09461 Abstracts Collection
Algorithms and Applications for Next Generation SAT Solvers
— Dagstuhl Seminar —

Bernd Becker[1], Valeria Bertacco[2], Rolf Drechsler[3] and Masahiro Fujita[4]

[1] Universität Freiburg, DE
becker@informatik.uni-freiburg.de
[2] Univ. of Michigan - Ann Arbor, US
[3] Universität Bremen, DE
drechsle@informatik.uni-bremen.de
[4] University of Tokyo, JP
fujita@is.kyushu-u.ac.jp

Zusammenfassung. From 8th to 13th November 2009, the Dagstuhl Seminar 09461 „Algorithms and Applications for Next Generation SAT Solvers“ was held in Schloss Dagstuhl–Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts, slides or full papers are provided, if available.

Topics: data structures / algorithms / complexity, hardware, verification / logic
Keywords. Boolean Satisfiability, Formal Methods, Word Level, Quantification, Multithreading

09441 Executive Summary – Algorithms and Applications for Next Generation SAT Solvers

In the last decade solvers for Boolean satisfiability (SAT solver) have successfully been applied in many different areas such as design automation, databases, artificial intelligence, etc. A major reason triggering this widespread adoption was the development of several sophisticated SAT techniques and as a result, today SAT solvers are the core solving engine behind many industrial and university tools as well.
However, common SAT solvers operate at the Boolean level and, in general, can only solve a satisfiability problem for formulas expressed in propositional logic. Due to the increasing complexity of the considered problems (e.g. exponential growth of the design sizes in circuit verification), in the last years several

approaches have been studied which lift the solving engine to higher levels of abstractions and/or logics that have additional representational power, such as quantified Boolean logic or word level descriptions.
A new generation of SAT solvers - namely Quantified Boolean Formula (QBF) solvers, word-level solvers and SAT Modulo Theories (SMT) solvers - have been introduced. Furthermore, due to the development of multi-core processors, research in the area of (thread-)parallel SAT solving is growing and will be increasingly important in the near future.
The seminar brought together 36 experts from both 'worlds', i.e. researchers investigating new algorithms for solving SAT instances and researchers using SAT for solving problems in a range of application domains, with a particular focus in VLSI CAD (but not exclusively restricted to this area).
An intensive exchange during the seminar initiated discussions and cooperation among the participants and will hopefully lead to further improvements in the next generation SAT algorithms. Moreover, since most of the new techniques are not yet deployed in applications - even if they are often more competitive in contrast to traditional solving paradigms - the seminar provided an excellent forum to familiarize researchers in this area with the new techniques.

SMT-Solving for the First-Order Theory of the Reals

Erika Ábrahám (RWTH Aachen, DE)

SAT-solving is a highly actual research area with increasing success and plenty of industrial applications. SMT-solving, extending SAT with theories, has its main focus on linear real constrains. However, there are only few solvers going further to more expressive logics like the first-order theory of the reals.

In this talk we discuss the problems arising in this latter setting, and suggest some first solutions.

Keywords: SMT-solving, first-order theory of the reals, verification

Joint work of: Ábrahám, Erika; Loup, Ulrich

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2508

Lazy Hyper Binary Resolution

Armin Biere (University of Linz, AT)

We describe a technique implemented in our award winning SAT solver PrecoSAT, which learns binary clauses during boolean constraint propagation. Together with simple equivalence reasoning and literal probing this achieves the same effect as preprocessing trough hyper binary resolution but in a controlled and cheap way.

