In effect, 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-based 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 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

Keywords: *B*, *TLA*, *interface*, *model checking*, *proof obligations*, *theorem proving*, *tool integration*.

The development of provably correct systems [2] relies on languages with a precise, mathematically defined semantics, in which system specifications are written and proof obligations are stated. For all but toy systems, formal development methods generate a huge number of proof obligations, and highly automated tools become essential to successfully apply the methods. Whereas automated deduction has made substantial progress, each tool typically covers a restricted domain, and the combination of different tools is an active area of research.

In this spirit, we introduced the format of *predicate diagrams* [4], [5] to represent Boolean abstractions of reactive systems in the form of finite-state diagrams, with annotations that express fairness and liveness properties. Predicate diagrams form an interface between theorem proving and model checking techniques: the former are useful for showing the correctness of the abstraction, whereas the latter can establish temporal properties from the finite-state diagram representation. The DIXIT tool (described in section 5.2) implements an editor for predicate diagrams, generates proof obligations to show the correctness of abstractions, and invokes external model checkers to verify properties of abstractions expressed in temporal logic. Members of MOSEL have also contributed intensively to the development of the SMT solver haRVey (described in section 5.1) and to its integration with interactive proof assistants (see section 6.7).

We believe that beyond the sheer capacity of provers for carrying out deductions, adequate interfaces are an important element in order to promote their actual use in system development. Dominique Cansell has developed an interface for the interactive prover of Atelier B, the primary support tool for the B method, freely available for academic users within the B4Free tool. Its development is based on a thorough study of interactive provers are used for system verification.

3.3. Applications

Keywords: *access control*, *digital TV*, *embedded systems*, *hardware-software codesign*, *security*, *service interaction*, *services*, *telecommunications*.

A substantial part of our research is driven by work on concrete applications and case studies, as well as by courses that we teach. Several applications currently studied by MOSEL concern hardware-software codesign for embedded systems. Within these industrial projects, we have applied the B method to produce a series of models, starting from standard requirement documents as inputs for the abstract models. As a result of several refinement steps, with accompanying proofs, we were obtained models at a level of granularity that allowed us to mechanically synthesize hardware descriptions.

Another interesting field of study is the application of formal description techniques to problems of information security. We have worked on extending logics and formalisms that we are familiar with for the specification of access control requirements (see section 6.5), and we have studied problems that arise in electronic voting (see section 6.10).

4. Application Domains

4.1. Application Domains

Keywords: *critical systems*, *embedded systems*, *networks*, *protocols*, *telecommunications*.

Our work mainly targets critical systems whose malfunctioning may endanger the health or life of persons, their privacy and security, or that may lead to serious financial consequences. We enjoy working on concrete examples that are developed in the context of industrial or cooperative projects, including telecommunications, embedded systems, networks and their protocols, problems of information security, and mobile systems.

5. Software

5.1. The haRVey reasoner

Keywords: *SMT prover*, *arithmetic*, *combination of decision procedures*, *congruence closure*, *difference logic*, *proof trace*.

Participants: Thomas Bouton, Diego Caminha, Pascal Fontaine [correspondant], Stephan Merz.

haRVey is an SMT (Satisfiability Modulo Theories) prover. It was initiated in cooperation with Silvio Ranise and Christophe Ringeissen of the CASSIS project team of INRIA Lorraine. It is developped in cooperation with David Déharbe from the Federal University of Rio Grande do Norte in Natal, Brasil. haRVey can handle large quantifier-free formulas containing uninterpreted predicates and functions, and some arithmetics. It also has some support for user-defined theories, quantifiers, and lambda-expressions. This allows users to easily express properties about "higher-order" concepts involving sets, relations, etc. The prover can produce an explicit proof trace when it is used as a decision procedure for quantifier-free formulas with uninterpreted symbols. This feature has been used to integrate it with the proof assistant Isabelle (see section 6.7).

Since 2006, the tool has been available at http://harvey.loria.fr. The main efforts in 2007 have gone into preparing a major new release of the tool, which will provide a better integration of the different available features, and a better support for arithmetic on rationals and integers. The beta version is running, and has already been presentedThe public release is planned for 2008, after extensive testing, code improvements, and polishing of the interface.

A regression test platform has been implemented during the second half of 2007. This platform is now in production, and will greatly ease some of the tests following code changes, thus permitting quicker development in the future.

Some implementation effort was also directed to improve the capabilities of the tool to handle arithmetic. In particular, a highly efficient decision procedure for difference logic has been implemented and is being integrated with the overall tool.

Future research and implementation efforts will be directed to furthermore extend the accepted language, increase the efficiency, and provide an optimal interface (including providing explicit proof traces) for the prover to be used within larger verification tools. We target applications where validation of formulas is crucial, such as validation of TLA$^+$ and B specifications.

5.2. The DIXIT toolkit

Keywords: *model checking*, *predicate abstraction*.

Participants: Loïc Fejoz, Dominique Méry, Stephan Merz [correspondant].

The DIXIT toolkit provides support for the verification of systems using Boolean abstractions in the form of predicate diagrams. It is organized around a visual editor that allows a user to draw a predicate diagram and enter node and edge annotations. Properties expressed in linear-time temporal logic can be verified from the interface by calling the Spin or LWAASpin model checkers, counter-examples are visualized in the editor, and proof obligations that ensure the correctness of the abstraction can be generated. Finally, the toolkit can verify that a predicate diagram refines a more abstract one, ensuring the preservation of temporal logic properties. One of the strong points of DIXIT is the capability for verifying liveness properties on the basis of predicate abstractions. DIXIT is registered with APP and is freely available for download.

