

When Computer Algebra Meets Satisfiability: A New Approach to Combinatorial Mathematics

New Technologies in Mathematics (Harvard University)

Vijay Ganesh (University of Waterloo) and Curtis Bright (University of Windsor)

Abstract

Solvers for the Boolean satisfiability (SAT) problem have been increasingly used to resolve problems in mathematics due to their excellent search algorithms. This talk will describe a new method for mathematical search that couples SAT solvers with computer algebra systems (CAS), thereby combining the expressiveness of CASs with the search power of SAT solvers. This paradigm has led to a number of results on long-standing mathematical questions such as the first computer-verifiable resolution of Lam's problem and the discovery of a new infinite class of Williamson matrices.

References

- 1 Leonard Baumert, S. W. Golomb, and Marshall Hall Jr. Discovery of an Hadamard matrix of order 92. *Bulletin of the American Mathematical Society*, 68(3):237 – 238, 1962.
- 2 Curtis Bright, Kevin Cheung, Brett Stevens, Dominique Roy, Ilias Kotsireas, and Vijay Ganesh. A nonexistence certificate for projective planes of order ten with weight 15 codewords. *Applicable Algebra in Engineering, Communication and Computing*, 31:195–213, 2020.
- 3 Curtis Bright, Kevin K. H. Cheung, Brett Stevens, Ilias Kotsireas, and Vijay Ganesh. A SAT-based resolution of Lam's problem. In *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence*, pages 3669–3676, 2021.
- 4 Curtis Bright, Vijay Ganesh, Albert Heine, Ilias Kotsireas, Saeed Nejati, and Krzysztof Czarnecki. MATHCHECK2: A SAT+CAS verifier for combinatorial conjectures. In *Computer Algebra in Scientific Computing - 18th International Workshop, CASC 2016*, pages 117–133. Springer, 2016.
- 5 Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, 100:187–209, 2020.
- 6 Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. New infinite families of perfect quaternion sequences and Williamson sequences. *IEEE Transactions on Information Theory*, 66(12):7739–7751, 2020.
- 7 John Conway and Simon Kochen. The free will theorem. *Foundations of Physics*, 36(10):1441–1473, jul 2006.
- 8 Dragomir Ž. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete mathematics*, 115(1):267–271, 1993.
- 9 Marijn J. H. Heule, Manuel Kauers, and Martina Seidl. New ways to multiply 3×3 -matrices. *Journal of Symbolic Computation*, 104:899–916, May 2021.
- 10 Ilias S. Kotsireas and Christos Koukouvinos. Constructions for Hadamard matrices of Williamson type. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 59:17, 2006.
- 11 Clement W. H. Lam, Larry Thiel, and Stanley Swiercz. The non-existence of finite projective planes of order 10. *Canadian Journal of Mathematics*, 41(6):1117–1123, 1989.
- 12 J. P. Marques-Silva and K. A. Sakallah. GRASP: a search algorithm for propositional satisfiability. *IEEE Transactions on Computers*, 48(5):506–521, 1999.

- 13 Matthew W. Moskewicz, Conor F. Madigan, Ying Zhao, Lintao Zhang, and Sharad Malik. Chaff: Engineering an efficient SAT solver. In *Proceedings of the 38th Annual Design Automation Conference, DAC '01*, page 530–535, New York, NY, USA, 2001. Association for Computing Machinery.
- 14 Edward Zulkoski, Vijay Ganesh, and Krzysztof Czarnecki. MathCheck: A math assistant via a combination of computer algebra systems and SAT solvers. In Amy P. Felty and Aart Middeldorp, editors, *Automated Deduction - CADE-25*, pages 607–622, Cham, 2015. Springer International Publishing.