Keywords: SAT, hyer binary resolution, dominators, preprocessing

Automata-based decision procedures for first-order logical theories with addition

Jochen Eisinger (Universität Freiburg, DE)

Büchi observed, in the 1960s, that automata over finite words can not only be used to decide various sequential and modal logics. Automata-based methods can also be used to analyze arithmetical theories. For example, automata over finite words can represent addition of natural numbers. Since automata are closed under boolean operations and projection, one immediately obtains a decision procedure for Presburger arithmetic, i.e., the first-order logical theory over the natural numbers with addition $\mathrm{FO}(\mathbb{N}, +)$ or $\mathrm{FO}(\mathbb{Z}, +, <)$. A similar approach works for mixed linear arithmetic, i.e., $\mathrm{FO}(\mathbb{R}, Z, +, <)$ using Büchi automata. Boigelot et. al. have shown that even weak deterministic Büchi automata suffice to decide this logical theory.

Although there exist efficient implementations of these automata-based decision procedures for $\mathrm{FO}(\mathbb{R}, Z, +, <)$, many research questions are still only partially answered, and it turns out that a limiting factor in the automata-based representation is the size of the automata.

This talk gives an overview of automata-based decision procedures for first-order logical theories with additions and highlights possible applications for solving SMT problems.

Keywords: Büchi automata, automata theorie, decision procedures, bounded arithmetic

Stochastic Satisfiability Modulo Theory

Martin Fraenzle (Universität Oldenburg, DE)

Aiming at symbolic methods for the analysis of probabilistic hybrid systems, we recently introduced the notion of stochastic satisfiability modulo theories (SSMT) problems and the corresponding SiSAT solving algorithm. The notion of SSMT extends SMT with randomized (aka. stochastic) as well as existential and universal quantification as known from stochastic propositional satisfiability (SSAT). In this talk, we describe the symbolic encoding of probabilistic hybrid automata as SSMT problems and explain the algorithms underlying SSMT solving.

Solving Hard Combinatorial Problems with SAT Solvers

Hiroshi Fujita (Kyushu University, JP)

SAT-based approaches seem useful to solve hard combinatorial problems. Recently we had a chance to use a new high performance computing facility at Research Center for Verification and Semantics (CVS) of National Institute of Advanced Industrial Science and Technology (AIST) of Japan. To make the most of it and to see how efficient and scalable state-of-the-art SAT solvers are, we tried to solve some hard combinatorial problems; quasigroup existence (QG), job shop scheduling problems (JSSP), and search for Ramsey numbers. QG5.18 that has long been open was solved only recently with MiniSat2 on one of the cluster machines of CVS-AIST that ran 224 cores in parallel. As for JSSP's, two open problems ABZ9 and YN1 were solved this summer. For each JSSP, many SAT instances were generated for an interval of a parameter (that represents a possible completion time of all the jobs,) between given lower bound (LB) and upper bound (UB). By solving them in parallel, we succeeded to find two adjacent instances of which the smaller one being UNSAT, and the larger SAT, thus providing a certification of the optimum schedule for the job shop. A Ramsey number, given its LB and UB, can be determined in a similar manner, though its certification is obtained as a (SAT,UNSAT) pair of SAT instances different from an (UNSAT,SAT) pair for JSSP's, and more difficult in general. We succeeded to reconfirm the current best LB's for R(5,5)>42 and R(3,10)>39, although we have not yet obtained new results (the exact Ramsey numbers or better LB's or UB's for them). These problems are indeed extremely hard and seems intractable. Still, you might have a chance to solve one, provided that you had a more powerful computing environment, more efficient scalable solvers, and more useful ideas, e.g. effective constraints and tactics.

Keywords: Quasigroup, JSSP, Ramsey number

Joint work of: Fujita, Hiroshi; Hasegawa, Ryuzo; Koshimura, Miyuki

Modular Arithmetic Decision Procedure with Auto-correction Mechanism

Masahiro Fujita (University of Tokyo, JP)

We present an efficient decision procedure which can deal with modulo equivalence based on Horner-Expansion-Diagram (HED) as a canonical decision diagram [1] in order to prove the equivalence of an ANDINVERTER- GRAPH (AIG) representation as the implementation against a polynomial expression over n Z2 as the specification. In other words, even if the implemented polynomials are different in representation, we are able to automatically check their equivalence to the given AIG under modulo equivalence. Furthermore, if the two models are not equivalent, our decision procedure is able to automatically

correct the AIG according to the specification. This decision procedure can be used as a theory for SMT solvers targeting non-linear arithmetic circuits. We evaluate our approach on several large arithmetic circuits thereby showing performance benefits of many orders of magnitude than widely accepted industrial techniques.