6. New Results

6.1. Incremental development of distributed algorithms

Keywords: *distributed algorithms*, *event B*, *refinement*.

Participants: Dominique Cansell, Dominique Méry.

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 works help to formalize pre-existing algorithms as well as to develop new algorithms.

Dominique Cansell and Dominique Méry have reconsidered the leader election algorithm of the Firewire protocol to obtain a new algorithm: it turns out that acknowlegments and confirmations are not necessary. The protocol works without these redundant messages. This work was published in [15]. Works on B patterns were published in [26], [17], [25], [34], [14].

6.2. Modelling of electronic systems

Keywords: *B method*, *BHDL*, *hardware description*, *refinement*, *theorem proving*.

Participants: Dominique Cansell, Yann Zimmermann.

As the complexity of electronics systems continues to increase and their reliability requirements become more and more important, the challenge is to master complexity in development while ensuring the correctness of systems. Test-based methods no longer provide sufficient coverage for realistic systems, and proof-based methods are attracting industrial attention because they are not limited by the complexity of systems. In his PhD thesis (defended in November 2006), Yann Zimmermann suggested using the B method and its concept of refinement to simplify the process of modelling and proving. At each refinement step, proof obligations are automatically generated by tools to ensure that the concrete model is correct with respect to the abstract model. This method ensures that the final implementation is correct with respect to the initial abstract specification. This work has been published at AFADL'2007 [36].

6.3. Time constraint patterns for event B development

Keywords: *distributed systems*, *event B*, *pattern*, *refinement*.

Participants: Dominique Cansell, Dominique Méry, Joris Rehm.

Real-time constraints are frequent requirements for distributed applications. In order to express such constraints in (mathematical) models, we intend to integrate time constraints in the modelling process based on event B models and refinement. The starting point of our work is the development in event B of the IEEE 1394 leader election protocol. From the documents of the standard, we derive temporal requirements to solve the contention problem and we propose a method for introducing time constraints using a pattern. The pattern captures time constraints in a generic event B development and it is applied to the IEEE 1394 case study. Joris Rehm proposed to introduce time constraints (propagation, sleeping time) in the B development of the IEEE 1394 protocol to solve the contention problem. To attend this goal he has defined a pattern in event B to introduce time constraint. A first paper [26] describing the introduction of time constraint using refinement was published at B 2007 and a second one [34], presenting a proved development of the IEEE 1394 Root Contention Protocol until a model with real-time properties, at the ISOLA'2007 workshop.

6.4. Modeling and designing systems with temporal requirements

Keywords: *control systems*, *real time*, *temporal logics*.

Participants: Jacques Jaray, Olfa Mosbahi, Mouna Saad.

The doctoral thesis of Olfa Mosbahi is co-supervised by Jacques Jaray and Samir Ben Ahmed from the Institut Supérieur d'Informatique in Tunis. It concerns the joint use of the B and TLA$^+$ methods for modeling and designing systems with temporal requirements. She has proposed to use composition techniques in order to combine models of control systems and is also looking at refinement of real-time systems and the use of design patterns to capture and implement time features. Her work has been published at three conferences [32], [31], [33].

6.5. Formalization of Access Control Specifications

Keywords: *B method*, *Event B*, *access control*, *refinement*.

Participants: Nazim Benaïssa, Dominique Cansell, Dominique Méry, Stephan Merz.

The project ACI DESIRS is completed since the end of 2006 and we have produced further researches. We [23] address the proof-based development of (system) models satisfying a security policy. The security policy is expressed in a model called OrBAC, which allows one to state permissions and prohibitions on actions and activities and belongs to the family of role-based access control formalisms. The main question is to validate the link between the security policy expressed in OrBAC and the resulting system; a first abstract B model is derived from the OrBAC specification of the security policy and then the model is refined to introduce properties that can be expressed in OrBAC. The refinement guarantees that the resulting B (system) model satisfies the security policy. We present a generic development of a system with respect to a security policy and it can be instantiated later for a given security policy. We [19] consider the extension of fair event system specifications by concepts of access control (prohibitions, user rights, and obligations). We give proof rules for verifying that an access control policy is correctly implemented in a system, and consider preservation of access control by refinement of event systems. Prohibitions and obligations are expressed as properties of traces and are preserved by standard refinement notions of event systems. Preservation of user rights is not guaranteed by construction; we propose to combine implementation-level user rights and obligations to implement high-level user rights.

6.6. Work on TLA+ and +CAL

Keywords: *TLA*, *distributed algorithms*, *model checking*, *proof*.

Participants: Stephan Merz, Sebti Mouelhi, Mauricio Notti, Martin Quinson [of project team Algorille].

Within a joint project between INRIA and Microsoft Research (see section 8.3) that aims at developing a verification environment for TLA$^+$ and the Cooperative Research Action VeriTLA$^+$ (see section 8.4), we have contributed to the formal definition of a declarative and hierarchical proof language for TLA$^+$ and its operational and logical semantics.

During his internship at LORIA, Mauricio Notti implemented a first prototype of an interpreter for this language in OCaml. He also experimented a number of rewrite rules intended for matching formulas modulo certain syntactic identities, proved their termination, and analyzed their complexity.

