João Marques-Silva
Karem A. Sakallah (Eds.)

LNCS 4501

# Theory and Applications of Satisfiability Testing – SAT 2007

10th International Conference
Lisbon, Portugal, May 2007
Proceedings

Springer

João Marques-Silva Karem A. Sakallah (Eds.)

# Theory and Applications of Satisfiability Testing – SAT 2007

10th International Conference
Lisbon, Portugal, May 28-31, 2007
Proceedings

Springer

Volume Editors

João Marques-Silva
University of Southampton
School of Electronics and Computer Science
Highfield, Southampton, S017 1BJ, UK
E-mail: jpms@ecs.soton.ac.uk

Karem A. Sakallah
University of Michigan
Department of Electrical and Computer Science
4603 CSE Building, 2260 Hayward Ave, Ann Arbor, MI 48109-2121, USA
E-mail: karem@umich.edu

Library of Congress Control Number: 2007927094

CR Subject Classification (1998): F.4.1, I.2.3, I.2.8, I.2, F.2.2, G.1.6

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-72787-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-72787-3 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12069392 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4501

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

# Preface

This volume contains the papers presented at SAT 2007: 10th International Conference on Theory and Applications of Satisfiability Testing.

The International Conferences on Theory and Applications of Satisfiability Testing (SAT) originated in 1996 as a series of workshops "on Satisfiability." By the third meeting in 2000, the workshop had attracted a mix of theorists and experimentalists whose common interest was the enhancement of our basic understanding of the theoretical underpinnings of the Satisfiability problem as well as the development of scalable algorithms for its solution in a wide range of application domains. In 2002 a competition of SAT solvers was inaugurated to spur further algorithmic and implementation developments, and to create an eclectic collection of benchmarks. The competition—expanded in subsequent years to include pseudo Boolean, QBF, and MAX-SAT solvers—has become an integral part of these meetings, adding an element of excitement and anticipation. The interplay between theory and application, as well as the increased interest in Satisfiability from a wider community of researchers, led to the natural evolution of these initial workshops into the current conference format. The annual SAT conference is now universally recognized as "the venue" for publishing the latest advances in SAT research.

This year marks the tenth SAT meeting. SAT is now interpreted in a broad sense to include not just propositional satisfiability, but also pseudo-Boolean constraint solving and optimization (PB), quantified Boolean formulae (QBF), constraint programming techniques (CP) for word-level problems and their propositional encoding, and satisfiability modulo theories (SMT). Submissions were solicited for original research on proof systems and proof complexity, search algorithms and heuristics, analysis of algorithms, hard instances, randomized formulae, problem encodings, industrial applications, solvers, simplifiers and tools, case studies and empirical results. A total of 74 submissions were received and rigorously reviewed by a 35-member international Technical Program Committee (TPC), with each paper receiving at least four independent reviews. Of these submissions, the TPC decided to accept 22 as regular papers (14 pages, 25-minute presentation) and 12 as short papers (6 pages, 12-minute presentation). The accepted papers were organized into nine sessions and their full text is included in these proceedings.

The conference program also featured two invited presentations. The first, by Martin Davis, chronicled the original development of the "DPLL" algorithm and proposed an unorthodox take on the P=NP problem. The second, by Andrei Voronkov, addressed new encodings that enable succinct representations of certain combinatorial problems in the Bernays – Schonfinkel fragment of first-order logic.

A number of additional events were associated with the SAT conference, including the SAT competition, the QBF evaluation, the PB evaluation, the MAX-SAT evaluation, and a special session on trends in modern SAT solvers.

We would like to acknowledge several people for their help: the SAT Local Chair, Ines Lynce; the organizers of the SAT competition, Daniel Le Berre, Laurent Simon, Ewald Speckenmeyer, Geoff Sutcliffe and Lintao Zhang; the organizers of the QBF evaluation, Massimo Narizzano, Luca Pulina and Armando Tacchella; the organizers of the PB evaluation, Vasco Manquinho and Olivier Roussel; and finally the organizers of the Max-SAT evaluation, Josep Argelich, Chu-Min Li, Felip Manyà and Jordi Planes. Last, but not least, we thank the Program Committee and the additional external reviewers for their careful and thorough work, without which it would not have been possible for us to put together such a high-quality conference program.

