Second Workshop on Formal and Automated Theorem Proving and Applications

Faculty of Mathematics, University of Belgrade

January 30/31, 2008.

Participants

Milan Banković

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~milan

Dragan Doder

Faculty of Mechanical Engineering, University of Belgrade, Serbia

http://www.mas.bg.ac.yu/obrazovanje/katedre/matematika/-KatedrazaMatematiku-nastavnici-sr/ddoder-la.html

Silvia Ghilezan

Faculty of Engineering, University o Novi Sad, Serbia

http://imft.ftn.ns.ac.yu/~silvia/

Miloš Gligorić

Faculty of Electrical Engineering, University of Belgrade, Serbia

http://kondor.etf.bg.ac.yu/~gliga/

Tihomir Gvero

Faculty of Electrical Engineering, University of Belgrade, Serbia

Florian Haftmann

Fakultät fr Informatik, Technische Universität München, Germany

http://www4.informatik.tu-muenchen.de/~haftmann/index_en.shtml

Hugo Herbelin

INRIA, École polytechnique, Paris, France

http://pauillac.inria.fr/~herbelin/index-eng.html

Jelena Ivetić

Faculty of Engineering, University o Novi Sad, Serbia

http://imft.ftn.ns.ac.yu/~jelena

Svetlana Jakšić

Faculty of Engineering, University o Novi Sad, Serbia

Predrag Janičić

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~janicic

Viktor Kunčak

School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne, Switzerland

http://lara.epfl.ch/~kuncak/

Filip Marić

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~filip

Walther Neuper

Institute for Softwaretechnology, Technische Universität Graz, Austria

http://www.ist.tugraz.at/staff/neuper/

Mladen Nikolić

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~nikolic

Jovanka Pantović

Faculty of Engineering, University o Novi Sad, Serbia

http://imft.ftn.ns.ac.yu/~vanja/

Vesna Pavlović

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~vesnap

Alexis Saurin

Università di Torino, Italy

http://www.normalesup.org/~saurin/

Sana Stojanović

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~sana

Milan Šešum

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~sesum

Milena Vujošević-Janičić

Faculty of Mathematics, University of Belgrade, Serbia

http://www.matf.bg.ac.yu/~milena

Makarius Wenzel

Institut für Informatik, Technische Universität München, Germany

http://wwwbroy.in.tum.de/~wenzelm/

Dragiša Žunić

École Normale Supérieure de Lyon, France

http://perso.ens-lyon.fr/dragisa.zunic/

Programme

January 30, 2008.	
Session *Formal Theorem Proving*	
10:00—10:05	Openning
10:05—10:50	Makarius Wenzel (TU Munich): *Pure Logical Reasoning in Isabelle/Isar*
11:00—11:45	Hugo Herbelin (INRIA, École polytechnique, Paris): *Validating Decisions Procedure for Coq in Coq*
12:00—12:45	Filip Marić (University of Belgrade): *Formalization of SAT Solvers*
13:00—14:30	Lunch break
Session *Logical Foundations*	
14:30—15:15	Silvia Ghilezan (University of Novi Sad): *Computational Interpretations of Logic*
15:30—15:55	Alexis Saurin (Università di Torino): *An Interactive Foundation for Computation as Proof-Search*
15:55—16:20	Jovanka Pantović (University of Novi Sad): *Web Data Modelling and Securing*
16:30—16:55	Dragiša Žunić, Pierre Lescanne (École Normale Supérieure de Lyon, France): *Diagrammatic Reasoning in Classical Logic*
16:55—17:20	Dragan Doder (University of Belgrade), Bojan Marinković, Petar Maksimović (Mathematical Institute, Belgrade), Aleksandar Perović (University of Belgrade): *A Logic With a Conditional Probability Operator*
January 31, 2008.	
Session *Formal Theorem Proving*	
10:00—10:45	Florian Haftmann (TU Munich): *Functional Programming with Isabelle/HOL*
11:00—11:25	Vesna Pavlović (University of Belgrade): *XML suite for Isar*
11:25—11:50	Sana Stojanović, Vesna Pavlović, Predrag Janičić (University of Belgrade): *Formalization and Automation of Euclidean Geometry*
12:00—12:45	Walther Neuper (TU Graz): *Educational Tools as Interactive Models of Mathematics*
13:00—14:30	Lunch break
Session *SAT and SMT Solving and Applications*	
14:30—15:15	Viktor Kunčak (EPF, Lausanne): *Automated Reasoning for Reliable Software*
15:30—15:55	Mladen Nikolić, Filip Marić, Predrag Janičić (University of Belgrade): *Instance-based Selection of Strategies for SAT Solvers*
15:55—16:20	Milan Šešum, Predrag Janičić (University of Belgrade): *Uniform Reduction of Cryptographic Problems to SAT*
16:30—16:55	Milan Banković, Filip Marić (University of Belgrade): *An SMT solver for the theory* all-different
16:55—17:20	Milena Vujošević-Janičić (University of Belgrade): *Using SMT Solver in Detection of Buffer Overflow Bugs*