We have also extended the +CAL language [44] defined by Lamport in order to simplify the modeling of concurrent algorithms. The extension is intended for describing and verifying models of distributed algorithms, whereas the original language is geared towards shared-memory concurrent programming. In his master's thesis, Sebti Mouelhi proposes several extensions to the existing +CAL language and compiler [38]. In particular, an arbitrary block can be marked as being executed atomically, several assignments to the same variable are allowed within a single group of statements executed atomically, the handling of local variables by the compiler is improved, and pre-defined macros for message passing are offered, inspired by the GRAS API of SimGrid. The validation of the new compiler over a number of examples has convinced us of the interest of the approach, but also of the necessity of a complete redesign of the language and the compiler, which is planned as future work.

6.7. Cooperation of reasoners

Keywords: *SMT solvers*, *decision procedures*, *proof assistants*, *proof reconstruction*, *theorem proving*.

Participants: Pascal Fontaine, Stephan Merz, Leonor Prensa Nieto.

The study of the foundations of combining decision procedures, the limits of doing so, and the necessary techniques constitutes the theoretical background for the development of the haRVey prover (see section 5.1). We proved in 2007 that any decidable language (subject to a minor requirement on cardinalities) can be extended with predicates described by a Bernays-Schönfinkel-Ramsey theory (BSR). A formula belongs to the BSR fragment if it is a conjunction of universal, function-free formulas.

As a consequence of this theoretical result, it is possible to augment decidable quantifier-free languages with set-theoretical constructions, including relations and orders. This will significantly extend the expressivity of SMT solvers (and notably, haRVey).

A subresult is interesting in itself: we proved that it is possible to know exactly which cardinalities are accepted by a satisfiable BSR theory. In particular, we can decide if a BSR theory has an infinite model or not. These results have been published in [29].

Automatic provers such as SMT solvers can be used successfully in combination with interactive proof assistants. In such a scenario, it is interesting to obtain a sufficient degree of confidence in the soundness of the combination. In previous work, we have designed such techniques, based on the certification within the proof assistant of a proof trace generated by the automatic prover. The cooperation framework has been extended to handle quantified formulae and certain set-theoretic operators. This extension is mainly motivated by the fact that languages such as TLA$^+$ or B rely heavily on set theory. This work has been the subject of a publication in 2007 at the Isabelle Workshop [30].

6.8. Verification of clock synchronization in the FlexRay protocol

Keywords: *FlexRay*, *clock synchronization*, *theorem proving*, *verification*.

Participants: Damián Barsotti, Leonor Prensa Nieto.

As a substantial case study for validating our work on the combination of reasoners (see section 6.7), we study the verification of parts of the FlexRay protocol. FlexRay is a communication protocol intended for advanced automotive control applications, including "X-by-wire" systems. The correctness of the clock synchronization algorithm is the most basic and most important property of the protocol.

In previous work we have formalized in Isabelle/HOL a framework for clock synchronization developed by Schneider and have mechanically verified the correctness of an abstract model of the Lundelius-Lynch midpoint algorithm, on which FlexRay is based. This work has been published in a special issue of the journal *Formal Aspects of Computing* [11]; the underlying theories are available at the Archive of Formal Proofs.

During his internship, Damián Barsotti has studied whether Schneider's abstract model can be adapted to the verification of FlexRay's clock synchronization algorithm. The main complications are that FlexRay considers two levels of time units (microticks and macroticks) whose relation should be kept approximately constant. Secondly, FlexRay adjusts local clocks by adding (microtick) offsets and by adjusting the macrotick length. The standard refers to an unpublished report on the correctness of the clock synchronization algorithm, which we obtained from the authors. We have so far been able to formally verify its correctness in the absence of faults, and we intend to complete the formalization by adding appropriate fault hypotheses.

6.9. Type Systems for Security

Keywords: *non-interference*, *security*, *theorem prover*, *type systems*.

Participants: Gilles Barthe [of INRIA project team Everest], Leonor Prensa Nieto.

Information flow type systems provide an elegant means to enforce confidentiality of programs. In joint work with Gilles Barthe from INRIA-Sophia Antipolis, we have specified, using the proof assistant Isabelle/HOL, an information flow type system for a concurrent language featuring primitives for scheduling. We have shown that well-typed programs are non-interfering for a possibilistic notion of non-interference. The development, which constitutes to our best knowledge the first machine-checked account of non-interference for a concurrent language, takes advantage of the proof assistant's facilities to structure the proofs about different views of the programming language and to identify the relationships among them and the type system. Our language and type system generalize previous work of Boudol and Castellani [42], in particular by including arrays and lifting several convenient but unnecessary conditions in the syntax and type system.

This work has been published in the Journal of Computing Security [12].

6.10. Modeling and Verification of E-voting systems

Keywords: *electronic vote*, *formal methods*, *requirements*.

Participants: Dominique Cansell, Paul Gibson, Dominique Méry.

Electronic voting systems have been subject to numerous severe flaws, and we believe that they constitute a prime example for the application of formal methods. In particular, the requirements of these systems and their interfaces need to be rigorously defined. As a first step in this direction, we have developed formal requirement models for a secure e-voting interface using the B method. A paper has been published at the FMIS workshop [13].

We have also proposed the application of formal methods (event-B) for guaranteeing, through construction, the correctness of a vote store with respect to the requirement for *tamper-evident* storage. We illustrate the utility of our refinement-based approach by verifying – through the application of a reusable formal design pattern – a store design that uses a specific PROM technology and applies a specific encoding mechanism. This work [24] has been presented at SEFM'2007.

