

# Application for a Dagstuhl Seminar

## *Deduction and Arithmetic*

Nikolaj Bjørner  
Reiner Hähnle  
Tobias Nipkow  
Christoph Weidenbach

24. December 2000

### **Abstract**

This application proposes a seminar bringing together researchers working in deduction and fields related to arithmetic constraint solving. Current research in deduction can be categorized in three main strands: SMT solvers, automated first-order provers, and interactive provers. Although dealing with arithmetic is currently in focus of all three for some years, they are still in need of much better support of arithmetic. It can be safely assumed that arithmetic will be a major focus in all three main approaches to automated deduction during the coming 5-10 years. In this situation it is extremely important that the various sub-communities communicate with each other to avoid duplicate effort and to exploit synergies.

## **Contents**

|                                                         |          |
|---------------------------------------------------------|----------|
| <b>1 Seminar title: <i>Deduction and Arithmetic</i></b> | <b>2</b> |
| <b>2 Organizers</b>                                     | <b>2</b> |
| <b>3 Classification</b>                                 | <b>3</b> |
| <b>4 Keywords</b>                                       | <b>3</b> |
| <b>5 Proposal for a Date</b>                            | <b>3</b> |
| <b>6 Description of the Seminar: Topics and Goals</b>   | <b>3</b> |
| <b>7 Relation to Previous Dagstuhl Seminars</b>         | <b>7</b> |
| <b>8 List of Potential Participants</b>                 | <b>8</b> |
| <b>9 Vitas of the Organizers</b>                        | <b>9</b> |

## 1 Seminar title: *Deduction and Arithmetic*

This event is meant to be the tenth in the series of the Dagstuhl “Deduction” seminars held biennially since 1993.

## 2 Organizers

- Dr. Nikolaj Bjørner  
Microsoft Research  
One Microsoft Way, Redmond, WA 98052, USA  
Phone: +1 (425) 7057928  
Fax: +1 (425) 936-7329  
Email: [nbjorner@microsoft.com](mailto:nbjorner@microsoft.com)  
Home page: <http://research.microsoft.com/~nbjorner>
- Prof. Dr. Reiner Hähnle  
Chalmers University of Technology  
Department of Computer Science and Engineering  
412 96 Gothenburg, Sweden  
Phone: +46 31 772 1061  
Fax: +46 31 772 3663  
Email: [reiner@chalmers.se](mailto:reiner@chalmers.se)  
Home page: <http://www.cse.chalmers.se/~reiner>
- Prof. Dr. Tobias Nipkow  
Technische Universität München  
Institut für Informatik  
Boltzmannstr. 3, 85748 Garching, Germany  
Phone: +49 (0)89 289 17302  
Fax: +49 (0)89 289 17307  
Email: [nipkow@in.tum.de](mailto:nipkow@in.tum.de)  
Home page: <http://www4.informatik.tu-muenchen.de/~nipkow>
- Prof. Dr. Christoph Weidenbach  
Max Planck Institute for Informatics  
Campus E1 4, 66123 Saarbrücken, Germany  
Phone: +49 (0)681 9325 900  
Fax: +49 (0)681 9325 999  
Email: [weidenbach@mpi-inf.mpg.de](mailto:weidenbach@mpi-inf.mpg.de)  
Home page: <http://www.mpi-inf.mpg.de/~weidenb>

The curricula vitae of the organizers are included.

### 3 Classification

- Artificial Intelligence
- Semantics / Formal Methods
- Verification / Logic

### 4 Keywords

Automated Deduction, Program Verification, Arithmetic Constraint Solving

### 5 Proposal for a Date

**Preferred:** January 1 – January 5, 20XX

**Alternate 1:** December 24 – December 29, 20XX

**Alternate 2:** January 8 – January 13, 20XX

**Alternate 3:** January 16 – January 21, 20XX

### 6 Description of the Seminar: Topics and Goals

This application proposes a meeting bringing together researchers working in deduction and fields related to arithmetic constraint solving.

In Section 6.1, we give an overview on the seminar’s topic and on the respective research communities. Afterwards, Section 6.2 describes the goals of the proposed seminar.

#### 6.1 Topics of the Seminar

Arithmetic plays a fundamental role in deduction. Since the advent of formal logic, the formalization of set theory and arithmetic has been the central problems forming the field of symbolic logic. Logical constraints over arithmetical properties occur frequently in diverse areas including classical theorems in mathematics, and in applications, such as program analysis and verification. But arithmetic has not always been an important topic in the theorem proving community.

