Enrico Giunchiglia
Armando Tacchella (Eds.)

LNCS 2919

Theory and Applications of Satisfiability Testing

6th International Conference, SAT 2003
Santa Margherita Ligure, Italy, May 2003
Selected Revised Papers

Springer

Enrico Giunchiglia Armando Tacchella (Eds.)

Theory and Applications of Satisfiability Testing

6th International Conference, SAT 2003
Santa Margherita Ligure, Italy, May 5-8, 2003
Selected Revised Papers

Springer

Volume Editors

Enrico Giunchiglia
Armando Tacchella
Università di Genova
DIST
Viale Causa 13, 16145 Genova, Italy
E-mail: giunchiglia@unige.it, tac@dist.unige.it

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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

ISSN 0302-9743
ISBN 3-540-20851-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10982143 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2919

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Lecture Notes in Computer Science

For information about Vols. 1–2849
please contact your bookseller or Springer-Verlag

Vol. 2802: D. Hutter, G. Müller, W. Stephan, M, Ullmann (Eds.), Security in Pervasive Computing. Proceedings, 2003. XI, 291 pages. 2004.

Vol. 2850: M.Y. Vardi, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. Proceedings, 2003. XIII, 437 pages. 2003. (Subseries LNAI)

Vol. 2851: C. Boyd, W. Mao (Eds.), Information Security. Proceedings, 2003. XI, 443 pages. 2003.

Vol. 2852: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. Proceedings, 2003. VIII, 509 pages. 2003.

Vol. 2853: M. Jeckle, L.-J. Zhang (Eds.), Web Services – ICWS-Europe 2003. Proceedings, 2003. VIII, 227 pages. 2003.

Vol. 2854: J. Hoffmann, Utilizing Problem Structure in Planning. XIII, 251 pages. 2003. (Subseries LNAI)

Vol. 2855: R. Alur, I. Lee (Eds.), Embedded Software. Proceedings, 2003. X, 373 pages. 2003.

Vol. 2856: M. Smirnov, E. Biersack, C. Blondia, O. Bonaventure, O. Casals, G. Karlsson, George Pavlou, B. Quoitin, J. Roberts, I. Stavrakakis, B. Stiller, P. Trimintzios, P. Van Mieghem (Eds.), Quality of Future Internet Services. IX, 293 pages. 2003.

Vol. 2857: M.A. Nascimento, E.S. de Moura, A.L. Oliveira (Eds.), String Processing and Information Retrieval. Proceedings, 2003. XI, 379 pages. 2003.

Vol. 2858: A. Veidenbaum, K. Joe, H. Amano, H. Aiso (Eds.), High Performance Computing. Proceedings, 2003. XV, 566 pages. 2003.

Vol. 2859: B. Apolloni, M. Marinaro, R. Tagliaferri (Eds.), Neural Nets. Proceedings, 2003. X, 376 pages. 2003.

Vol. 2860: D. Geist, E. Tronci (Eds.), Correct Hardware Design and Verification Methods. Proceedings, 2003. XII, 426 pages. 2003.

Vol. 2861: C. Bliek, C. Jermann, A. Neumaier (Eds.), Global Optimization and Constraint Satisfaction. Proceedings, 2002. XII, 239 pages. 2003.

Vol. 2862: D. Feitelson, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. Proceedings, 2003. VII, 269 pages. 2003.

Vol. 2863: P. Stevens, J. Whittle, G. Booch (Eds.), «UML» 2003 – The Unified Modeling Language. Proceedings, 2003. XIV, 415 pages. 2003.

Vol. 2864: A.K. Dey, A. Schmidt, J.F. McCarthy (Eds.), UbiComp 2003: Ubiquitous Computing. Proceedings, 2003. XVII, 368 pages. 2003.

Vol. 2865: S. Pierre, M. Barbeau, E. Kranakis (Eds.), Ad-Hoc, Mobile, and Wireless Networks. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2866: J. Akiyama, M. Kano (Eds.), Discrete and Computational Geometry. Proceedings, 2002. VIII, 285 pages. 2003.

Vol. 2867: M. Brunner, A. Keller (Eds.), Self-Managing Distributed Systems. Proceedings, 2003. XIII, 274 pages. 2003.

Vol. 2868: P. Perner, R. Brause, H.-G. Holzhütter (Eds.), Medical Data Analysis. Proceedings, 2003. VIII, 127 pages. 2003.