6.11. Validating and Animating Higher-Order Recursive Functions in B

Keywords: *B method*, *animation*, *higher-order functions*.

Participant: Dominique Cansell.

ProB is an animation and model checking tool for the B Method, which can deal with many interesting specifications. Some specifications, however, contain complicated functions which cannot be represented explicitly by a tool. We present a scheme to encode higher-order recursive functions in B, and we establish soundness of this scheme. We describe a symbolic representation for such functions. This representation enables ProB to successfully animate and model check a new class of relevant specifications, where animation is especially important due to the involved nature of the specification. This work was done with Michael Leuschel and Michael Butler and was published in [18]

6.12. Modelling and Proof Analysis of Interrupt Driven Scheduling

Keywords: *event B*, *interrupt*, *scheduling*.
Participant: Dominique Cansell.

In this work we have described a distributed Event B model of interrupt driven scheduling. We first consider a model with two executing tasks, presented with the aid of state machine diagrams. We then present a faulty variant of this model which, under particular event timings, may "drop" an interrupt. We show how the failure to discharge a particular proof obligation leads us to a conceptual error in this model. Finally we generalize the correct model to n tasks, leading to a reduction in proof effort. This work was done with Bill Stoddart and Frank Zeyda and was published at B 2007 [35].

6.13. Pattern-Based Development for Structured Programs

Keywords: *event B*, *proof pattern*, *structured programming*.
Participants: Dominique Cansell, Dominique Méry.

The development of structured programs is carried out either using bottom-up techniques, or top-down techniques; we show how refinement and proof can be used to help in the top-down development of structured imperative programs. When a problem is stated, the incremental proof-based methodology of event B starts by stating a very abstract model and further refinements lead to finer-grained event-based models which are used to build an algorithm. In this paper, the main idea is to consider each procedure call as an abstract event of a model corresponding to the development of the procedure; generally, a procedure is specified by a pre/post specification and then the refinement process can lead to a set of events, which are then combined to obtain the body of the procedure. It means that the abstraction corresponds to the procedure call and the body is derived by the refinement process. The refinement process may also use recursive procedures and it supports the top-down refinement. This work [25] was presented at CSR'2007.

6.14. Provably correct lock-free data structures

Keywords: *automatic proof*, *linearizability*, *lock-free algorithm*, *verification*.
Participants: Loïc Fejoz, Stephan Merz.

The development of multi-threaded programs is no longer restricted to operating system experts and specialised application areas, but is entering mainstream programming. A central problem is to ensure that different threads can access shared data structures without interference. The traditional solutions are based on locks, which can be either coarse-grained (applying to the entire data structure) or fine-grained (applying to individual elements of the data structure). Both cases have severe drawbacks: coarse-grained locks limit the possible degree of parallelism, while fine-grained locks are hard to control and prone to deadlocks. Several mechanisms of concurrent programming without locks have been proposed in the literature. In this project, funded by a Microsoft ERO PhD grant and carried out in cooperation with Tim Harris from Microsoft Research Cambridge, we investigate verification techniques for lock-free data structures. A dedicated program transformation technique has been elaborated and formalized in Isabelle/HOL. It results in proof obligations that are tailored to this class of algorithms and ensures that concurrent accesses are linearizable. In particular, a user of a lock-free data structure can reason as if all accesses by the different processes occurred atomically, in some unpredictable order. A toy example has been automatically verified with the SPASS prover backend. We intend to validate our technique over more complex case studies, while preserving a high degree of automation. A preliminary publication appeared in AFADL 2007 [28].

6.15. Abstraction-based verification for real-time systems

Keywords: *abstraction*, *real-time systems*, *refinement*, *timed automaton*.

Participants: Eun-Young Kang, Stephan Merz.

We propose an extension of the format of predicate diagrams, initially defined for discrete systems, for the verification of real-time systems. This line of work combines predicate abstraction, theorem proving, and model checking, and their application in a methodology called IAR (Iterative Abstract-Refinement Algorithm), where predicates for the abstraction are discovered iteratively. In 2007, the approach has been generalized to encompass the verification of parameterized systems. We have successfully used SMT solvers to discharge proof obligations generated by this approach for a number of familiar case studies, resulting in a very high degree of automation.

This work has been published in a special issue of the journal *Formal Aspects of Computing* [16]. Eun-Young Kang successfully defended her PhD thesis in November 2007.

6.16. Computer graphics and typesetting

Keywords: *Metapost*, *descriptive geometry*, *graphics*.

Participant: Denis Roegel.

Denis Roegel has continued to develop extensions to METAPOST addressing various abstract representations of objects. He has in particular been studying the correct representation of spheres, with their great circles and parallels, after having observed that almost all such depictions in the literature were contradictory. An article was published summarizing these results [22].

Another very important application of METAPOST lies in descriptive geometry. The representation of objects in descriptive geometry is a good example where a drawing shows several points of view, and these points of view have to respect a number of geometrical relationships. METAPOST is very well suited to that task, and two case studies have been explored: in the first, a figure representing a complex gear arrangement was reproduced from a 19th century book by Théodore Olivier [20]; in the second, descriptive geometry was used to provide a survey of classical sundials [37], and show their relationships.

Denis Roegel has also reviewed Bill Casselman's book on geometry and PostScript for the Notices of the AMS [21].

Finally, Denis Roegel has also co-authored the second edition of the book *LaTeX Graphics Companion* [8], which is the main book in the area of LaTeX graphics.