The first automatic theorem prover was an implementation of Presburger Arithmetic by Martin Davis in the summer of 1954. Yet with the availability of powerful propositional and predicate calculus proof procedures some years later, arithmetic would be relegated to the sidelines. Pure logic would take center stage with resolution, tableaux calculi and natural deduction the most prominent inference systems. Interest in arithmetic

revived in the 1980s with the advent of powerful interactive theorem provers that needed and supported arithmetic for their applications. The need for efficient computer aided deduction with support for arithmetic in the area of program analysis and verification recently gave birth to a new technology, so called SMT solvers. Although relatively new, SMT solvers have had significant impact. Efficient handling of quantifiers is a challenge for SMT solvers and has lead to a number of recent efforts integrating arithmetic into first-order provers.

Thus we have three strands of automated deduction (1) SMT solvers, (2) automated first-order provers, and (3) interactive provers in need of (more) arithmetic. Below we describe the relationship in more detail.

1. SMT:

Satisfiability Modulo Theories (SMT) solvers distinguish themselves by integrating built-in support for a combination of theories, including prominently the theory of arithmetic. In spite of long-running attention, research in decision procedures for additive, or so-called linear, arithmetic remains highly active. Recent progress includes variants of dual simplex, new cutting plane methods for integer linear programming (Dillig and Dillig), symmetry breaking methods (Hentenryck), using Ford-Fulkerson graph search algorithms for solving sparse sets of difference arithmetic constraints (Cotton and Mahler, Somenzi and Kim) (constraints are of the form  $x - y \leq k$ ), and extending methods to octagon constraints (constraints are of the form  $\pm x \pm y \leq k$ ). One recent development is the re-examination of a Fourier-Motzkin style satisfiability procedure in the light of using models to guide resolution inferences (Cotton, McMillan, Korovin, Tsiskaridze and Voronkov).

It is common for modern SMT solvers to use a backtracking proof-search procedure, yet it was not well understood how to integrate solvers for linear arithmetic efficiently until a break-through in 2006 in the context of the Yices system (Dutertre and de Moura). Concurrent and subsequent efforts on SMT solvers have furthered the understanding on efficient integration of arithmetic with deduction.

Most often handling arithmetic formulas in isolation is not sufficient. Applications typically use a non-disjoint combination of arithmetic and other theory reasoning. Examples include mixing arithmetic with arrays, sets, multi-sets and term algebras (Bradley, Ting Zhang, Kuncak and Piskac).

SMT solvers nowadays handle quantifier-free arithmetic well, but are not directly equipped to solve arithmetical formulas with quantifiers. Recent progress on building in quantifier-elimination procedures for linear and non-linear arithmetic have made practical integration of such richer arithmetic deduction viable. The progress includes combining efficient SMT solvers with a quantifier-elimination procedure, it includes tools and theory using automata for quantifier-elimination over the (additive/linear) integers and reals, and the development of formally verified quantifier elimination procedures (Iosif, Kapur, Klaedtke, Monniaux, Nipkow, Passmore, Tiwari).

On the ground level one can encode problems alternatively in logic or in integer

arithmetic. Hooker tries to identify synergies between both formulations.

## 2. ATP:

Until the end of the last century, research in first-order logic theorem proving concentrated on efficient calculi in general and the integration of equational theories in particular. One of the most sophisticated calculi out of this research is Uwe Waldmann’s superposition calculus for totally ordered divisible abelian groups. Although this calculus represents already a realm of arithmetic, due to its complexity it is obvious that further integration of “richer” arithmetic theories into first-order logic should be done by rather a combination approach than an integration approach.

One major challenge of combining first-order logic calculi with arithmetic (decision) procedures is that of compactness/completeness and termination. While Boolean combinations of ground atoms, as they are considered by SMT solvers typically do not cause trouble with respect to those challenges, combining first-order clauses including variables and free function/predicate symbols with an arithmetic theory can never result in a compact/complete/terminating calculus, in general. Starting from the beginning of the previous century, a new branch of research has grown trying to understand the combination of first-order logic with arithmetic theories. Major results up to now are sufficient conditions for compactness/completeness/termination and the actual development of combination procedures.

