Searching for projective planes with computer algebra and SAT solvers

***Curtis Bright*[1], *Kevin Cheung*[2], *Brett Stevens*[2], *Dominique Roy*[3], *Ilias Kotsireas*[4], *Vijay Ganesh*[1]**

[1] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
[2] School of Mathematics and Statistics, Carleton University, Ottawa, Canada
[3] Canada Revenue Agency, Ottawa, Canada
[4] Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada

In the 1970s and 1980s a series of exhaustive searches [1–4] showed that projective planes of order ten do not exist. These searches required a significant amount of computing power including almost three months of time on a CRAY-1A supercomputer. However, due to the nature of the search it was not possible to present a formal proof of the result. Recently SAT solvers have been used to derive proofs of results that require extensive computer search [5], raising the possibility that SAT solvers could be useful searching for projective planes and proving that projective planes of certain orders do not exist.

In this talk we report on work we have done in this direction, in particular, employing a hybrid satisfiability checking and computer algebra (SAT+CAS) approach that has been recently proposed [6] and successfully used in searches for other combinatorial objects [7–9]. In the SAT+CAS paradigm a computer algebra system is used to generate theory lemmas that a SAT solver would otherwise not be able to learn. In the search for projective planes we found that a CAS is an effective tool for finding symmetries of partial projective planes that can be used to dramatically improve the efficiency of the SAT solver.

Keywords
Projective planes, satisfiability checking, symbolic computation, symmetry breaking, search

References

[1] F. J. MACWILLIAMS; N. J. A. SLOANE; J. G. THOMPSON, On the existence of a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, **14**(1), 66–78 (1973).
[2] J. L. CARTER, *On the existence of a projective plane of order ten*. PhD thesis, University of California, Berkeley, 1974.
[3] C. W. H. LAM; L. THIEL; S. SWIERCZ, The nonexistence of code words of weight 16 in a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, **42**(2), 207–214 (1986).

[4] C. W. H. LAM; L. THIEL; S. SWIERCZ, The non-existence of finite projective planes of order 10. *Canadian Journal of Mathematics*, **41**(6), 1117–1123 (1989).
[5] M. J. H. HEULE; O. KULLMANN; V. W. MAREK, Solving and verifying the boolean Pythagorean triples problem via cube-and-conquer. In *Theory and Applications of Satisfiability Testing – SAT 2016*, N. Creignou and D. Le Berre (eds.), 228–245. Springer, Cham, 2016.
[6] E. ÁBRAHÁM, Building bridges between symbolic computation and satisfiability checking. In *ISSAC'15 Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, S. Linton (ed.), 1–6. ACM, New York, 2015.
[7] C. BRIGHT; I. KOTSIREAS; V. GANESH, Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, to appear (2019).
[8] C. BRIGHT; I. KOTSIREAS; A. HEINLE; V. GANESH, Enumeration of complex Golay pairs via Programmatic SAT. In *ISSAC '18 Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, C. Arreche (ed.), 111–118. ACM, New York, 2018.
[9] C. BRIGHT; D. Ž. ĐOKOVIC; I. KOTSIREAS; V. GANESH, A SAT+CAS approach to finding good matrices: New examples and counterexamples. To appear in *Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence*, AAAI Press, Palo Alto, 2019.