We also thank Andrei Voronkov for the EasyChair system. EasyChair was instrumental in handling of paper submissions, paper reviewing, paper discussion, and assembly of the proceedings. Finally, we would like to thank the following sponsors for their generous support of SAT 2007: Cadence Design Systems, Cornell's Intelligent Information Systems Institute, Intel Corporation, Luso-American Foundation, Magma Design Automation, Microsoft Corporation, NEC Laboratories, and Synopsys Inc. A number of other institutions provided critical logistical support for managing the organization of the conference: INESC-ID, Instituto Superior Técnico, the University of Michigan, and the University of Southampton.

May 2007

Joao Marques-Silva
Karem Sakallah

# Organization

## Conference Chairs

Joao Marques-Silva
Karem Sakallah

## Local Chair

Ines Lynce

## Technical Program Committee

Fahiem Bacchus
Paul Beame
Armin Biere
Adnan Darwiche
Leonardo de Moura
Niklas Een
John Franco
Ian Gent
Enrico Giunchiglia
Carla Gomes
Aarti Gupta
Ziyad Hanna
Edward Hirsch
Joonyoung Kim
Hans Kleine-Büning
James Kukula
Oliver Kullmann
Daniel Le Berre
Chu-Min Li
Ines Lynce
Panagiotis Manolios
Vasco Manquinho
Slawomir Pilarski
Steve Prestwich
Roberto Sebastiani
Hossein Sheini
Laurent Simon
Ewald Speckenmeyer
Ofer Strichman
Stefan Szeider
Armando Tacchella
Allen Van Gelder
Hans van Maaren
Toby Walsh
Lintao Zhang

## External Reviewers

Dimitris Achlioptas
Johan Alfredsson
Fadi Aloul
Anbulagan Anbulagan
Josep Argelich
Gilles Audemard
Ritwik Bhattacharya
Jesse Bingham
Per Bjesse
Nikolaj Bjorner
Roberto Bruttomesso
Uwe Bubeck
Arthur Choi
Alessandro Cimatti
Stefan Dantchev
Jessica Davies
Gilles Dequen
Laure Devendeville
Peter Dillinger
Kutsy Ekaterina
Yulik Feldman
Anders Franzen
Zhaohui Fu
Roman Gershman
Eugene Goldberg
Dan Goldwasser
Alberto Griggio
Marijn Heule
Jinbo Huang
Dmitry Itsykson
Attila Jurecska
Toni Jussila
Zurab Khasidashvili
Matthew Kitching
Arist Kojevnikov
Andrei Krokhin
Alexander Kulikov
Elitza Maneva
Felip Manya

Marco Maratea
Igor Markov
Arie Matsliah
Bertrand Mazure
Thomas Meyer
Alan Mishchenko
António Morgado
Alexander Nadel
Naren Narasimhan
Massimo Narizzano
Peter Nightingale
Sergey Nikolenko
Cedric Piette
Knot Pipatsrisawat
Stefan Porschen
Olivier Roussel
Bert Randerath
Federico Ricci-Tersenghi
Michael Ryavchev
Vadim Ryvchin
Ashish Sabharwal
Marko Samer
Horst Samulowitz
Tian Sang
Carsten Sinz
Sudarshan Srinivasan
Ted Stanion
Baruch Sterin
Peter Stuckey
Niklas Sörensson
Heather Trumbower
Bubeck Uwe
Michael Veksler
Michele Vescovi
Daron Vroon
Sean Weaver
Wanxia Wei
Jesse Whittemore
Hans Zantema

## Sponsoring Institutions

Cadence Design Systems
Intel Corp.
Intelligent Information Systems Institute, Cornell
Luso-American Foundation
Magma Design Automation
Microsoft Research
NEC Research Laboratories
Synopsys Inc.
INESC-ID
Instituto Superior Técnico
The University of Michigan
The University of Southampton

Printing: Mercedes-Druck, Berlin
Binding: Stein + Lehmann, Berlin

# Lecture Notes in Computer Science

For information about Vols. 1–4396

please contact your bookseller or Springer

Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y. Park, L.T. Yang, S.W. Kim (Eds.), Embedded Software and Systems. XIX, 829 pages. 2007.

Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 382 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4514: S.N. Artemov, A. Nerode (Eds.), Logical Foundations of Computer Science. XI, 513 pages. 2007.

Vol. 4510: P. Van Hentenryck, L. Wolsey (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 391 pages. 2007.