Vol. 2869: A. Yazici, C. Şener (Eds.), Computer and Information Sciences – ISCIS 2003. Proceedings, 2003. XIX, 1110 pages. 2003.

Vol. 2870: D. Fensel, K. Sycara, J. Mylopoulos (Eds.), The Semantic Web - ISWC 2003. Proceedings, 2003. XV, 931 pages. 2003.

Vol. 2871: N. Zhong, Z.W. Raś, S. Tsumoto, E. Suzuki (Eds.), Foundations of Intelligent Systems. Proceedings, 2003. XV, 697 pages. 2003. (Subseries LNAI)

Vol. 2873: J. Lawry, J. Shanahan, A. Ralescu (Eds.), Modelling with Words. XIII, 229 pages. 2003. (Subseries LNAI)

Vol. 2874: C. Priami (Ed.), Global Computing. Proceedings, 2003. XIX, 255 pages. 2003.

Vol. 2875: E. Aarts, R. Collier, E. van Loenen, B. de Ruyter (Eds.), Ambient Intelligence. Proceedings, 2003. XI, 432 pages. 2003.

Vol. 2876: M. Schroeder, G. Wagner (Eds.), Rules and Rule Markup Languages for the Semantic Web. Proceedings, 2003. VII, 173 pages. 2003.

Vol. 2877: T. Böhme, G. Heyer, H. Unger (Eds.), Innovative Internet Community Systems. Proceedings, 2003. VIII, 263 pages. 2003.

Vol. 2878: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Part I. Proceedings, 2003. XXXIII, 819 pages. 2003.

Vol. 2879: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Part II. Proceedings, 2003. XXXIV, 1003 pages. 2003.

Vol. 2880: H.L. Bodlaender (Ed.), Graph-Theoretic Concepts in Computer Science. Proceedings, 2003. XI, 386 pages. 2003.

Vol. 2881: E. Horlait, T. Magedanz, R.H. Glitho (Eds.), Mobile Agents for Telecommunication Applications. Proceedings, 2003. IX, 297 pages. 2003.

Vol. 2882: D. Veit, Matchmaking in Electronic Markets. XV, 180 pages. 2003. (Subseries LNAI)

Vol. 2883: J. Schaeffer, M. Müller, Y. Björnsson (Eds.), Computers and Games. Proceedings, 2002. XI, 431 pages. 2003.

Vol. 2884: E. Najm, U. Nestmann, P. Stevens (Eds.), Formal Methods for Open Object-Based Distributed Systems. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2885: J.S. Dong, J. Woodcock (Eds.), Formal Methods and Software Engineering. Proceedings, 2003. XI, 683 pages. 2003.

Vol. 2886: I. Nyström, G. Sanniti di Baja, S. Svensson (Eds.), Discrete Geometry for Computer Imagery. Proceedings, 2003. XII, 556 pages. 2003.

Vol. 2887: T. Johansson (Ed.), Fast Software Encryption. Proceedings, 2003. IX, 397 pages. 2003.

Vol. 2888: R. Meersman, Zahir Tari, D.C. Schmidt et al. (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. Proceedings, 2003. XXI, 1546 pages. 2003.

Vol. 2889: Robert Meersman, Zahir Tari et al. (Eds.), On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. Proceedings, 2003. XXI, 1096 pages. 2003.

Vol. 2890: M. Broy, A.V. Zamulin (Eds.), Perspectives of System Informatics. Proceedings, 2003. XV, 572 pages. 2003.

Vol. 2891: J. Lee, M. Barley (Eds.), Intelligent Agents and Multi-Agent Systems. Proceedings, 2003. X, 215 pages. 2003. (Subseries LNAI)

Vol. 2892: F. Dau, The Logic System of Concept Graphs with Negation. XI, 213 pages. 2003. (Subseries LNAI)

Vol. 2893: J.-B. Stefani, I. Demeure, D. Hagimont (Eds.), Distributed Applications and Interoperable Systems. Proceedings, 2003. XIII, 311 pages. 2003.

Vol. 2894: C.S. Laih (Ed.), Advances in Cryptology - ASIACRYPT 2003. Proceedings, 2003. XIII, 543 pages. 2003.

Vol. 2895: A. Ohori (Ed.), Programming Languages and Systems. Proceedings, 2003. XIII, 427 pages. 2003.

Vol. 2896: V.A. Saraswat (Ed.), Advances in Computing Science – ASIAN 2003. Proceedings, 2003. VIII, 305 pages. 2003.