Abstracts

Makarius Wenzel (TU Munich)
Title: *Pure logical reasoning in Isabelle/Isar*

Abstract: We shall explain the relationship between (1) the Isabelle/Pure framework, (2) the Isar proof language, and (3) Isabelle object logics such as HOL. The aim is to point out practically relevant techniques for more direct formal reasoning in the framework, avoiding logical connectives of the object language to obscure applications by excessive formality.

When appealing to Pure natural deduction principles, structured Isar proofs can be produced with little formal overhead, and the demand for automated proof tools is reduced. In this paradigm of generic reasoning, the object-logic mostly serves as a way to produce suitable reasoning patterns in a fully foundational manner. For example, inductive predicates in Isabelle/HOL yield suitable introduction, elimination, and induction principles for pure logical reasoning, while hiding internals of existential quantifiers, conjunction, disjunctions, and fixed-points in the guts of the implementation. Using inductive predicates instead of primitive definitions, user applications usually work out more smoothly, and the effort for proof construction is significantly reduced, both for the machine and the user.

Hugo Herbelin (INRIA, École polytechnique, Paris)
Title: *Validating Decisions Procedure for Coq in Coq*

Abstract: After a quick overview of the Coq proof assistant and its underlying formalism (the Calculus of Inductive Constructions), we will survey the different approaches used in Coq to validate automated deduction procedures or semi-procedures, ranging from decision procedures directly written in the proper language Coq (so-called reflexion), decision procedures producing traces in some ad hoc formal system mappable to the language of Coq (trace-based reflexion) and decision procedures directly producing inference steps in the language of Coq (shallow embedding).

In a last step, we will survey ongoing works by Sylvain Conchon, Evelyne Contejean and Stéphane Lescuyer aiming to fully certify the Alt Ergo SMT solver in Coq (http://ergo.lri.fr).

Filip Marić (University of Belgrade)
Title: *Formalization of SAT Solvers*

Abstract: The propositional satisfiability problem (SAT problem) is the problem of checking if there is a truth assignment under which a given propositional formula evaluates to true. SAT solvers are tools that solve the SAT problem. This talk will present our experience in formalization and formal verification

of SAT solver correctness within the system Isabelle. We have formalized and verified many different SAT solving techniques, starting from the basic DPLL procedure and ending with some state-of-the art solver implementations. Also, several different verification techniques were used. These include verification of high level state-transition-system descriptions, Hoare-logic formalizations of imperative code, and verification of shallow embedding into HOL.

Silvia Ghilezan (University of Novi Sad)
Title: *Computational Interpretations of Logic*

Abstract: The fundamental connection between logic and computation, known as the Curry–Howard correspondence or formulae-as-types and proofs-as-programs paradigm, relates logical and computational systems. We present an overview of computational interpretations of intuitionistic and classical logic:

- intuitionistic natural deduction — lambda calculus;
- intuitionistic sequent calculus — lambda Gentzen calculus;
- classical natural deduction — lambda mu calculus;
- classical sequent calculus — lambda mu mu calculus.

Fundamental properties of these calculi, such as confluence, normalisation properties, reduction strategies call-by-value and call-by-name, separability, reducibility method, lambda-models are in focus. These fundamental properties and their counterparts in logics, via the Curry–Howard correspondence, are discussed.