Vol. 4509: Z. Kobti, D. Wu (Eds.), Advances in Artificial Intelligence. XII, 552 pages. 2007. (Sublibrary LNAI).

Vol. 4506: D. Zeng, I. Gotham, K. Komatsu, C. Lynch, M. Thurmond, D. Madigan, B. Lober, J. Kvach, H. Chen (Eds.), Intelligence and Security Informatics: Biosurveillance. XI, 234 pages. 2007.

Vol. 4504: J. Huang, R. Kowalczyk, Z. Maamar, D. Martin, I. Müller, S. Stoutenburg, K.P. Sycara (Eds.), Service-Oriented Computing: Agents, Semantics, and Engineering. X, 175 pages. 2007.

Vol. 4501: J. Marques-Silva, K.A. Sakallah (Eds.), Theory and Applications of Satisfiability Testing – SAT 2007. XI, 384 pages. 2007.

Vol. 4500: N. Streitz, A. Kameas, I. Mavrommati (Eds.), The Disappearing Computer. XVIII, 307 pages. 2007.

Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part III. XXVI, 1215 pages. 2007.

Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part II. XXVII, 1321 pages. 2007.

Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part I. LIV, 1365 pages. 2007.

Vol. 4490: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part IV. XXXVII, 1211 pages. 2007.

Vol. 4489: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part III. XXXVII, 1257 pages. 2007.

Vol. 4488: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part II. XXXV, 1251 pages. 2007.

Vol. 4487: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part I. LXXXI, 1275 pages. 2007.

Vol. 4486: M. Bernardo, J. Hillston (Eds.), Formal Methods for Performance Evaluation. VII, 469 pages. 2007.

Vol. 4484: J.-Y. Cai, S.B. Cooper, H. Zhu (Eds.), Theory and Applications of Models of Computation. XIII, 772 pages. 2007.

Vol. 4483: C. Baral, G. Brewka, J. Schlipf (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4482: A. An, J. Stefanowski, S. Ramanna, C.J. Butz, W. Pedrycz, G. Wang (Eds.), Rough Sets, Fuzzy Sets, Data Mining and Granular Computing. XIV, 585 pages. 2007. (Sublibrary LNAI).

Vol. 4481: J. Yao, P. Lingras, W.-Z. Wu, M. Szczuka, N.J. Cercone, D. Ślęzak (Eds.), Rough Sets and Knowledge Technology. XIV, 576 pages. 2007. (Sublibrary LNAI).

Vol. 4480: A. LaMarca, M. Langheinrich, K.N. Truong (Eds.), Pervasive Computing. XIII, 369 pages. 2007.

Vol. 4479: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C.d. Oliveira, J. McNair (Eds.), NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. XXVII, 1252 pages. 2007.

Vol. 4472: M. Haindl, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XI, 524 pages. 2007.

Vol. 4471: P. Cesar, K. Chorianopoulos, J.F. Jensen (Eds.), Interactive TV: a Shared Experience. XIII, 236 pages. 2007.

Vol. 4470: Q. Wang, D. Pfahl, D.M. Raffo (Eds.), Software Process Dynamics and Agility. XI, 346 pages. 2007.

Vol. 4465: T. Chahed, B. Tuffin (Eds.), Network Control and Optimization. XIII, 305 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4463: I. Măndoiu, A. Zelikovsky (Eds.), Bioinformatics Research and Applications. XV, 653 pages. 2007. (Sublibrary LNBI).

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4459: C. Cérin, K.-C. Li (Eds.), Advances in Grid and Pervasive Computing. XVI, 759 pages. 2007.

Vol. 4453: T. Speed, H. Huang (Eds.), Research in Computational Molecular Biology. XVI, 550 pages. 2007. (Sublibrary LNBI).

Vol. 4452: M. Fasli, O. Shehory (Eds.), Agent-Mediated Electronic Commerce. VIII, 249 pages. 2007. (Sublibrary LNAI).

Vol. 4451: T.S. Huang, A. Nijholt, M. Pantic, A. Pentland (Eds.), Artifical Intelligence for Human Computing. XVI, 359 pages. 2007. (Sublibrary LNAI).

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4448: M. Giacobini et al. (Ed.), Applications of Evolutionary Computing. XXIII, 755 pages. 2007.