Vol. 2897: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. Proceedings, 2003. XI, 240 pages. 2003.

Vol. 2898: K.G. Paterson (Ed.), Cryptography and Coding. Proceedings, 2003. IX, 385 pages. 2003.

Vol. 2899: G. Ventre, R. Canonico (Eds.), Interactive Multimedia on Next Generation Networks. Proceedings, 2003. XIV, 420 pages. 2003.

Vol. 2900: M. Bidoit, P.D. Mosses, CASL User Manual. XIII, 240 pages. 2004.

Vol. 2901: F. Bry, N. Henze, J. Maluszyński (Eds.), Principles and Practice of Semantic Web Reasoning. Proceedings, 2003. X, 209 pages. 2003.

Vol. 2902: F. Moura Pires, S. Abreu (Eds.), Progress in Artificial Intelligence. Proceedings, 2003. XV, 504 pages. 2003. (Subseries LNAI).

Vol. 2903: T.D. Gedeon, L.C.C. Fung (Eds.), AI 2003: Advances in Artificial Intelligence. Proceedings, 2003. XVI, 1075 pages. 2003. (Subseries LNAI).

Vol. 2904: T. Johansson, S. Maitra (Eds.), Progress in Cryptology – INDOCRYPT 2003. Proceedings, 2003. XI, 431 pages. 2003.

Vol. 2905: A. Sanfeliu, J. Ruiz-Shulcloper (Eds.), Progress in Pattern Recognition, Speech and Image Analysis. Proceedings, 2003. XVII, 693 pages. 2003.

Vol. 2906: T. Ibaraki, N. Katoh, H. Ono (Eds.), Algorithms and Computation. Proceedings, 2003. XVII, 748 pages. 2003.

Vol. 2908: K. Chae, M. Yung (Eds.), Information Security Applications. Proceedings, 2003. XII, 506 pages. 2004.

Vol. 2910: M.E. Orlowska, S. Weerawarana, M.P. Papazoglou, J. Yang (Eds.), Service-Oriented Computing – ICSOC 2003. Proceedings, 2003. XIV, 576 pages. 2003.

Vol. 2911: T.M.T. Sembok, H.B. Zaman, H. Chen, S.R. Urs, S.H.Myaeng (Eds.), Digital Libraries: Technology and Management of Indigenous Knowledge for Global Access. Proceedings, 2003. XX, 703 pages. 2003.

Vol. 2912: G. Liotta (Ed.), Graph Drawing. Proceedings, 2003. XV, 542 pages. 2004.

Vol. 2913: T.M. Pinkston, V.K. Prasanna (Eds.), High Performance Computing – HiPC 2003. Proceedings, 2003. XX, 512 pages. 2003.

Vol. 2914: P.K. Pandya, J. Radhakrishnan (Eds.), FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science. Proceedings, 2003. XIII, 446 pages. 2003.

Vol. 2916: C. Palamidessi (Ed.), Logic Programming. Proceedings, 2003. XII, 520 pages. 2003.

Vol. 2918: S.R. Das, S.K. Das (Eds.), Distributed Computing – IWDC 2003. Proceedings, 2003. XIV, 394 pages. 2003.

Vol. 2919: E. Giunchiglia, A. Tacchella (Eds.), Theory and Applications of Satisfiability Testing. Proceedings, 2003. XI, 530 pages. 2004.

Vol. 2920: H. Karl, A. Willig, A. Wolisz (Eds.), Wireless Sensor Networks. Proceedings, 2004. XIV, 365 pages. 2004.

Vol. 2921: G. Lausen, D. Suciu (Eds.), Database Programming Languages. Proceedings, 2003. X, 279 pages. 2004.

Vol. 2922: F. Dignum (Ed.), Advances in Agent Communication. Proceedings, 2003. X, 403 pages. 2004. (Subseries LNAI).

Vol. 2923: V. Lifschitz, I. Niemelä (Eds.), Logic Programming and Nonmonotonic Reasoning. Proceedings, 2004. IX, 365 pages. 2004. (Subseries LNAI).

Vol. 2924: J. Callan, F. Crestani, M. Sanderson (Eds.), Distributed Multimedia Information Retrieval. Proceedings, 2003. XII, 173 pages. 2004.

Vol. 2926: L. van Elst, V. Dignum, A. Abecker (Eds.), Agent-Mediated Knowledge Management. Proceedings, 2003. XI, 428 pages. 2004. (Subseries LNAI).