Alexis Saurin (Università di Torino)
Title: *An Interactive Foundation for Computation as Proof-Search*

Abstract: Proof search and proof normalization are usually considered as the two main approaches to a proof-theoretical modelling of computation. Although they are both deeply related to Gentzen's Hauptsatz, the relations between these two dynamical views of proofs are not well understood. In this talk, I shall present a way to relate proof search and proof normalization (or cut-elimination) by considering the interactive framework of Girard's ludics as a setting for considering proof-search as guided by a normalization procedure with tests or counter-proofs, which I call interactive proof-search. Moreover, I shall advocate how this setting could serve as a uniform foundation to several features of logic programming languages in particular backtracking and control operators.

Jovanka Pantović (University of Novi Sad)
Title: *Web data modelling and securing*

Abstract: Web data manipulation requires the complex interaction and coordination between processes and data at different locations. This coordination is modelled by Xdπ calculus, introduced by Gardner and Maffeis in 2003. The Xdπ is a peer-to-peer model for mobile processes and distributed semi-structured data. I shall present a type system for Xdπ, in which a well-typed network can reduce only to a well-typed network, assuring access and migration rights. This resulted from a joint work with Mariangiola Dezani-Cianciaglini (Università di Torino), Silvia Ghilezan (University of Novi Sad) and Daniele Varacca (University of Paris 7 & CNRS, France).

Dragiša Žunić, Pierre Lescanne (École Normale Supérieure de Lyon, France)
Title: *Diagrammatic Reasoning in Classical Logic*

Abstract: Gentzen's sequent calculus is one of the formalisms best suited to represent classical logic. However there is certain 'syntactic bureaucracy' in sequent derivations. Proofs which differ only in the order of applying two independent inference rules should be considered the same, but they have different syntactic representations.

We start from the standard classical sequent system G1 with explicit weakening and contraction rules. We introduce its two-dimensional counterpart - the diagrammatic calculus, which abstracts away from unessential details, and captures the essential computation. Weakening plays a computational role of an eraser, whilst contraction plays a role of a duplicator of diagrams.

In the style of Curry-Howard, diagrams correspond to proofs in classical logic (modulo permutation of independent inference rules). The computation corresponds to proof transformation.

Dragan Doder, Bojan Marinković, Petar Maksimović, and Aleksandar Perović (University of Belgrade and Mathematical Institute, Belgrade)
Title: *A Logic With a Conditional Probability Operator*

Abstract: We will present a sound and strongly complete axiomatization of the reasoning about linear combinations of conditional probabilities, including comparative statements. The developed logic is decidable, with a PSPACE containment for the decision procedure.

Florian Haftmann (TU Munich)
Title: *Functional Programming with Isabelle/HOL*

Abstract: Recently, the logic Isabelle/HOL and functional programming have become more close, due to two developments: new specification tools have been developed, notably for recursive functions and type classes; new facilities for turning logical specification into executable code in SML, OCaml and Haskell have emerged. This tutorial gives a short overview on those topics; the aim is not to give a through investigation of the meta theory behind, but to demonstrate the application of the techniques sketched above in practice.

Vesna Pavlović (University of Belgrade)
Title: *XML suite for Isar*

Abstract: EXtensible Markup Language (XML) technology provides a convenient way for representing complex kind of data. We have developed an XML format for storing proofs in Isar-style syntax (i.e. formal proofs given in human-readable way). This format can be used for representing a class of geometrical statements and their formal proofs in Isar language. We have also developed a corresponding suite of XML tools that includes: a tool for transforming the XML documents into valid Isar proofs; a tool for converting XML documents into HTML documents consisting of proved geometrical statements and their graphical illustrations.

Sana Stojanović, Vesna Pavlović, Predrag Janičić (University of Belgrade)
Title: *Formalization and Automation of Euclidean Geometry*

Abstract: Formalizations of Euclidean geometry within proof assistants (Isabelle and Coq) have already been developed for several axiom systems, such as Hilbert's one and Tarski's one. These formalizations are important for building formalized mathematical knowledge base, but also in mathematical education and in applications of computational geometry. In this talk we will present one method for automated proving of theorems of Euclidean geometry. The method is based on simple forward-chaining, but can still prove a large number of theorems and can export short proofs to proof assistants.