Vol. 4447: E. Marchiori, J.H. Moore, J.C. Rajapakse (Eds.), Evolutionary Computation,Machine Learning and Data Mining in Bioinformatics. XI, 302 pages. 2007.

Vol. 4446: C. Cotta, J. van Hemert (Eds.), Evolutionary Computation in Combinatorial Optimization. XII, 241 pages. 2007.

Vol. 4445: M. Ebner, M. O'Neill, A. Ekárt, L. Vanneschi, A.I. Esparcia-Alcázar (Eds.), Genetic Programming. XI, 382 pages. 2007.

Vol. 4444: T. Reps, M. Sagiv, J. Bauer (Eds.), Program Analysis and Compilation, Theory and Practice. X, 361 pages. 2007.

Vol. 4443: R. Kotagiri, P.R. Krishna, M. Mohania, E. Nantajeewarawat (Eds.), Advances in Databases: Concepts, Systems and Applications. XXI, 1126 pages. 2007.

Vol. 4440: B. Liblit, Cooperative Bug Isolation. XV, 101 pages. 2007.

Vol. 4439: W. Abramowicz (Ed.), Business Information Systems. XV, 654 pages. 2007.

Vol. 4438: L. Maicher, A. Sigel, L.M. Garshol (Eds.), Leveraging the Semantics of Topic Maps. X, 257 pages. 2007. (Sublibrary LNAI).

Vol. 4433: E. Şahin, W.M. Spears, A.F.T. Winfield (Eds.), Swarm Robotics. XII, 221 pages. 2007.

Vol. 4432: B. Beliczynski, A. Dzielinski, M. Iwanowski, B. Ribeiro (Eds.), Adaptive and Natural Computing Algorithms, Part II. XXVI, 761 pages. 2007.

Vol. 4431: B. Beliczynski, A. Dzielinski, M. Iwanowski, B. Ribeiro (Eds.), Adaptive and Natural Computing Algorithms, Part I. XXV, 851 pages. 2007.

Vol. 4430: C.C. Yang, D. Zeng, M. Chau, K. Chang, Q. Yang, X. Cheng, J. Wang, F.-Y. Wang, H. Chen (Eds.), Intelligence and Security Informatics. XII, 330 pages. 2007.

Vol. 4429: R. Lu, J.H. Siekmann, C. Ullrich (Eds.), Cognitive Systems. X, 161 pages. 2007. (Sublibrary LNAI).

Vol. 4427: S. Uhlig, K. Papagiannaki, O. Bonaventure (Eds.), Passive and Active Network Measurement. XI, 274 pages. 2007.

Vol. 4426: Z.-H. Zhou, H. Li, Q. Yang (Eds.), Advances in Knowledge Discovery and Data Mining. XXV, 1161 pages. 2007. (Sublibrary LNAI).

Vol. 4425: G. Amati, C. Carpineto, G. Romano (Eds.), Advances in Information Retrieval. XIX, 759 pages. 2007.

Vol. 4424: O. Grumberg, M. Huth (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XX, 738 pages. 2007.

Vol. 4423: H. Seidl (Ed.), Foundations of Software Science and Computational Structures. XVI, 379 pages. 2007.

Vol. 4422: M.B. Dwyer, A. Lopes (Eds.), Fundamental Approaches to Software Engineering. XV, 440 pages. 2007.

Vol. 4421: R. De Nicola (Ed.), Programming Languages and Systems. XVII, 538 pages. 2007.

Vol. 4420: S. Krishnamurthi, M. Odersky (Eds.), Compiler Construction. XIV, 233 pages. 2007.

Vol. 4419: P.C. Diniz, E. Marques, K. Bertels, M.M. Fernandes, J.M.P. Cardoso (Eds.), Reconfigurable Computing: Architectures, Tools and Applications. XIV, 391 pages. 2007.

Vol. 4418: A. Gagalowicz, W. Philips (Eds.), Computer Vision/Computer Graphics Collaboration Techniques. XV, 620 pages. 2007.

Vol. 4416: A. Bemporad, A. Bicchi, G. Buttazzo (Eds.), Hybrid Systems: Computation and Control. XVII, 797 pages. 2007.

Vol. 4415: P. Lukowicz, L. Thiele, G. Tröster (Eds.), Architecture of Computing Systems - ARCS 2007. X, 297 pages. 2007.