Vol. 2927: D. Hales, B. Edmonds, E. Norling, J. Rouchier (Eds.), Multi-Agent-Based Simulation III. Proceedings, 2003. X, 209 pages. 2003. (Subseries LNAI).

Vol. 2928: R. Battiti, M. Conti, R. Lo Cigno (Eds.), Wireless On-Demand Network Systems. Proceedings, 2004. XIV, 402 pages. 2004.

Vol. 2929: H. de Swart, E. Orlowska, G. Schmidt, M. Roubens (Eds.), Theory and Applications of Relational Structures as Knowledge Instruments. Proceedings. VII, 273 pages. 2003.

Vol. 2932: P. Van Emde Boas, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2004: Theory and Practice of Computer Science. Proceedings, 2004. XIII, 385 pages. 2004.

Vol. 2935: P. Giorgini, J.P. Müller, J. Odell (Eds.), Agent-Oriented Software Engineering IV. Proceedings, 2003. X, 247 pages. 2004.

Vol. 2937: B. Steffen, G. Levi (Eds.), Verification, Model Checking, and Abstract Interpretation. Proceedings, 2004. XI, 325 pages. 2004.

Vol. 2950: N. Jonoska, G. Păun, G. Rozenberg (Eds.), Aspects of Molecular Computing. XI, 391 pages. 2004.

Preface

This book is devoted to the *6th International Conference on Theory and Applications of Satisfiability Testing* (*SAT 2003*) held in Santa Margherita Ligure (Genoa, Italy), during May 5–8, 2003. SAT 2003 followed the Workshops on Satisfiability held in Siena (1996), Paderborn (1998), and Renesse (2000), and the Workshop on Theory and Applications of Satisfiability Testing held in Boston (2001) and in Cincinnati (2002). As in the last edition, the SAT event hosted a SAT solvers competition, and, starting from the 2003 edition, also a Quantified Boolean Formulas (QBFs) solvers comparative evaluation.

There were 67 submissions of high quality, authored by researchers from all over the world. All the submissions were thoroughly evaluated, and as a result 42 were selected for oral presentations, and 16 for a poster presentation. The presentations covered the whole spectrum of research in propositional and QBF satisfiability testing, including proof systems, search techniques, probabilistic analysis of algorithms and their properties, problem encodings, industrial applications, specific tools, case studies and empirical results. Further, the program was enriched by three invited talks, given by Riccardo Zecchina (on *"Survey Propagation: from Analytic Results on Random k-SAT to a Message-Passing Algorithm for Satisfiability"*), Toby Walsh (on *"Challenges in SAT* (and QBF)*"*) and Wolfgang Kunz (on *"ATPG Versus SAT: Comparing Two Paradigms for Boolean Reasoning"*). SAT 2003 thus provided a unique forum for the presentation and discussion of research related to the theory and applications of propositional and QBF satisfiability testing.

The book includes 38 contributions. The first 33 are revised versions of some of the articles that were presented at the conference. The last 5 articles present the results of the SAT competition and of the QBF evaluation, solvers that won the SAT competition, and results on survey and belief propagation. All 38 papers were thoroughly reviewed.

We would like to thank the many people who contributed to the SAT 2003 organization (listed in the following pages), the SAT 2003 participants for the lively discussions, and the sponsors.

September 2003

Enrico Giunchiglia
Armando Tacchella

SAT 2003 Organization

SAT 2003 was organized by DIST (Dipartimento di Informatica, Sistemistica e Telematica), Università di Genova.

Chair

Enrico Giunchiglia, DIST, Università di Genova

Organizing Committee

John Franco, University of Cincinnati
Enrico Giunchiglia, Università di Genova
Henry Kautz, University of Washington
Hans Kleine Büning, Universität Paderborn
Hans van Maaren, University of Delft
Bart Selman, Cornell University
Ewald Speckenmayer, Universität Köln

SAT Competition Organizers

Daniel Le Berre, CRIL, Université d'Artois
Laurent Simon, LRI Laboratory, Université Paris-Sud

QBF Comparative Evaluation Organizers

Daniel Le Berre, CRIL, Université d'Artois
Laurent Simon, LRI Laboratory, Université Paris-Sud
Armando Tacchella, DIST, Università di Genova