Keywords: Arithmetic circuit, multiplier, Decision Diagram, debug, correction, carry logic

Full Paper:
http://www.hldvt.com/

See also: Proceedings of IEEE International High Level Design Validation and Test Workshop 2009

Propelling Satisfiability-solvers with application-specific encoding

Malay K. Ganai (NEC Laboratories America, Inc. - Princeton, US)

SAT/SMT solvers are widely adopted engines for solving decision problems arising from various applications. These solvers are mostly heuristic-driven, and are able to achieve their feats for reasonably-sized problems. However, these heuristics are often inadequate in meeting the required performance as needed in many of the key applications. Some such applications are software (sequential and concurrent) model checking, decision procedures for non-linear (real and integer) arithmetic, and parallelization in a distributed environment.

To address the issue, we discuss application-specific encoding and meta-level decision algorithms that propel the satisfiability solvers to continue show their feats. Specifically, we show that application-aware encoding can reduce the size of decision formula (i.e., simplification), remove functional redundancy (i.e., reduction), and reduce the search space (i.e., small domain encoding)–which a SAT solver, in general, may not be able to do so efficiently on a directly encoded formula.

Towards Model Validation and Verification with SAT Techniques

Martin Gogolla (Universität Bremen, DE)

After sketching how system development and the UML (Unified Modeling Language) and the OCL (Object Constraint Language) are related, validation and verification with the tool USE (UML-based Specification Environment) is demonstrated. As a more efficient alternative for verification tasks, two approaches using SAT-based techniques are put forward: First, a direct encoding of UML

and OCL with Boolean variables and propositional formulas, and second, an encoding employing an intermediate, higher-level language (KODKOD, stongly connected to ALLOY). A number of further, presently not realized verification and validation tasks and the transformation of higher-level modeling concepts into simple UML/OCL models, which are checkable with SAT-based techniques, are shortly discussed. Finally, the potential of SAT-based techniques for model development is again emphasized.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2507

Boundary Point Elimination: A Path to Structure Aware SAT-solvers

Eugene Goldberg (Northeastern Univ. - Boston, US)

Taking into account formula's structure is extremely important for making SAT-solvers scalable. One of the problems here is that a SAT solver with conflict clause learning creates its own structure (induced by conflicts) that may have little to do with the real structure of the formula. In particular, a single resolution is meaninglessïn a SAT-solver based on the DPLL procedure unless it is used in deriving a conflict clause. We describe a SAT-algorithm called IBP (Interpolation with Boundary Point elimination) that is not conflict driven and so builds a proof from ïndividualresolution operations. We show that IBP compares favorably with state- of-the-art SAT-solvers on narrow formulas. We also argue that IBP can be viewed as a generalization of the conflict clause generation procedure and so can be used to advance the state of the art in SAT-solvers based on the DPLL procedure.

Formal Verification of Abstract SystemC Models

Daniel Grosse (Universität Bremen, DE)

In this talk we present a formal verification approach for abstract SystemC models. The approach allows checking expressive properties and lifts induction known from bounded model checking to a higher level, to cope with the large state space of abstract SystemC programs. The technique is tightly integrated with our SystemC to C transformation and generation of monitoring logic to form a complete and efficient method. Properties specifying both hardware and software aspects, e.g. pre- and post-conditions as well as temporal relations of transactions and events, can be specified. As shown by experiments modern proof techniques allow verifying important non-trivial behavior. Moreover, our inductive technique gives significant speed-ups in comparison to simple methods.