The approaches for the combination of first-order logic with arithmetic which have been mainly developed in recent years are: hierarchic superposition (Bachmaier, Ganzinger, Waldmann), local theory extensions (Ihlemann, Jacobs, Sofronie-Stokkermans), LASCA (Korovin, Voronkov), non-disjoint combinations (Ghilardi, Nicolini, Ringeissen, Rusinowitch, Zucchelli), DPLL( $\Gamma$ ) (Bjørner, de Moura), constraint sequent calculi (Rümmer), SUP(LA) (Althaus, Kruglov, Weidenbach),  $\mathcal{ME}$ (LIA) (Baumgartner, Fuchs, Tinelli), decidable fragments (Fontaine), and DPLL( $G + \Gamma$ ) (Bonancina, Lynch, de Moura). Out of these approaches the following combination procedures are available: SPASS+T (Prevesto, Waldmann), Z3( $\mathcal{SP}$ ) (Bjørner, de Moura), H-PILoT (Ihlemann, Sofronie-Stokkermans), veriT (Bouton, de Oliveira, Déharbe, Fontaine), and SPASS(LA) (Althaus, Kruglov, Weidenbach), KeYmaera (Platzer, Quesel, Rümmer).

The actual combination typically requires the solution of purely arithmetic problems in order to establish valid inferences and simplifications. These problems are of a specific nature in that the form of the arithmetic formulas (conjunctions of atoms or implications thereof) and the way they need to be tested (typically fixing one part of the implication and varying the other several ten thousands of times) require specific variants of the known arithmetic procedures for an eventual efficient combination.

## 3. ITP:

Interactive theorem provers initially came with built-in decision procedures for

quantifier-free linear arithmetic (Nqthm, Nuprl and PVS). More foundational systems (Coq, HOL, Isabelle) then developed new techniques to implement these decision procedures by reducing them to pure logic, trading efficiency for guaranteed correctness. John Harrison established interactive proof about real numbers both as a research area and as an industrial application: at Intel he proves correctness of floating point algorithms and hardware with the help of his HOL Light system. Closely related is the area of unlimited precision real arithmetic where interactive theorem provers provided the first verified and practical algorithms.

John Harrison also started a line of work where he used methods from nonlinear optimization, namely semi-definite programming, to prove quantifier-free nonlinear formulae. An open challenge is to provide a practical yet verified implementation of full quantifier elimination for the reals with addition and multiplication. Mahboubi had formalized Collin’s CAD algorithm but did not manage to verify it because of the wealth of mathematics required.

A very challenging application of interactive proof and arithmetic is the Flyspeck project by Thomas Hales. He is leading an effort to formalize his proof of the Kepler conjecture in an interactive theorem prover. One subproblem where not much progress has yet been made is the automatic proof of hundreds of nonlinear inequalities required in the overall proof.

Further aspects of arithmetic reasoning are present in deductive software verification systems: interactive systems such as KIV and KeY combine a number of automatic arithmetic reasoning methods and control them with heuristics that are specific for verification. In verification of safety-critical software it is necessary to reason about the accuracy of floating point computations.

The time is clearly ripe to bring together experts in the above subareas of deduction, and in reasoning about arithmetic, to exchange experiences and insights.

## 6.2 Goals of the Seminar

**Synergies and Research Questions** It can be safely assumed that arithmetic will be a major focus in all three main approaches to automated deduction during the coming 5–10 years. In this situation it is extremely important that the various sub-communities communicate with each other to avoid duplicate effort and to exploit synergies. The research questions to be pursued and answered include

- which arithmetic problems are best solved with which approach?
- how to handle very complex numeric representations such as the IEEE floating point standard with a high degree of automation?
- arithmetic in combination with other theories results easily in languages with a very complex decision problem—how can a high degree of automation be obtained nevertheless?
- how can SMT-based reasoning be combined with Abstract Interpretation?

- what is the best way to incorporate arithmetic simplification available in computer algebra systems into deductive frameworks?
- how can the specific structure of arithmetic problems generated by deduction systems be exploited?

The proposed Dagstuhl seminar will bring together:

- researchers working on deduction methods and tools aiming at the integration of arithmetic;
- specialists in formalization of and reasoning about arithmetic;
- consumers of deduction technology that is capable of arithmetic reasoning such as in program analysis and verification.

**Impact on the Research Community** The importance of arithmetical reasoning is currently realized in different conferences, such as the ITP conference (dedicated to interactive provers) and in IJCAR (dedicated to automated reasoning), the SMT workshop and the FroCoS (frontiers of combining systems) community. Such a meeting may help in the organization of future joint conferences.

We feel that such a meeting will further raise the awareness for the importance of supporting arithmetic in automated deduction and provide a point of focus and reference: publications on deduction with arithmetic are currently scattered over a plethora of different workshops and conferences and it is not easy to find out about the state-of-art for a given problem. This seminar with the associated Dagstuhl proceedings will provide a convenient point of reference, not only for latest results, but also for currently active researchers.

The meeting will not only allow for cross-fertilization between research on deduction and arithmetic, but it will also help to bridge gaps between foundational research on these topics and application-driven approaches; e.g., the transfer of new theoretical results into applications, or the discovery of new research problems motivated by applications.