7. Contracts and Grants with Industry

7.1. Microsoft ERO PhD Grant

Participants: Loïc Fejoz, Stephan Merz.

The PhD thesis of Loïc Fejoz (see section 6.14) is supported by a Microsoft ERO PhD grant from January 2006 to December 2008. Our main contact at Microsoft Research is Tim Harris who develops algorithms for lock-free data structures that we intend to verify.

8. Other Grants and Activities

8.1. ANR SETIN RIMEL

Keywords: *B patterns*, *distributed algorithms*, *event B*, *refinement*.

Participants: Dominique Méry, Nazim Benaïssa, Dominique Cansell, Joris Rehm.

The project RIMEL, carried out in cooperation with the teams led by Mohamed Mosbah and by Yves Métivier at LABRI Bordeaux and with ClearSy Systems Engineering, focuses on the *refinement* of event-based models and aims to develop new features related to refinement, such as the reusability of refinement-based development, the composition and decomposition of models with respect to the refinement, the definition of proof-based design patterns, the integration of time constraints and probabilistic aspects, and the development of case studies, especially related to distributed systems. Probabilistic and/or timing aspects are of central importance for many distributed algorithms (such as the IEEE 1394 Tree Identification algorithm), and should therefore be integrated into the framework based on refinement. In this project, we are focusing on distributed algorithms and applications able to recover from a bad state, so-called self-healing systems. We also plan to apply the techniques to system engineering. Our proposed work is decomposed into several research directions:

1. Theory of refinement: integration of fairness constraints and liveness properties, probabilistic refinement and extensions of refinement scope.
2. Proof-based design patterns: a system engineering approach to justifying claims for security and trustworthiness.
3. Self-Healing Systems and Distributed Algorithms.
4. Tools and Dissemination.

The RIMEL project coordinates its research activities through case studies and applications, which give us concrete points of departure for our conceptual research.

8.2. QSL Operation InSpain

Keywords: *FlexRay clock synchronization protocol*, *combination of proof tools*.

Participants: Leonor Prensa Nieto, Damián Barsotti, Diego Caminha, Pascal Fontaine, Stephan Merz.

The operation InSpain was accepted in June 2006 by the council of the QSL (Qualité et Sûreté des Logiciels) theme at LORIA and expires at the end of 2007. Its main objectives are:

- the design and implementation of cooperative reasoning between the interactive theorem prover Isabelle and automatic provers, in particular SMT solvers such as haRVey (see section 6.7);
- the verification of fragments of the FlexRay protocol with the help of the combination of interactive and automatic proof tools mentioned above. More precisely, we aim at verifying the correction of the clock synchronization algorithm implemented in FlexRay (see also section 6.8).

Thanks to this operation we were able to invite Damián Barsotti for three months to work on the verification of FlexRay, and Diego Caminha for six months, to work on enhancing the haRVey prover with decision procedures for arithmetics.

8.3. Tools and Methodologies for Formal Specifications and for Proofs

Participant: Stephan Merz.

As part of the Joint Laboratory between INRIA and Microsoft Research, Stephan Merz participates in the project on Tools and Methodologies for Formal Specifications and for Proofs. The objective of the project is to develop an environment for modeling and verifying distributed algorithms in TLA$^+$ (see also section 6.6).

8.4. Project VeriTLA+

Participants: Stephan Merz, Pascal Fontaine, Dominique Méry, Sebti Mouelhi, Mauricio Notti.

Our team cooperates with the INRIA projects GALLIUM (Damien Doligez), OBASCO (Gilles Muller), and PHOENIX (Charles Consel), as well as with Julia Lawall of DIKU Copenhague and Leslie Lamport of Microsoft Research in the Cooperative Research Initiative VeriTLA$^+$ (2006/07). The objective of this project was to contribute to the development of a TLA$^+$ verification environment and, more specifically, to study the verification of domain-specific languages. Our work in 2007 concentrated on the proof manager for TLA$^+$ and on an extension of the language +CAL for modeling distributed algorithms (described in section 6.6).

8.5. Exchanges with Tunisia

Participants: Jacques Jaray, Houda Fekih, Dominique Méry, Stephan Merz, Olfa Mosbahi, Mouna Saad.

We have had a very fruitful cooperation with the team led by Professor Samir Ben Ahmed at the Institut Supérieur d'Informatique (ISI) in Tunis for several years. Jacques Jaray was invited several times to teach courses at the Master's level. The cooperation is currently supported by CMCU (*Comité Mixte de Coopération Universitaire*) through the project DEFI coordinated by Jeanine Souquières and Samir Ben Ahmed. Houda Fekih, Olfa Mosbahi, and Mouna Saad are preparing their Ph.D. thesis in joint supervision between the University of Tunis and the INPL at Nancy. Houda Fekih and Mouna Saad visited LORIA for a month each in 2007, whereas Olfa Mosbahi is currently employed by INPL as a research and teaching assistant.

9. Dissemination

9.1. Program committees and conference organisation

- Dominique Cansell was a member of the program committee of AFADL'2007 and B2007.
- Dominique Méry was a member of the program committees of ISOLA 2007 and IFM 2007; he has participated to the organisation of AFIS 2007 at Nancy in November 2007.
- Stephan Merz served on the program committees of the workshop Verify'07 at CADE 2007. He was co-editor of the proceedings of AVACS 2006 which appeared in ENTCS [9] and is co-editing a special issue of the journal Formal Aspects of Computing devoted to advances in system verification, to appear in 2008. Together with Nicolas Navet, he edited a book on the modeling and verification of real-time systems. He organized the meeting of IFIP Working Group 2.2, which took place on September 16-20, 2007, at LORIA. Together with Pascal Fontaine he organized a 2-day inter-regional workshop on rigorous system development and analysis at LORIA.

