Solving Lam's Problem via SAT and Isomorph-Free Exhaustive Generation

Curtis Bright[1,2], **Kevin K. H. Cheung**[2], **Brett Stevens**[2], **Ilias Kotsireas**[3] and **Vijay Ganesh**[4]

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

Abstract

Lam's problem is to prove the nonexistence of a type of geometric structure that has intrigued mathematicians for centuries. In this work we reduce Lam's problem to a Boolean satisfiability (SAT) problem and generate certificates which for the first time can be used to verify the resolution of Lam's problem. The search space underlying the problem has many nontrivial symmetries—necessitating an approach that detects and removes symmetries as early as possible. We couple a method of isomorph-free exhaustive generation with a SAT solver and show that this significantly improves the performance of the solver when symmetries are present.

Introduction

Projective geometry was developed by Renaissance artists in order to describe how to represent a three-dimensional scene on a two-dimensional canvas. Any two lines in a projective geometry must meet—for example, a pair of train tracks will meet on the horizon when projected onto two dimensions. A complete classification of projective geometries is still unknown and *Lam's problem* is to resolve the first uncertain case: is it possible for a projective geometry have every line contain exactly eleven points and every point lie on exactly eleven lines?

No purely mathematical resolution of Lam's problem is known, but a computer-assisted resolution required months of computational time using custom-written programs run on a CRAY-1A supercomputer (Lam 1991). Because the software and hardware are no longer available it is impossible to verify that these searches ran to completion. Moreover, writing custom programs is an inherently error-ridden process (Lam 1990). Indeed, cases missing in the original search were later uncovered (Roy 2011) in an independent check—a check that itself missed cases (Bright et al. 2020a; Bright et al. 2021).

Contributions

We provide the first verifiable resolution of Lam's problem. We reduce Lam's problem to an instance of the Boolean satisfiability (SAT) problem (Gomes et al. 2008) and use a SAT solver to perform the search. The SAT solver itself does not need to be trusted, since it produces certificates of unsatisfiability that we verify using a proof checker. In addition, in order to remove symmetries from the search space and reduce the search to a feasible size it was necessary to augment the SAT solver with an isomorph-free exhaustive generation method.

Representation, Reasoning, and Isomorph Rejection

The reduction to SAT is accomplished by using a Boolean variable for every possible point-line incidence. For example, a Boolean variable a_{ij} will represent that point i lies on line j. Axioms specifying projective geometry are encoded using these variables; e.g., if points 1 and 2 lie on line 1 they cannot both lie on line 2 which in Boolean logic is $(a_{11} \wedge a_{21}) \rightarrow \neg(a_{12} \wedge a_{22})$.

All projective geometry axioms are encoded using logical clauses, allowing a SAT solver to apply Boolean resolution to derive new clauses. Every derived clause is recorded and the list of derived clauses forms a proof certificate which can be verified using a proof verifier like DRAT-trim (Wetzler, Heule, and Hunt 2014) or GRATgen (Lammich 2019). A derivation of the empty clause is then a verifiable proof that the SAT instance has no solutions.

Additional constraints are necessary to reduce the number of symmetries present in the search space. For example, the lines and points of a projective plane can be reordered with impunity. Thus, we add "symmetry breaking" clauses which enforce a lexicographic order on the lines and points of the plane when viewed as binary row and column vectors (Flener et al. 2002). This breaks the row and column symmetries individually, though many nontrivial symmetries remain which are not easy to break with static constraints (Bright et al. 2020b; Bright et al. 2020c).

We therefore combine our SAT approach with the "recorded objects" approach to isomorph-free exhaustive generation (Kaski and Östergård 2006). As the solver finds partial solutions to Lam's problem those intermediate objects are recorded. Whenever a new object is isomorphic to a previous object, a conflict clause is learned blocking the new object. This approach improves the efficiency of the search for all possibilities of the initial lines of the plane by a factor of 150. With this optimization the search required about 2 CPU years and produced certificates of about 110 TiB in size.

References

Bright, C.; Cheung, K.; Stevens, B.; Roy, D.; Kotsireas, I.; and Ganesh, V. 2020a. A nonexistence certificate for projective planes of order ten with weight 15 codewords. *Applicable Algebra in Engineering, Communication and Computing*.

Bright, C.; Cheung, K. K. H.; Stevens, B.; Kotsireas, I.; and Ganesh, V. 2020b. Nonexistence certificates for ovals in a projective plane of order ten. In *Proceedings of the 31st International Workshop on Combinatorial Algorithms*, 97–111.

Bright, C.; Cheung, K. K. H.; Stevens, B.; Kotsireas, I.; and Ganesh, V. 2020c. Unsatisfiability proofs for weight 16 codewords in Lam's problem. *Proceedings of the 29th International Joint Conference on Artificial Intelligence*.

Bright, C.; Cheung, K. K. H.; Stevens, B.; Kotsireas, I.; and Ganesh, V. 2021. A SAT-based resolution of Lam's problem. In *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence*, 3669–3676.

Flener, P.; Frisch, A. M.; Hnich, B.; Kiziltan, Z.; Miguel, I.; Pearson, J.; and Walsh, T. 2002. Breaking row and column symmetries in matrix models. In *Lecture Notes in Computer Science*. Springer Berlin Heidelberg. 462–477.

Gomes, C. P.; Kautz, H.; Sabharwal, A.; and Selman, B. 2008. Satisfiability solvers. In van Harmelen, F.; Lifschitz, V.; and Porter, B., eds., *Handbook of Knowledge Representation*. Elsevier. 89–134.

Kaski, P., and Östergård, P. R. 2006. *Classification Algorithms for Codes and Designs*. Springer-Verlag.

Lam, C. W. H. 1990. How reliable is a computer-based proof? *Mathematical Intelligencer* 12(1):8–12.

Lam, C. W. H. 1991. The search for a finite projective plane of order 10. *The American Mathematical Monthly* 98(4):305–318.

Lammich, P. 2019. Efficient verified (UN)SAT certificate checking. *Journal of Automated Reasoning* 64(3):513–532.

Roy, D. J. 2011. Confirmation of the non-existence of a projective plane of order 10. Master's thesis, Carleton University.

Wetzler, N.; Heule, M. J. H.; and Hunt, W. A. 2014. DRAT-trim: Efficient checking and trimming using expressive clausal proofs. In *Lecture Notes in Computer Science*. Springer International Publishing. 422–429.