The applying research scientists have high international standing in the area. For example, several of them have been program chairs of the main deduction-related international conferences: International Joint Conference on Automated Deduction, IJCAR (Nipkow, Hähnle), Rewriting Techniques and Applications, RTA (Nipkow), TABLEAUX (Hähnle). Tobias Nipkow is editor-in-chief of the Journal of Automated Reasoning, JAR. All four applicants are also involved in the design of leading tools in the area of automated deduction: Z3 (Bjørner), KeY (Hähnle), Isabelle (Nipkow), Spass (Weidenbach).

## 7 Relation to Previous Dagstuhl Seminars

The Dagstuhl seminars on “Deduction” have been a major success since the first one held in 1993. The unique atmosphere of Dagstuhl and the high level of communication

resulted in a series of meetings that have a significant impact on the area.

The organizers of the proposed seminar participated in most previous editions of the “Deduction” Dagstuhl seminars. Moreover, Reiner Hähnle and Tobias Nipkow were among the organizers of the previous “Deduction” seminar in 2009.

Since 2003, each edition of the “Deduction” seminar is devoted to a special sub-topic (e.g., “Deduction and Infinite-state Model Checking” in 2003, “Deduction and Applications” in 2005, “Deduction and Decision Procedures” in 2007, and “Interaction versus Automation” in 2009). The proposed seminar continues the tradition of the “Deduction” seminars, but its focus on the combination deduction and arithmetic is substantially different from the focus of the earlier seminars.

The choice of this focus was influenced by the many recent results in logic modeling of arithmetic as well as integration of arithmetic in deduction procedures for which verification is the driving application. Another strong motivation is recent results in the formalization of deep mathematical results about arithmetic.

These developments were already partly visible at the latest Dagstuhl seminars on “Deduction”, in particular, “Deduction and Decision Procedures”, but also at related other Dagstuhl seminars attended by the organizers. For example, these include Dagstuhl seminars on “Mathematics, Algorithms, Proofs”, “The Java Modeling Language”, and “The Challenge of Software Verification”. Seeing the last two seminars in perspective with the “Deduction” seminar series gives rise to the conviction that efficient handling of arithmetic is crucial to scale up verification for mainstream industrial usage.

## 8 List of Potential Participants

We have at this point identified 85 international researchers whose research involve Deduction and Arithmetic.

We distinguish between *first round invitees* and *second round invitees*. For each invitee, the following information beyond its affiliation, Email address, and URL is provided in the tables below:

**SMT / Automated / Interactive Deduction / Arithmetic (SMT/AD/ID/ARI):**

For each invitee we indicate whether his/her primary direction of research is in the area of SMT (SMT) automated (AD) of interactive deduction (ID), or arithmetic (ARI). Notice that some invitees intersect with more than one category.

**Person from Academia / Person from Industry (A/I).**

**Young Researchers:** Invitees of age 35 or below are marked with a star (★).

**Women:** Female invitees are marked with a plus (+).

There is a total of 78 first round invitees and a total of 15 second round invitees.

## Germany

| Name<br><i>Affiliation</i>              | SMT/AD/ID/ARI<br><i>A/I</i> | E-Mail<br><i>URL</i>                                                                  |
|-----------------------------------------|-----------------------------|---------------------------------------------------------------------------------------|
| <b>First round invitees (total: 14)</b> |                             |                                                                                       |
| +Prof. Dr. ABC<br>Flatland University   | AD<br>A                     | abc@uflat.edu<br><a href="http://www.uflat.edu/~abc">http://www.uflat.edu/~abc</a>    |
| *Dr. DEF<br>The Research Company TRC    | ARI<br>I                    | def@trc.com<br><a href="http://www.trc.com">http://www.trc.com</a>                    |
| ...                                     |                             |                                                                                       |
| <hr/>                                   |                             |                                                                                       |
| <b>Second round invitees (total: 4)</b> |                             |                                                                                       |
| Dr. XYZ<br>Earth University             | SMT<br>A                    | xyz@uearth.edu<br><a href="http://www.uearth.edu/~xyz">http://www.uearth.edu/~xyz</a> |
| ...                                     |                             |                                                                                       |

## Europe except Germany

Omitted.

## USA & Canada

Omitted.

## Asia and Australia

Omitted.

## 9 Vitas of the Organizers

(Original CVs of this sample proposal omitted.) *Please provide a 0.5–1 page research CV of each organizer that gives an overview of an organizer's academic career and especially points out community services and recognitions. However, it should not list every paper ever published as the five most relevant papers are sufficient.*