Vol. 4414: S. Hochreiter, R. Wagner (Eds.), Bioinformatics Research and Development. XVI, 482 pages. 2007. (Sublibrary LNBI).

Vol. 4412: F. Stajano, H.J. Kim, J.-S. Chae, S.-D. Kim (Eds.), Ubiquitous Convergence Technology. XI, 302 pages. 2007.

Vol. 4411: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 249 pages. 2007. (Sublibrary LNAI).

Vol. 4410: A. Branco (Ed.), Anaphora: Analysis, Algorithms and Applications. X, 191 pages. 2007. (Sublibrary LNAI).

Vol. 4409: J.L. Fiadeiro, P.-Y. Schobbens (Eds.), Recent Trends in Algebraic Development Techniques. VII, 171 pages. 2007.

Vol. 4407: G. Puebla (Ed.), Logic-Based Program Synthesis and Transformation. VIII, 237 pages. 2007.

Vol. 4406: W. De Meuter (Ed.), Advances in Smalltalk. VII, 157 pages. 2007.

Vol. 4405: L. Padgham, F. Zambonelli (Eds.), Agent-Oriented Software Engineering VII. XII, 225 pages. 2007.

Vol. 4403: S. Obayashi, K. Deb, C. Poloni, T. Hiroyasu, T. Murata (Eds.), Evolutionary Multi-Criterion Optimization. XIX, 954 pages. 2007.

Vol. 4401: N. Guelfi, D. Buchs (Eds.), Rapid Integration of Software Engineering Techniques. IX, 177 pages. 2007.

Vol. 4400: J.F. Peters, A. Skowron, V.W. Marek, E. Orłowska, R. Słowiński, W. Ziarko (Eds.), Transactions on Rough Sets VII, Part II. X, 381 pages. 2007.

Vol. 4399: T. Kovacs, X. Llorà, K. Takadama, P.L. Lanzi, W. Stolzmann, S.W. Wilson (Eds.), Learning Classifier Systems. XII, 345 pages. 2007. (Sublibrary LNAI).

Vol. 4398: S. Marchand-Maillet, E. Bruno, A. Nürnberger, M. Detyniecki (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 269 pages. 2007.

Vol. 4397: C. Stephanidis, M. Pieper (Eds.), Universal Access in Ambient Intelligence Environments. XV, 467 pages. 2007.

# Table of Contents

# SAT: Past and Future

Martin Davis

## Part I. Davis-Putnam: An Accidental Algorithm

During the summer of 1957, Hilary Putnam and I, both junior faculty, were attending an unprecedented month-long "institute" devoted to logic at Cornell University along with 82 other logicians. Our families were sharing a house and the two of us were together every day working together and separately on a number of things, but not on the satisfiability problem. After we had made some progress towards a negative solution of Hilbert's 10th Problem (H10: the question of the existence of an algorithm for determining whether a given polynomial equation has an integer solution), we were eager to continue collaborating. Our idea was to seek funding through my institution which was a branch of Rensselaer Polytechnic in Eastern Connecticut so Hilary and his family could escape steamy summers in Princeton for the attractive lakeside accommodations available in my locale. Not believing that anyone would pay us to work on H10, considered a super long shot, we patched together a proposal to investigate procedures for theorem-proving in first-order logic. Because it was too late for the usual funding agencies, following a tip we submitted our proposal to the National Security Agency. They funded it on condition that our report *not* mention them, and that we forget about first-order logic, and just concentrate on satisfiability. Our report, which was submitted at the end of the summer of 1958, contained all the procedures that were eventually combined in the algorithms later designated as DP and DPLL. During the summer of 1959, we were supported by the US Air Force Office of Scientific Research. We worked very hard on H10 and made some significant progress. But because our proposal had emphasized theorem-proving procedures, we hastily concocted one using some of the work from the previous summer, and submitted it to the JACM. That was the origin of Davis-Putnam. After I moved to New York, I wanted to see our procedure implemented, and NYU put two very talented student programmers at my disposal for the purpose: Donald Loveland (who later became one of my first doctoral students) and George Logemann. The crude search we implemented led to satisfiability questions involving thousands of clauses and the original DP swamped the memory of the IBM 704. So we replaced the "rule for eliminating propositional variables" (i.e. ground binary resolution) with the splitting rule giving the algorithm a "divide and conquer" form with instances waiting to be processed swapped out onto a tape. This was the DPLL algorithm.

