Journal of Universal Computer Science, vol. 10, no. 12 (2004), 1559-1561
submitted: 16/12/04, accepted: 22/12/04, appeared: 28/12/04 © J.UCS

Tuning SAT for Formal Verification and Testing
J.UCS Special Issue

Miroslav N. Velev
(Reservoir Labs, New York, NY, U.S.A.
velev@reservoir.com)

During the last four years, tremendous progress was made in the field of Boolean Satisfiability (SAT). Now SAT solvers are 3 to 4 orders of magnitude faster, and can solve formulas that are 3 to 4 orders of magnitude bigger. SAT methods are critical to Electronic Design Automation (EDA) tool flows for state-of-the-art microprocessors. SAT-based techniques are the enabling technology behind formal verification—the mathematical proof that a design is implemented correctly. Statistics from recent cutting-edge microprocessors indicate that up to 70% of the engineering effort is spent on verification, which increasingly becomes the bottleneck when developing new products. Formal verification, presently gaining wider acceptance in industry, has the potential to significantly reduce the design time, while also guaranteeing complete correctness and avoiding costly design bugs—as expensive as 500 million dollars in the Intel Pentium processor. The five papers in this special issue present recent exciting work on tuning SAT for formal verification and testing.

In the first paper, entitled *MINCE: A Static Global Variable-Ordering Heuristic for SAT Search and BDD Manipulation*, Fadi Aloul from the American University of Sharjah (U.A.E.), and Igor Markov and Karem Sakallah from the University of Michigan (U.S.A.) present a static variable-ordering heuristic that operates on Boolean formulas in Conjunctive Normal Form (CNF). The derived variable order can be used in any SAT procedure, such as a SAT solver or a Binary Decision Diagram (BDD) package. Experimental results indicate that the proposed heuristic often outperforms existing state-of-the-art heuristics by a factor of 2 or more.

The second paper, *Using Global Structural Relationships of Signals to Accelerate SAT-based Combinational Equivalence Checking*, is by Rajat Arora from Cadence Design Systems (U.S.A.) and Michael Hsiao from Virginia Tech (U.S.A.). They perform static analysis of gate-level circuits by applying indirect and extended backward implications in order to identify implications between pairs of signals. Such implications are added as 2-literal clauses to the CNF formula derived from the gate-level circuit. Experimental results show that the added implications help to prune the search space and result in up to an order of magnitude speedup when checking the equivalence of combinational circuits.

The third paper, *A Signal Correlation Guided Circuit-SAT Solver*, is by Feng Lu, Li-C. Wang, and Kwang-Ting (Tim) Cheng from the University of California at Santa Barbara (U.S.A.), and John Moondanos and Ziyad Hanna from Intel Corporation (U.S.A.). The authors use random simulation to identify possible correlations between pairs of signals. Then they apply two heuristics to derive conflict clauses by having a

gate-level SAT solver make decisions that are likely to result in a conflict, based on the circuit behavior under random simulation. The derived conflict clauses reduce the search space and result in up to 2 orders of magnitude speedup when solving instances from combinational equivalence checking of complex Intel circuits.

The fourth paper is entitled *Function-Complete Lookahead in Support of Efficient SAT Search Heuristics* and is by John Franco, Michal Kouril, John Schlipf, and Sean Weaver from the University of Cincinnati (U.S.A.), and Michael Dransfield, and W. Mark Vanfleet from the National Security Agency (U.S.A.). They have combined BDDs and search methods to implement efficient decision heuristics by exploiting information collected in a preprocessing step. This approach outperformed existing state-of-the-art SAT solvers by more than 4 times when SAT-solving complex formulas from Bounded Model Checking (BMC), and scaled for formulas that the existing SAT solvers could not handle.

The fifth and final paper is *Improving SAT-based Bounded Model Checking by Means of BDD-based Approximate Traversals*. The authors are Gianpiero Cabodi, Sergio Nocco, and Stefano Quer from Politecnico di Torino (Italy). They combine BDD and SAT methods to increase the efficiency of BMC. That is done by applying BDD-based symbolic approximate reachability analysis to collect information about the model. This information is used to restrict the search space of a SAT-based BMC. The approach sped up BMC runs by up to 30 times.

The following 36 colleagues helped review papers submitted to the special issue:

Fadi Aloul, American University in Dubai, United Arab Emirates
Armin Biere, ETH Zürich, Switzerland
Roderick Bloem, Graz University of Technology, Austria
Gilles Dequen, LaRIA, France
Tao Feng, University of California at Santa Barbara, U.S.A.
John Franco, University of Cincinnati, U.S.A.
Eugene Goldberg, Cadence Berkeley Labs, U.S.A.
Michael Hsiao, Virginia Tech, U.S.A.
Madhu Iyer, University of California at Santa Barbara, U.S.A.
Rune M. Jensen, IT University of Copenhagen, Denmark
HoonSang Jin, University of Colorado at Boulder, U.S.A.
Priyank Kalla, University of Utah, U.S.A.
Oliver Kullmann, University of Wales Swansea, the U.K.
Daniel Le Berre, CRIL-CNRS, Université d'Artois, France
Matthew Lewis, Albert-Ludwigs-Universität, Freiburg, Germany
Inês Lynce, Technical University of Lisbon, Portugal
Igor L. Markov, University of Michigan, U.S.A.
João Marques-Silva, Technical University of Lisbon, Portugal
In-Ho Moon, Synopsys, U.S.A.
Alexander Nadel, Tel Aviv University, Israel
Yakov Novikov, Konrad-Zuse-Zentrum für Informationstechnik Berlin, Germany
Mukul Prasad, Fujitsu, U.S.A.
Stefano Quer, Politecnico di Torino, Italy
T. L. Rajaprabhu, University of Bristol, the U.K.

Kavita Ravi, Cadence, U.S.A.
Sherief Reda, University of California at San Diego, U.S.A.
Jussi Rintanen, Albert-Ludwigs-Universität Freiburg, Germany
Jarrod Roy, University of Michigan at Ann Arbor, U.S.A.
Lawrence Ryan, Synopsys, U.S.A.
Sathiamoorthy Subbarayan, IT University of Copenhagen, Denmark
Allen Van Gelder, University of California at Santa Cruz, U.S.A.
Toby Walsh, University College Cork, Ireland
Chao Wang, University of Colorado at Boulder, U.S.A.
Emmanuel Zarpas, IBM Haifa Research Lab, Israel
Hantao Zhang, University of Iowa, U.S.A.
Lintao Zhang, Microsoft Research Silicon Valley Lab, U.S.A.

On behalf of the Editorial Board of the Journal of Universal Computer Science, I thank the authors for their contributions, and the reviewers for their insightful comments. The five papers are representative of the recent exciting advances in the field of SAT and its applications to formal verification and testing.

New York, NY, U.S.A. Miroslav N. Velev,
December 2004 Reservoir Labs