9.2. Tutorials, invited talks, panels

- Stephan Merz wrote a tutorial introduction on model checking techniques, which appears in a book on the modeling and verification of real-time systems, by Nicolas Navet and himself.
- Denis Roegel contributed a review of the book *Mathematical Illustrations* by Bill Casselman, for the Notices of the AMS [21].

9.3. Theses, habilitations, academic duties

- Dominique Cansell is a coordinator of the French MFDL (Méthodes Formelles pour le Développement Logiciel) working group of the GPL research group within CNRS (leader Yves Ledru).
- Pascal Fontaine is a member of an international working group designing the proof format for SMT solvers.
- Jacques Jaray is Vice President of Institut National Polytechnique de Lorraine.
- Dominique Méry
  - is a member of the IFIP Working Group 1.3 on *Foundations of System Specification*.

  - is the Head of the master programme in computer science for the three universities of Nancy.
  - is a member of the scientific council of the University Henri Poincaré Nancy 1.
  - is a member of the scientific council of the LORIA laboratory.
  - is an expert for the French Ministry of Education (DS9).
  - is an expert for the French Agence Nationale de la Recherche (ANR).
  - is director of international affairs at ESIAL Nancy.
  - is the president of the APCB association.
- Stephan Merz wrote a report on the PhD thesis of Rachele Fuzzati at Ecole Polytechnique Fédérale de Lausanne and was a member of the jury of the thesis of Mathieu Grenier at LORIA.
- Stephan Merz coordinates, together with Dominique Sauter, the research theme on Systems Safety and Security within the Research Cluster on Digital Modeling in Lorraine.
- Stephan Merz is the delegate for international relations at LORIA and INRIA Nancy. He was a member of the managing board of LORIA and INRIA Lorraine until August 2007 and is a member of the extended managing board of INRIA Nancy since September 2007. He represents INRIA in the supervisory board for the partnership with the Saarbrücken-Kaiserslautern area in Germany and acted as president of that board in 2007.
- Stephan Merz has been a member of the sub-group on initiative actions of the Conseil d'orientation scientifique et technologique (COST) of INRIA until November 2007.
- Stephan Merz is an elected member of the evaluation committee of INRIA.
- Stephan Merz is a member of the IFIP Working Group 2.2 *Formal Description of Programming Concepts*.
- Stephan Merz is an expert for the French Agence Nationale de la Recherche (ANR).
- Leonor Prensa Nieto is a member of the hiring boards for computer science of INPL and Nancy 2 universities.
- Leonor Prensa Nieto is responsible for international relations between ENSEM and Spain, in 2007 she visited the universities of Castilla-La Mancha and Sevilla.

9.4. Teaching

The majority of the members of the MOSEL team are university employees and have significant teaching obligations. We only indicate the graduate courses they have been teaching in 2007.

- Dominique Cansell and Dominique Méry gave a course in the Master's program at Nancy on the specification and modelling of computer-based systems.
- Pascal Fontaine gives introductory courses on specification and verification in the Master's program of the Miage section at Nancy.
- Stephan Merz gave a course on algorithmic verification (together with Olivier Bournez) at the Master's program in Nancy.

10. Bibliography

Major publications by the team in recent years

[1] J.-R. ABRIAL, D. CANSELL, D. MÉRY. *A Mechanically Proved and Incremental Development of IEEE 1394 Tree Identify Protocol*, in "Formal Aspects of Computing", vol. 14, n^{o} 3, 2003, p. 215-227.

[2] J.-R. ABRIAL, D. CANSELL, D. MÉRY. *Refinement and Reachability in Event$_B$*, in "ZB", 2005, p. 222-241.

[3] D. CANSELL, D. MÉRY. *Foundations of the B method*, in "Computers and Informatics", vol. 22, n^o 3–4, 2003, p. 221–256.

[4] D. CANSELL, D. MÉRY, S. MERZ. *Predicate Diagrams for the Verification of Reactive Systems*, in "2nd Intl. Conf. on Integrated Formal Methods (IFM 2000), Dagstuhl, Germany", Lecture Notes in Computer Science, vol. 1945, Springer-Verlag, November 2000, p. 380–397.

[5] D. CANSELL, D. MÉRY, S. MERZ. *Diagram Refinements for the Design of Reactive Systems*, in "Journal of Universal Computer Science", vol. 7, n^o 2, 2001, p. 159–174.

[6] S. MERZ. *On the Logic of TLA+*, in "Computers and Informatics", vol. 22, n^o 3–4, 2003, p. 351–379.

[7] S. MERZ. *A More Complete TLA*, in "FM'99: World Congress on Formal Methods, Toulouse, France", J. WING, J. WOODCOCK, J. DAVIES (editors), Lecture Notes in Computer Science, vol. 1709, Springer-Verlag, 1999, p. 1226–1244.

Year Publications

Books and Monographs

[8] M. GOOSSENS, F. MITTELBACH, S. RAHTZ, D. ROEGEL, H. VOSS. *The LaTeX Graphics Companion, Second Edition - Tools and Techniques for Computer Typesetting*, Addison-Wesley, 2007, http://hal.inria.fr/inria-00172405/en/.