Local Organization

Roberta Ferrara, Università di Genova
Marco Maratea, DIST, Università di Genova
Massimo Narizzano, DIST, Università di Genova
Adriano Ronzitti, DIST, Università di Genova
Armando Tacchella, DIST, Università di Genova (Chair)

Program Committee

Dimitris Achlioptas, Microsoft Research
Fadi Aloul, University of Michigan
Fahiem Bacchus, University of Toronto
Armin Biere, ETH Zurich
Nadia Creignou, Université de la Méditerranée, Marseille
Olivier Dubois, Université Paris 6
Uwe Egly, Technische Universität Wien
John Franco, University of Cincinnati
Ian Gent, St. Andrews University
Enrico Giunchiglia, DIST, Università di Genova
Carla Gomez, Cornell University
Edward A. Hirsch, Steklov Institute of Mathematics at St. Petersburg
Holger Hoos, University of British Columbia
Henry Kautz, University of Washington
Hans Kleine Büning, Universität Paderborn
Oliver Kullmann, University of Wales, Swansea
Daniel Le Berre, CRIL, Université d'Artois
Joo Marques-Silva, Instituto Superior Técnico, Univ. Técnica de Lisboa
Hans van Maaren, University of Delft
Remi Monasson, Laboratoire de Physique Théorique de l'ENS
Daniele Pretolani, Università di Camerino
Paul W. Purdom, Indiana University
Jussi Rintanen, Freiburg University
Bart Selman, Cornell University
Malik Sharad, Princeton University
Laurent Simon, LRI Laboratory, Université Paris-Sud
Ewald Speckenmeyer, Universität Köln
Armando Tacchella, DIST, Università di Genova
Allen Van Gelder, UC Santa Cruz
Miroslav N. Velev, Carnegie Mellon University
Toby Walsh, University of York

Additional Referees

G. Audemard
F. Corradini
S. Coste-Marquis
H. Daudé
L. Drake
M. Fink
Z. Fu
A. Kojevnikov
A. Kulikov
T. Lettmann
I. Lynce
M. Maratea
M. Molloy
M. Narizzano
S. Nikolenko
A. Polleres
S. Porschen
S. Prestwich
B. Randerath
O. Roussel
A. Rowley
U. Schoening
A. Shmygelska
K. Smyth
D. Tang
H. Tompits
D. Tompkins
H. Vollmer
S. Woltran
Y. Yu

Sponsoring Institutions

CoLogNet, Network of Excellence in Computational Logic
DIST, Università di Genova
IISI, Intelligent Information Systems Institute at Cornell University
Microsoft Research
MIUR, Ministero dell'Istruzione, dell'Università e della Ricerca

Table of Contents

Satisfiability and Computing van der Waerden Numbers

Michael R. Dransfield[1], Victor W. Marek[2], and Mirosław Truszczyński[2]

[1] National Security Agency, Information Assurance Directorate, Ft. Meade, MD 20755
[2] Department of Computer Science, University of Kentucky, Lexington, KY 40506-0046, USA

Abstract. In this paper we bring together the areas of combinatorics and propositional satisfiability. Many combinatorial theorems establish, often constructively, the existence of positive integer functions, without actually providing their closed algebraic form or tight lower and upper bounds. The area of Ramsey theory is especially rich in such results. Using the problem of computing van der Waerden numbers as an example, we show that these problems can be represented by parameterized propositional theories in such a way that decisions concerning their satisfiability determine the numbers (function) in question. We show that by using general-purpose complete and local-search techniques for testing propositional satisfiability, this approach becomes effective — competitive with specialized approaches. By following it, we were able to obtain several new results pertaining to the problem of computing van der Waerden numbers. We also note that due to their properties, especially their structural simplicity and computational hardness, propositional theories that arise in this research can be of use in development, testing and benchmarking of SAT solvers.

1 Introduction

In this paper we discuss how the areas of propositional satisfiability and combinatorics can help advance each other. On one hand, we show that recent dramatic improvements in the efficiency of SAT solvers and their extensions make it possible to obtain new results in combinatorics simply by encoding problems as propositional theories, and then computing their models (or deciding that none exist) using off-the-shelf general-purpose SAT solvers. On the other hand, we argue that combinatorics is a rich source of structured, parameterized families of hard propositional theories, and can provide useful sets of benchmarks for developing and testing new generations of SAT solvers.