Joint work of: Grosse, Daniel; Le, Hoang M.; Drechsler, Rolf

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2510

Control-based Clause Sharing in Parallel SAT Solving

Youssef Hamadi (Microsoft Research UK - Cambridge, GB)

Conflict driven clause learning allows clause sharing between multiple processing units working on related (sub-)problems. However, without limitation, sharing clauses might lead to an exponential blow up in communication or to the sharing of irrelevant clauses. This work, proposes two innovative policies to dynamically adjust the size of shared clauses between any pair of processing units. The first approach controls the overall number of exchanged clauses whereas the second additionally exploits the relevance quality of shared clauses. Experimental results show important improvements of the state-of the-art parallel SAT solver.

Keywords: Parallel SAT, multi-threading

Full Paper:
http://research.microsoft.com/en-us/people/youssefh/ijcai09-1.pdf

See also: Y. Hamadi, S. Jabbour, and L. Sais, Twenty-first International Joint Conference on Artificial Intelligence (IJCAI'09), July 2009, Pasadena, USA.

Minimal Model Generation with MGTP and DPLL

Ryuzo Hasegawa (Kyushu University, JP)

Minimal model generation is a technique to prune nonminimal models and redundant branches dynamically.

Several methods for it were proposed within the framework of model generation or tableaux:

Bry & Yahya presented a procedure for generating minimal models by means of *complement splitting* and constrained search with *model constraint*; Niemelä presented a *groundedness test* for checking minimality without using model constraints.

Both methods, however, may perform unnecessary minimality tests and cannot prune all redundant branches.

To overcome these problems, we presented a method that employs *branching assumptions* and *branching lemmas* .

The above methods can also be applied to the DPLL procedure, which has been widely used in practical SAT applications.

In DPLL, giving priority to negative branching corresponds to complement splitting.

Furthermore, our framework of minimal model generation can be easily extended to circumscription, that is generating minimal models with respect to a specific atom set.

We have implemented two types of minimal model generation systems MM-MGTP and MM-Minisat, using a model generation based prover MGTP in Java and a DPLL based SAT solver Minisat in C.

Preliminary experimental results obtained by running them on SAT benchmarks show the following:

MM-MGTP outperforms MM-Minisat for the Industrial and MM categories, while MM-Minisat outperforms MM-MGTP for the Random category.

Moreover, they are comparable to each other for the Crafted category.

Keywords: Minimal model generation, MGTP, DPLL, SAT benchmarks

Joint work of: Hasegawa, Ryuzo; Fujita, Hiroshi; Koshimura, Miyuki

Device emulation code generation - an unusual application for SMT

Thomas Heinz (Robert Bosch GmbH - Schwieberdingen, DE)

Binary translation is a promising method to automatically retarget embedded software such that it can be executed on another platform than it was originally designed for. A particular problem occurring within this scope is device emulation where accesses to a particular microcontroller peripheral such as a CAN controller must be translated into equivalent accesses to a similar device, e.g. another CAN controller (integrated in a different microcontroller) which is programmed in a different way.

This talk shows how SMT for fixed width bit vector arithmetic is useful to formalize a semantics of device accesses which enables automatic device emulation code generation based on device specifications of a source and a corresponding target device given that they are sufficiently similar.

Blocked Clause Elimination

Matti Jaervisalo (University of Helsinki, FI)

Boolean satisfiability (SAT) and its extensions are becoming a core technology for the analysis of systems. The SAT-based approach divides into three steps: encoding, preprocessing, and search. It is often argued that by encoding arbitrary Boolean formulas in conjunctive normal form (CNF), structural properties of the original problem are not reflected in the CNF. This should result in the fact that CNF-level preprocessing and SAT solver techniques have an inherent disadvantage compared to related techniques applicable on the level of more structured SAT instance representations such as Boolean circuits. In this work we study the effect of a CNF-level simplification technique called blocked clause elimination (BCE). We show that BCE is surprisingly effective both in theory and in practice on CNFs resulting from a standard CNF encoding for circuits:

without explicit knowledge of the underlying circuit structure, it achieves the same level of simplification as a combination of circuit-level simplifications and previously suggested polarity-based CNF encodings. Experimentally, we show that by applying BCE in preprocessing, further formula reduction and faster solving can be achieved, giving promise for applying BCE for speeding up solvers.