[9] S. MERZ, T. NIPKOW. , M. MISLOVE (editor)*Proceedings of the 6th International Workshop on Automated Verification of Critical Systems (AVoCS 2006)*, Electronic Notes in Theoretical Computer Science, vol. 185, Elsevier, 2007, http://hal.inria.fr/inria-00187585/en/.

Doctoral dissertations and Habilitation theses

[10] E. KANG. *Abstractions booléennes pour la vérification des systèmes temps-réel*, Ph. D. Thesis, Université Henri Poincaré - Nancy I, November 2007, http://tel.archives-ouvertes.fr/tel-00195096/en/.

Articles in refereed journals and book chapters

[11] D. BARSOTTI, L. PRENSA NIETO, A. TIU. *Verification of Clock Synchronization Algorithms: Experiments on a combination of deductive tools*, in "Formal Aspects of Computing", vol. 19, 2007, p. 321-341, http://hal.inria.fr/inria-00097383/en/.

[12] G. BARTHE, L. PRENSA NIETO. *Secure Information Flow for a Concurrent Language with Scheduling*, in "Journal of Computer Security", vol. 16, 2007, p. 647-689, http://hal.inria.fr/inria-00097395/en/.

[13] D. CANSELL, P. GIBSON, D. MÉRY. *Refinement: A Constructive Approach to Formal Software Design for a Secure e-voting Interface*, in "Electr. Notes Theor. Comput. Sci.", vol. 183, 2007.

[14] D. CANSELL, D. MÉRY. *Incremental Parametric Development of Greedy Algorithms*, in "Electr. Notes Theor. Comput. Sci.", vol. 185, 2007, p. 47-62.

[15] D. CANSELL, D. MÉRY. *Designing old and new distributed algorithms by replaying an incremental proof-based development*, in "Festschrift for Egon Börger LNCS", J.-R. ABRIAL, U. GLÄSSER (editors), Lecture Notes in Computer Science, Springer, 2007, http://hal.inria.fr/inria-00174023/en/.

[16] E. KANG, S. MERZ. *Predicate Diagrams for the Verification of Real-Time Systems*, in "Formal Aspects of Computing", vol. 19, 2007, p. 401-413, http://hal.inria.fr/inria-00112065/en/.

[17] T. LECOMTE, D. MÉRY, D. CANSELL. *Patrons de conception prouvés*, in "Génie Logiciel - Magazine de l'ingéniérie du logiciel et des systèmes", 2007, p. 14-18, http://hal.inria.fr/inria-00184827/en/.

[18] M. LEUSCHEL, D. CANSELL, M. BUTLER. *Validating and Animating Higher-Order Recursive Functions in B*, in "Festschrift for Egon Börger", J.-R. ABRIAL, U. GLÄSSER (editors), Lecture Notes in Computer Science, Springer, 2007, http://hal.inria.fr/inria-00174013/en/.

[19] D. MÉRY, S. MERZ. *Specification and Refinement of Access Control*, in "Journal of Universal Computer Science", vol. 13, 2007, p. 1073-1093, http://hal.inria.fr/inria-00147824/en/.

[20] D. ROEGEL. *A complex drawing in descriptive geometry*, in "Tugboat", vol. 28, 2007, p. 218-228, http://hal.inria.fr/inria-00172406/en/.

[21] D. ROEGEL. *Review of "Mathematical Illustrations: A Manual of Geometry and PostScript"*, in "Notices of the American Mathematical Society", vol. 54, 2007, p. 38-42, http://hal.inria.fr/inria-00111243/en/.

[22] D. ROEGEL. *Sphères, grands cercles et parallèles*, in "Cahiers Gutenberg", vol. Avril 2007, 2007, p. 7-22, http://hal.inria.fr/inria-00111240/en/.

Publications in Conferences and Workshops

[23] N. BENAISSA, D. CANSELL, D. MÉRY. *Integration of Security Policy into System Modeling*, in "7th International B Conference - B2007, Besançon, France", J. JULLIAND, O. KOUCHNARENKO (editors), Lecture Notes in Computer Science, vol. 4355, Springer, 2007, p. 232-247, http://hal.inria.fr/inria-00155143/en/.

[24] D. CANSELL, P. GIBSON, D. MÉRY. *Formal verification of tamper-evident storage for e-voting*, in "5th IEEE International Conference on Software Engineering and Formal Methods - SEFM 2007, London, United Kingdom", M. HINCHEY, T. MARGARIA (editors), IEEE, 2007, p. 329-338, http://hal.inria.fr/inria-00184833/en/.

[25] D. CANSELL, D. MÉRY. *Proved-Patterns-Based Development for Structured Programs*, in "Computer Science - Theory and Applications, Second International Symposium on Computer Science in Russia - CSR 2007, Ekaterinburg Russia", V. DIEKERT, M. V. VOLKOV, A. VORONKOV (editors), Lecture Notes in Computer Science, vol. 4649, Springer, 2007, p. 104-114, http://hal.inria.fr/inria-00168307/en/.

[26] D. CANSELL, D. MÉRY, J. REHM. *Time Constraint Patterns for Event B Development*, in "7th International Conference of B Users - B 2007, Besançon, France", J. JULLIAND, O. KOUCHNARENKO (editors), Lecture Notes in Computer Science, vol. 4355, Springer, 2007, p. 140-154, http://hal.archives-ouvertes.fr/hal-00149163/en/.