Walther Neuper (TU Graz)
Title: *Educational Tools as Interactive Models of Mathematics*

Abstract: Dynamic Geometry as well as Algebra Systems can be conceived as "models of mathematics". Learning mathematics then can occur by interaction with such models. The design of such systems raises novel questions like:

- Starting from some context C (i.e. given objects and assumptions), what are the operations O creating another context C', $C \longrightarrow_O C'$? Can C and O be abstracted to cover both, geometry and algebra ?
- How can stepwise operations $C \longrightarrow_O C'$ be related to logics like LCF, Natural Deduction or Calculus of Inductive Constructions ?
- How can a system "modeling mathematics" be related to the concepts of Isabelle/Isar (document, context, theory, command, method, attribute etc) ?

These questions will be illustrated by examples and would hopefully led to discussions without expecting final answers.

Viktor Kunčak (EPF, Lausanne)
Title: *Automated Reasoning for Reliable Software*

Abstract: I will present our experience with developing and using tools to prove correctness properties of software systems. Using these tools we have verified correctness of data structures such as lists, trees, and hash tables.

Algorithms for deciding satisfiability of logical formulas play an important role in these approaches. I will present our work on deciding satisfiability of formulas involving sets, multisets, and cardinality operators. We show a polynomial-time reduction from satisfiability of multiset formulas to satisfiability of formulas in linear arithmetic extended with a new 'star' operator. Using properties of integer cones and bounds on generators of solutions of integer linear programming problems, we show that formulas of linear arithmetic with star have polynomial-sized witnesses to satisfiability. Consequently, we prove that the satisfiability problem for multiset formulas is NP-complete, exponentially improving complexity compared to previously known algorithms.

Mladen Nikolić, Filip Marić, Predrag Janičić (University of Belgrade)
Title: *Instance-based Selection of Strategies for SAT Solvers*

Abstract: In checking satisfiability of a propositional formula by a SAT solver, typically solver's default strategies or strategies known to perform well in some domains are used. We will present a methodology for choosing suitable strategies with respect to the syntactical structure of the formula being solved. The methodology is based on data mining techniques and shows significant improvements in performance compared to the best fixed combination of strategies.

Milan Šešum, Predrag Janičić (University of Belgrade)
Title: *Uniform Reduction of Cryptographic Problems to SAT*

Abstract: Logical cryptoanalysis problems can often be expressed as computing an inverse of a function. However, computing an inverse for a given function is often very hard, if not impossible. It often requires a deep analysis of the function considered and specific solutions. If a function is given only by its implementation, this analysis is even more difficult and error-prone. We will describe one generic approach for computing inverse functions (from a certain class), given their implementations in programming language C/C++. The approach is based on *(i)* reducing the problem to SAT and *(ii)* exploiting the polymorphism of the C++ language. We present a case-study of the approach — on the logical cryptoanalysis of the DES algorithm and show that our approach gives better results than one domain-specific approach. The approach can be applied to a wide range of problems, not only logical cryptoanalysis problems.

Milan Banković, Filip Marić (University of Belgrade)
Title: *An SMT solver for the theory* all-different

Abstract: All-different type of constraint is one of the most common global constraints found in practise. Broad variety of problems in scheduling, puzzle solving, etc. can be reduced to all-different constraint satisfaction problem. In recent years, research topic of special interest is how to represent this problem within a first order theory, and then solve it using the SMT approach. In this talk, one new decision procedure for all-different theory based on the matching theory in bipartite graphs will be presented. A special attention will be given to theory propagations explainations, and a new efficient algorithm for this purpose will be proposed.

Milena Vujošević-Janičić (University of Belgrade)
Title: *Using SMT Solver in Detection of Buffer Overflow Bugs*

Abstract: SAT and SMT solvers have a number of applications in software and hardware verification tasks. We will describe how an SMT solver for linear arithmetic can be used for detecting buffer overflow bugs in C programs. This sort of bugs is very important because buffer overflows are suitable targets for security attacks and sources of serious programs' misbehavior. We will also describe our tool for this problem. It uses an external and easily extendable

knowledge database that stores all the reasoning rules so they are not hard-coded. The analysis performed is flow-sensitive and inter-procedural, and deals with both statically and dynamically allocated buffers. The tool uses ArgoLib SMT solver, but can also use use any external automated theorem prover that follows SMT-LIB standards.