Joint work of: Järvisalo, Matti; Biere, Armin; Heule, Marijn

Hybrid SAT solving using reference points

Stephan Kottler (Universität Tübingen, DE)

Conflict driven SAT solvers with clause learning (CDCL) have become vastly successful for SAT instances arising from real-world applications. However, slight differences in the algorithm or just only a bad initial random seed may turn instances from hard to easy and vice versa.

The concept of restarts tries to overcome this drawback by giving the solver the chance to escape from bad parts of the search tree. Usually at a restart the partial assignment is completely rejected even though it might be very close to a solution. Our hybrid approach uses the idea of reference points to analyse partial assignments before completely rejecting them. This turns out to improve solving performance and reliability for some families of instances, both satisfiable and unsatisfiable ones.

Keywords: Hybrid, Reference Point, DMRP

Parallel SAT/QBF Solving and Applications

Matthew Lewis (Universität Freiburg, DE)

In our talk we will give an overview of the parallel SAT & QBF solvers developed at the Chair of Computer Architecture, and present how these solvers have been integrated into our in-house ATPG, BMC, and Black Box Verification tools (joint presentation of Matthew Lewis / Tobias Schubert).

Joint work of: Lewis, Matthew; Schubert, Tobias

Making a QBF Solver ready for new computer architectures

Paolo Marin (University of Genova, IT)

In this talk I will give an overview of the techniques developed into our QBF Preprocessor and Solver. I will also present its parallel version and the problems arising when running sequential and parallel Solvers on new architecture computer such as multi-cores.

Keywords: QBF, Preprocessor, Parallel Solver

Joint work of: Marin, Paolo; Giunchiglia, Enrico; Narizzano, Massimo; Lewis, Matthew; Schubert, Tobias; Becker, Bernd

AIGSolve - An AIG-Based QBF Solver

Florian Pigorsch (Universität Freiburg, DE)

In this talk we present our QBF solver AIGSolve, which relies on AIGs (And-Inverter Graphs) for compactly representing QBF formulas instead of using a CNF based data-structure, allowing for the application of efficient symbolic quantifier elimination techniques.

Moreover, the solver makes extensive use of structural information extracted from the input formula, such as functional definitions of variables, which can directly be exploited in the symbolic, AIG based representation.

Experimental results prove the effectiveness of our approach and show that our solver is able to outperform other state-of-the-art solvers on a representative set of benchmarks.

Keywords: Quantified Boolean Formulas, And-Inverter Graphs

Beyond classical clause learning

Lakhdar Sais (Université d'Artois - Lens, FR)

In this talk we present several contributions to Conflict Driven Clause Learning (CDCL), which is one of the key components of modern SAT solvers. First, we propose an extended notion of implication graph containing additional arcs, called inverse arcs. These are obtained by taking into account the satisfied clauses of the formula, which are usually ignored by conflict analysis. Secondly, we present an original adaptation of conflict analysis for dynamic clauses subsumption. Our last contribution demonstrates that clause learning can be exploited at each step of the search process, even if a conflict do not occurs. This last contribution aims to derive new but more powerful reasons leading to the implication of a given literal. For all these contributions, we discuss their possible integration to modern SAT solvers.