[27] D. C. B. DE OLIVEIRA, D. DÉHARBE, P. FONTAINE. *haRVey : satisfaisabilité et théories*, in "Approches Formelles dans l'Assistance au Développement de Logiciels - AFADL'07, Namur, Belgium", M.-L. POTET, P.-Y. SCHOBBENS, H. TOUSSAINT, G. SAVAL (editors), 2007, p. 287-288, http://hal.inria.fr/inria-00186640/en/.

[28] L. FEJOZ, S. MERZ. *Dérivation d'algorithmes sans verrou à partir d'une spécification atomique*, in "Approches Formelles dans l'Assistance au Développement de Logiciels - AFADL07, Namur, Belgium", M.-L. POTET, P.-Y. SCHOBBENS, H. TOUSSAINT, G. SAVAL (editors), Presses universitaires de Namur, 2007, p. 213-226, http://hal.inria.fr/inria-00162146/en/.

[29] P. FONTAINE. *Combinations of Theories and the Bernays-Schönfinkel-Ramsey Class*, in "4th International Verification Workshop - VERIFY'07, Bremen Allemagne", B. BECKERT (editor), CEUR Workshop Proceedings, vol. 259, 2007, p. 37-54, http://hal.inria.fr/inria-00186639/en/.

[30] C. HURLIN, A. CHAIB, P. FONTAINE, S. MERZ, T. WEBER. *Practical Proof Reconstruction for First-order Logic and Set-Theoretical Constructions*, in "Isabelle Workshop 2007, Bremen, Germany", L. DIXON, M. JOHANSSON (editors), 2007, p. 2-13, http://hal.inria.fr/inria-00186638/en/.

[31] O. MOSBAHI, J. JARAY. *Specification and Proof of Liveness Properties in B Event Systems*, in "2nd International Conference on Software and Data Technologies - ICSOFT 2007, Barcelona, Spain", Institute for Systems and Technologies of Information, Control and Communication, 2007, http://hal.inria.fr/inria-00158906/en/.

[32] O. MOSBAHI, J. JARAY, S. BEN AHMED. *Spécification et vérification des propriétés de vivacité en B événementiel*, in "6ème Colloque Francophone sur la Modélisation des Systèmes Réactifs - MSR 2007, Lyon France", 2007, 16 pages, http://hal.inria.fr/inria-00172417/en/.

[33] O. MOSBAHI, L. JEMNI, J. JARAY. *A Formal Approach for the Development of Automated Systems*, in "2nd International Conference on Software and Data Technologies - ICSOFT 2007, Barcelona, Spain", Institute for Systems and Technologies of Information, Control and Communication, 2007, http://hal.inria.fr/inria-00158908/en/.

[34] J. REHM, D. CANSELL. *Proved Development of the Real-Time Properties of the IEEE 1394 Root Contention Protocol with the Event B Method*, in "ISoLA 2007 Workshop On Leveraging Applications of Formal Methods, Verification and Validation, Poitiers-Futuroscope, France", Y. AÏT-AMEUR, F. BONIOL, V. WIELS (editors), vol. RNTI-SM-1, Cépaduès, 2007, p. 179-190, http://hal.archives-ouvertes.fr/hal-00184837/en/.

[35] B. STODDART, D. CANSELL, F. ZEYDA. *Modelling and Proof Analysis of Interrupt Driven Scheduling*, in "7th International B Conference - B 2007, Besançon, France", J. JULLIAND, O. KOUCHNARENKO (editors), Lecture Notes in Computer Science, vol. 4355, Springer, 2007, p. 155-170, http://hal.inria.fr/inria-00156871/en/.

[36] Y. ZIMMERMANN. *Développement formel de circuits électroniques par la méthode B*, in "Approches Formelles dans l'Assistance au Développement de Logiciels - AFADL'07, Namur Belgium", M.-L. POTET, P.-Y. SCHOBBENS, H. TOUSSAINT, G. SAVAL (editors), Presses universitaires de Namur, 2007, p. 181-198, http://hal.inria.fr/inria-00172745/en/.

Internal Reports

[37] D. ROEGEL. *Three dials, and a few more: a practical introduction to accurate gnomonics*, Technical Report, 2007, http://hal.inria.fr/inria-00172407/en/.

Miscellaneous

[38] S. MOUELHI. *Vérification formelle d'algorithmes distribués en +CAL*, Technical report, Nancy Université (Université Henri Poincaré), Nancy, France, June 2007.

References in notes

[39] W.-P. DE ROEVER, H. LANGMAACK, A. PNUELI (editors). *Compositionality: The Significant Difference*, Lecture Notes in Computer Science, vol. 1536, Springer-Verlag, 1998.

[40] J.-R. ABRIAL. *Extending B without changing it (for developing distributed systems)*, in "1st Conference on the B method", H. HABRIAS (editor), IRIN Institut de recherche en informatique de Nantes, 1996, p. 169–190.

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

[42] G. BOUDOL, I. CASTELLANI. *Noninterference for Concurrent Programs and Thread Systems*, in "Theoretical Computer Science", vol. 281 (Merci, Maurice. A mosaic in honour of Maurice Nivat), n^{o} 1, 2002, p. 109–130.

[43] L. LAMPORT. *Specifying Systems*, Addison-Wesley, Boston, Mass., 2002.

[44] L. LAMPORT. *Checking a Multithreaded Algorithm with +CAL*, in "20th Intl. Symp. Distributed Computing (DISC 2006), Stockholm, Sweden", S. DOLEV (editor), Lecture Notes in Computer Science, vol. 4167, 2006, p. 151–163.