In our paper we focus on the problem of computing van der Waerden numbers. The celebrated van der Waerden theorem [20] asserts that for every positive integers k and l there is a positive integer m such that every partition of $\{1,\ldots,m\}$ into k blocks (parts) has at least one block with an arithmetic progression of length l. The problem is to find the least such number m. This

E. Giunchiglia and A. Tacchella (Eds.): SAT 2003, LNCS 2919, pp. 1–13, 2004.

number is called the *van der Waerden number* $W(k,l)$. Exact values of $W(k,l)$ are known only for five pairs (k,l). For other combinations of k and l there are some general lower and upper bounds but they are very coarse and do not give any good idea about the actual value of $W(k,l)$. In the paper we show that SAT solvers such as POSIT [6], and SATO [21], as well as recently developed local-search solver *walkaspps* [13], designed to compute models for propositional theories extended by cardinality atoms [4], can improve lower bounds for van der Waerden numbers for several combinations of parameters k and l.

Theories that arise in these investigations are determined by the two parameters k and l. Therefore, they show a substantial degree of structure and similarity. Moreover, as k and l grow, these theories quickly become very hard. This hardness is only to some degree an effect of the growing size of the theories. For the most part, it is the result of the inherent difficulty of the combinatorial problem in question. All this suggests that theories resulting from hard combinatorial problems defined in terms of tuples of integers may serve as benchmark theories in experiments with SAT solvers.

There are other results similar in spirit to the van der Waerden theorem. The Schur theorem states that for every positive integer k there is an integer m such that every partition of $\{1,\ldots,m\}$ into k blocks contains a block that is not sum-free. Similarly, the Ramsey theorem (which gave name to this whole area in combinatorics) [16] concerns the existence of monochromatic cliques in edge-colored graphs, and the Hales-Jewett theorem [11] concerns the existence of monochromatic lines in colored cubes. Each of these results gives rise to a particular function defined on pairs or triples of integers and determining the values of these functions is a major challenge for combinatorialists. In all cases, only few exact values are known and lower and upper estimates are very far apart. Many of these results were obtained by means of specialized search algorithms highly depending on the combinatorial properties of the problem. Our paper shows that generic SAT solvers are maturing to the point where they are competitive and sometimes more effective than existing advanced specialized approaches.

2 Van der Waerden Numbers

In the paper we use the following terminology. By $\mathbb{Z}^+$ we denote the set of positive integers and, for $m \in \mathbb{Z}^+$, $[m]$ is the set $\{1,\ldots,m\}$. A *partition* of a set X is a collection $\mathcal{A}$ of nonempty and mutually disjoint subsets of X such that $\bigcup \mathcal{A} = X$. Elements of $\mathcal{A}$ are commonly called *blocks*.

Informally, the van der Waerden theorem [20] states that if a sufficiently long initial segment of positive integers is partitioned into a few blocks, then one of these blocks has to contain an arithmetic progression of a desired length. Formally, the theorem is usually stated as follows.

Theorem 1 (van der Waerden theorem). *For every $k,l \in \mathbb{Z}^+$, there is $m \in \mathbb{Z}^+$ such that for every partition $\{A_1,\ldots,A_k\}$ of $[m]$, there is i, $1 \leq i \leq k$, such that block A_i contains an arithmetic progression of length at least l.*

We define the *van der Waerden number* $W(k,l)$ to be the least number m for which the assertion of Theorem 1 holds. Theorem 1 states that van der Waerden numbers are well defined.

One can show that for every k and l, where $l \geq 2$, $W(k,l) > k$. In particular, it is easy to see that $W(k,2) = k+1$. From now on, we focus on the non-trivial case when $l \geq 3$.

Little is known about the numbers $W(k,l)$. In particular, no closed formula has been identified so far and only five exact values are known. They are shown in Table 1 [1,10].

k \ l	3	4	5
2	9	35	178
3	27		
4	76		

Table 1. Known non-trivial values of van der Waerden numbers

Since we know few exact values for van der Waerden numbers, it is important to establish good estimates. One can show that the Hales-Jewett theorem entails the van der Waerden theorem, and some upper bounds for the numbers $W(k,l)$ can be derived from the Shelah's proof of the former [18]. Recently, Gowers [9] presented stronger upper bounds, which he derived from his proof of the Szemerédi theorem [19] on arithmetic progressions.