Keywords: SAT, clause learning, modern SAT solvers

Full Paper:
http://www.cril.fr/~sais

The Reveal Turn-Key Formal Verification System

Karem A. Sakallah (University of Michigan, US)

Reveal is a formal functional verification system. It employs counterexample-guided abstraction refinement, or CEGAR, and is suitable for verifying the complex control logic of designs with wide datapaths. Reveal performs automatic datapath abstraction yielding an approximation of the original design with a much smaller state space. This approximation is subsequently used to verify the correctness of control logic interactions. If the approximation proves to be too coarse, it is automatically refined based on the spurious counterexample it generates. Such refinement can be viewed as a form of on-demand "learning" similar in spirit to conflict-based learning in modern Boolean satisfiability solvers. The abstraction/refinement process is iterated until the design is shown to be correct or an actual design error is reported. The Reveal system allows some user control over the abstraction and refinement steps. Reveal has been demonstrated on a variety of publicly-available benchmarks as well as some proprietary industrial designs. Reveal is currently being prepared for commercialization through a start-up company by the same name.

Keywords: Datapath bstraction, refinement, CEGAR, formal verification

Joint work of: Andraus, Zaher S.; Sakallah, Karem A.

Answer Set Programming, the Solving Paradigm for Knowledge Representation and Reasoning

Torsten Schaub (Universität Potsdam, DE)

Answer Set Programming (ASP) is a declarative problem solving approach, combining a rich yet simple modeling language with high-performance solving capacities.

ASP allows for solving all search problems in NP (and NP^{NP}) in a uniform way (being more compact than SAT).

Applications of ASP include automatic synthesis of multiprocessor systems, decision support systems for NASA shuttle controllers, reasoning tools in systems biology, and many more.

The versatility of ASP is also reflected by the ASP solver clasp, developed at the University of Potsdam, and winning first places at ASP'09, PB'09, and SAT'09.

Keywords: Answer Set Programming, Knowledge Representation

Using SMT for Optimizing Symbolic Representations

Christoph Scholl (Universität Freiburg, DE)

We present an SMT (Satisfiability Modulo Theories) based method which commputes optimized representations for non-convex polyhedra.

The approach is applied in the context of model checking for Linear Hybrid Automata where both the discrete part and the continuous part of the hybrid state space are represented by one symbolic representation called LinAIGs. This symbolic representation is especially well-suited for hybrid systems with large discrete state spaces (where an explicit representation of discrete states is difficult).

Our method detects so-called redundant linear constraints in these representations by using an incremental SMT solver and then removes the redundant constraints based on Craig interpolation.

The method provides an essential step making quantifier elimination for linear arithmetic much more efficient.

Finally, for hybrid system verification we briefly present 'constraint minimization' which further optimizes non-convex polyhedra by exploiting the fact that states already reached in previous steps can be interpreted as 'don't cares' in the current step.

Abandoning Prenex Clausal Normal Form in QBF Solving

Martina Seidl (TU Wien, AT)

In the last decades, a wealth of successful QSAT solvers has been developed. However, most of these solvers process formulas only in prenex conjunctive normal form (PCNF). As for many practical applications encodings into QBFs usually do not result in PCNF formulas, a further transformation step is necessary. This transformation often introduces new variables and disrupts the structure of the formula.

We briefly discuss the disadvantages of prenex conjunctive normal form and describe an alternative way to process QBFs without the drawbacks of the normal form transformations. We briefly describe our solver, qpro, which is able to handle formulas in negation normal form. To this end, we extend algorithms for QBFs to the non-normal form case. Especially, we generalize well-known pruning concepts to the non-clausal case. In order to prove properties of the algorithms generalized to non-clausal form, we use a sequent-style reconstruction of DPLL.

Keywords: Quantified Boolean Formulas, Negation Normal Form

Next generation must be understood: Predicting learnt clauses quality may be a first step in this direction

Laurent Simon (INRIA - Orsay, FR)

Beside impressive progresses made by SAT solvers over the last ten years, only few works tried to understand why Conflict Directed Clause Learning algorithms (CDCL) are so strong and efficient on most industrial applications. We report in this work a key observation of CDCL solvers behavior on this family of benchmarks and explain it by an unsuspected side effect of their particular Clause Learning scheme. This new paradigm allows us to solve an important, still open, question: How to designing a fast, static, accurate, and predictive measure of new learnt clauses pertinence.