## Part II. SAT $\notin P$?

Although everyone seems to believe that $P \neq NP$, the evidence is scant and somewhat circular. There is the fact that the problems for which good feasible worst-case algorithms are known, are solvable in poly-time. But in practice, "poly-time" really means $O(n \log n)$ or maybe $O(n^2)$ and with a manageable multiplicative constant. No-one would regard an algorithm that runs in time $10^{10^{10}} n^2$ or $O(n^{1000})$ as "feasible". But

J. Marques-Silva and K.A. Sakallah (Eds.): SAT 2007, LNCS 4501, pp. 1–2, 2007.

it is only the identification of poly-time computability with feasibility, in analogy with the identification of Turing computability with effective computability, that makes the existence of so many NP-complete problems seem to be evidence for $P \neq NP$. If there are horrendous poly-time algorithms for these NP-complete problems, how might we come to know it? Is anyone seeking such algorithms? Theorists have built their poly-time hierarchy in stages mimicking the arithmetic hierarchy of the logicians with $P$ at the bottom and $P$-SPACE at the top. But they have been unable to prove a single separation theorem between the levels. For all we know, the entire edifice could collapse with $P = P$-SPACE. Computer science is a very young subject. Mathematicians know from hard experience that problems easy to state can take hundreds of years to resolve. But theorists blithely conclude from an implication $A \Rightarrow P = NP$ that the proposition $A$ must be false. The case of linear programming provides a good example which can well resonate with experts on SAT. The very useful simplex method runs in exponential time in the worst case. It was thought for years that there is no poly-time algorithm for linear programming. Experts were astounded when it turned out that in fact poly-time algorithms for linear programming do exist. However, ironically enough in practice the old reliable exponential-time simplex method does better than these poly-time time algorithms. So what do we know about the question: Is SAT $\in P$? Almost nothing! It could go either way. But if it should turn out that the answer is "Yes", that would of course imply that $P = NP$, and so would entitle the person who succeeded in proving it to receive the million dollar prize the Clay Institute of Mathematics is offering. If I were 60 years younger, I'd be tempted to try!

# Encodings of Problems in Effectively Propositional Logic

Juan Antonio Navarro-Pérez and Andrei Voronkov

The University of Manchester
School of Computer Science
{navarroj,voronkov}@cs.manchester.ac.uk

Solving various combinatorial problems by their translation to the propositional satisfiability problem has become commonly accepted. By optimising such translations and using efficient SAT solvers one can often solve hard problems in various domains, such as formal verification and planning.

This approach to solving combinatorial problems is usually implemented by a translation procedure turning a formal description of the problem written in a domain-specific language $L$ (for example, SMV for model checking problems [3] or STRIPS [2] for planning problems) into a SAT problem. Such translation procedures share the following common features:

1. They contain many isomorphic or nearly isomorphic subsets of clauses obtained by the translation of the same expression of $L$.
2. The size of the resulting SAT problem is dominated by these copies.

In this talk the second author will present encodings able to specify some combinatorial problems, namely LTL bounded model checking [1] and planning within the Bernays-Schönfinkel fragment of first-order logic. This fragment, which also corresponds to the category of effectively propositional problems (EPR) of the CASC system competitions [4], allows a natural and succinct representation of both the transition systems corresponding to the problems and the property that one wants to verify, while avoiding the problem of creating isomorphic copies.

Our technique provides a rich collection of benchmarks with close links to real-life applications for the automated reasoning community and may boost development of new translation techniques and solvers for effectively propositional problems.

## References

[1] A. Biere, A. Cimatti, E.M. Clarke, and Y. Zhu. Symbolic model checking without BDDs. In R. Cleaveland, editor, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'99)*, volume 1579 of *Lecture Notes in Computer Science*, pages 193–207, 1999.

[2] R. Fikes and N.J. Nilsson. A new approach to the application of theorem proving to problem solving. *Artificial Intelligence*, 2(3/4):189–208, 1971.

[3] K.L. McMillan. *Symbolic Model Checking*. Kluwer, 1993.

[4] G. Sutcliffe and C.B. Suttner. The state of CASC. *AI Communications*, 19(1):35–48, 2006.

J. Marques-Silva and K.A. Sakallah (Eds.): SAT 2007, LNCS 4501, p. 3, 2007.