In our work, we focus on lower bounds. Several general results are known. For instance, Erdös and Rado [5] provided a non-constructive proof for the inequality

$$W(k,l) > (2(l-1)k^{l-1})^{1/2}.$$

For some special values of parameters k and l, Berlekamp obtained better bounds by using properties of finite fields [2]. These bounds are still rather weak. His strongest result concerns the case when $k = 2$ and $l-1$ is a prime number. Namely, he proved that when $l-1$ is a prime number,

$$W(2,l) > (l-1)2^{l-1}.$$

In particular, $W(2,6) > 160$ and $W(2,8) > 896$.

Our goal in this paper is to employ propositional satisfiability solvers to find lower bounds for several small van der Waerden numbers. The bounds we find significantly improve on the ones implied by the results of Erdös and Rado, and Berlekamp.

We proceed as follows. For each triple of positive integers $\langle k,l,m \rangle$, we define a propositional CNF theory $\mathrm{vdW}_{k,l,m}$ and then show that $\mathrm{vdW}_{k,l,m}$ is satisfiable if and only if $W(k,l) > m$. With such encodings, one can use SAT solvers (at least in principle) to determine the satisfiability of $\mathrm{vdW}_{k,l,m}$ and, consequently,

find $W(k,l)$. Since $W(k,l) > k$, without loss of generality we can restrict our attention to $m > k$. We also show that more concise encodings are possible, leading ultimately to better bounds, if we use an extension of propositional logic by *cardinality atoms* and apply to them solvers capable of handling such atoms directly.

To describe $\mathrm{vdW}_{k,l,m}$ we will use a standard first-order language, without function symbols, but containing a predicate symbol *in_block* and constants $1,\ldots,m$. An intuitive reading of a ground atom $in\_block(i,b)$ is that an integer i is in block b.

We now define the theory $\mathrm{vdW}_{k,l,m}$ by including in it the following clauses:

vdW1: $\neg in\_block(i,b_1) \vee \neg in\_block(i,b_2)$, for every $i \in [m]$ and every $b_1, b_2 \in [k]$ such that $b_1 < b_2$,

vdW2: $in\_block(i,1) \vee \ldots \vee in\_block(i,k)$, for every $i \in [m]$,

vdW3: $\neg in\_block(i,b) \vee \neg in\_block(i+d,b) \vee \ldots \vee \neg in\_block(i+(l-1)d,b)$, for every $i,d \in [m]$ such that $i+(l-1)d \leq m$, and for every b such that $1 \leq b \leq k$.

As an aside, we note that we could design $\mathrm{vdW}_{k,l,m}$ strictly as a theory in propositional language using propositional atoms of the form $in\_block_{i,b}$ instead of ground atoms $in\_block(i,b)$. However, our approach opens a possibility to specify this theory as finite (and independent of data) collections of *propositional schemata*, that is, open clauses in the language of first-order logic without function symbols. Given a set of appropriate constants (to denote integers and blocks) such theory, after grounding, coincides with $\mathrm{vdW}_{k,l,m}$. In fact, we have defined an appropriate syntax that allows us to specify both data and schemata and implemented a grounding program *psgrnd* [4] that generates their equivalent ground (propositional) representation. This grounder accepts arithmetic expressions as well as simple regular expressions, and evaluates and eliminates them according to their standard interpretation. Such approach significantly simplifies the task of developing propositional theories that encode problems, as well as the use of SAT solvers [4].

Propositional interpretations of the theory $\mathrm{vdW}_{k,l,m}$ can be identified with subsets of the set of atoms $\{in\_block(i,b)\colon i \in [m],\ b \in [k]\}$. Namely, a set $M \subseteq \{in\_block(i,b)\colon i \in [m],\ b \in [k]\}$ determines an interpretation in which all atoms in M are true and all other atoms are false. In the paper we always assume that interpretations are represented as sets.

It is easy to see that clauses (vdW1) ensure that if M is a model of $\mathrm{vdW}_{k,l,m}$ (that is, is an interpretation satisfying all clauses of $\mathrm{vdW}_{k,l,m}$), then for every $i \in [m]$, M contains at most one atom of the form $in\_block(i,b)$. Clauses (vdW2) ensure that for every $i \in [m]$ there is at least one $b \in [k]$ such that $in\_block(i,b) \in M$. In other words, clauses (vdW1) and (vdW2) together ensure that if M is a model of $\mathrm{vdW}_{k,l,m}$, then M determines a partition of $[m]$ into k blocks.

The last group of constraints, clauses (vdW3), guarantee that elements from $[m]$ forming an arithmetic progression of length l do not all belong to the same block. All these observations imply the following result.