Joint work of: Simon, Laurent; Audemard, Gilles

Visualizing and Exploiting the Structure of Real-World SAT Instances

Carsten Sinz (KIT - Karlsruhe, DE)

Today's SAT solvers can handle real-world instances of considerable size, whereas many much smaller (hard) instances still cannot be solved. The reason for this dichotomy is often attributed to the structure inherent in real-world problems.

By visualizing graph representations of real-world SAT instances further information on this internal structure can be obtained.

In this talk we discuss on-going research on how the structure may be exploited.

Keywords: Visualization, real-world SAT instances, graph layout

Integrating conjectured information in SAT solving using hints

Ofer Strichman (Technion - Haifa, IL)

We consider the problem of using conjectured information in SAT solving. The goal is to use this information for speeding up the search without losing soundness in case the conjecture is wrong.

Keywords: SAT solving, hints

On the Relation of OBDD-based and Resolution-based Proof Systems

Olga Tveretina (KIT - Karlsruhe, DE)

Many of the algorithms for satisfiability testing are based either on resolution or on Ordered Binary Decision Diagrams (OBDDs). In my talk I will present proof systems based on OBDDs [Atserias, Kolatis, Vardi] and compare the efficiency of these proof systems with proof systems based on resolution and extended resolution.

Solving hard instances in QF-BV combining Boolean reasoning with computer algebra

Markus Wedler (TU Kaiserslautern, DE)

We present ideas for integrating techniques from Boolean reasoning (SAT), computer algebra (CA) and arithmetic bit level reasoning (ABL) into an SMT-solver for the quantifier free logic over bit vectors (QF-BV).

In particular, we use normal form computation for polynomials over finite Rings $Z/2^n$ with respect to a Gröbner basis. This technique simplify the arithmetic problem parts of the SMT-instances significantly and allows for solving hard problems originating from functional hardware verification.

In order to cope with local hand-crafted optimizations of arithmetic components which are conducted at the gate level, we extract an equivalent circuit description at the arithmetic bit level. The extraction is based on local Reed-Muller forms.

Finally, the simplified SMT-Instance is bit-blasted and handeled by SAT.

Preliminary results obtained with our solver STABLE indicate that the presented techniques scale, such that industrial problems can be solved.

Keywords: Gröbner Basis Theory over finite rings, SMT, SAT, arithmetic bit level extraction

Joint work of: Wedler, Markus; Pavlenko, Evgeny; Dreyer, Alexander; Seelisch, Frank; Stoffel, Dominik; Greuel, Gert-Martin; Kunz, Wolfgang

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2509

From SAT to Saturation Based First-Order Decision Procedures and Back

Christoph Weidenbach (MPI für Informatik - Saarbrücken, DE)

The talk is a survey of recently developed saturation based calculi that serve as decision procedures for and beyond propositional logic.

The logics include finite domain first-order logic with or without equality as well as fragments with infinite domain structures.

SWORD – Module-based SAT Solving

Robert Wille (Universität Bremen, DE)

In the talk SWORD is described – a decision procedure for bit-vector logic that uses SAT techniques and exploits word level information. The main idea of SWORD is based on the following observation: While current SAT solvers perform very well on instances with a large number of logic operations, their performance on arithmetic operations degrades with increasing data-path width. In contrast, pure word-level approaches are able to handle arithmetic operations very fast, but suffer from irregularities in the word-level structure (e.g. bit slicing). SWORD tries to combine the best of both worlds: On the one hand, it includes fast propagation, sophisticated data structures, as well as advanced techniques like non-chronological backtracking and learning from modern SAT solvers. On the other hand word-level information is exploited in the decision heuristic and during propagation. Applications in circuit verification and logic synthesis show how the combination of Boolean and word level can be utilized during the solve process.

Joint work of: Wille, Robert; Jung, Jean Christoph; Sülflow, André; Drechsler, Rolf

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2506