Lam's Problem Benchmarks for the SAT Competition 2020

Curtis Bright
Carleton University & University of Waterloo
Ottawa & Waterloo, Canada
cbright@uwaterloo.ca

Saeed Nejati
University of Waterloo
Waterloo, Canada
snejati@uwaterloo.ca

Vijay Ganesh
University of Waterloo
Waterloo, Canada
vijay.ganesh@uwaterloo.ca

***Abstract*—This document describes a collection of satisfiability instances that arise in Lam's problem from discrete geometry.**

I. Introduction

Instances in this benchmark encode subproblems that arise in Lam's problem from finite projective geometry—the problem of determining whether or not a finite projective plane of order ten exists. Studied since the 1800s, Lam's problem was resolved in the late 1980s by a computer search culminating in months of computational effort on a CRAY-1A supercomputer [1]. Recently, we used SAT solvers to verify a significant portion of this search [2]–[4].

II. Background

A finite projective plane of order ten is defined to consist of a collection of 111 points, 111 lines, and an incidence relationship between points and lines such that any two points are incident with a unique line and any two lines are incident with a unique point. Furthermore, every line is incident with exactly 11 points and every point is incident with 11 lines.

From a computational perspective, a convenient way of representing a finite projective plane of order ten is by a square incidence matrix A of order 111 whose (i, j)th entry contains a 1 exactly when the ith line is incident to the jth point. The projective plane incidence relationship requires that any two distinct rows or columns of A have an inner product of exactly one. It follows that A satisfies the relationship

$$AA^T = A^TA = 10I + J$$

where I denotes the identity matrix and J denotes the matrix consisting of all 1s.

It is hopeless to determine if such an A exists using this simple definition alone—even though the search space is finite it is far too large to be effectively searched. In the 1970s, coding theory was used to derive conditions that A must satisfy if it exists. In particular, it can be shown mathematically that the rowspace of A (mod 2) must contain vectors of Hamming weight 15 or 19 [5]. Furthermore, the existence of such vectors greatly restrict the structure of A.

In particular, a vector of Hamming weight 15 appearing in A's rowspace implies that every entry appearing in either the first 21 rows or 15 columns of A can be assumed without loss of generality [6]. Similarly, the vectors of Hamming weight 19 are of three possible types (called oval, 16-type, or primitive [5]) and each case places restrictions on the possible structure of A.

The twenty benchmarks in this collection each specify a different starting configuration for A—one benchmark resulting from the weight 15 starting configuration, three benchmarks resulting from 16-type starting configurations, and sixteen benchmarks resulting from primitive weight 19 starting configurations.

III. Encoding

Let $a_{i,j}$ be a Boolean variable that is true exactly when $A[i, j] = 1$. We say that two columns or rows of A *intersect* if they share a 1 in the same location. The projective plane incidence relationship requires that any two rows and any two columns of A intersect exactly once. In our encoding we require that

1) any two rows or columns intersect *at most* once, and
2) any row or column entirely specified by the starting configuration intersects every other row or column *at least* once.

These two conditions are sufficient to show that A cannot exist (at least in the starting configurations that occur in this collection of benchmarks). Moreover, these conditions are naturally encoded in conjunctive normal form.

In the first condition, suppose that i and j are arbitrary row indices. Then

$$\bigwedge_{1\leq k<l\leq 111} (\neg a_{i,k} \vee \neg a_{i,l} \vee \neg a_{j,k} \vee \neg a_{j,l})$$

specify that rows i and j do not intersect twice (i.e., they intersect at most once). Conditions of this form are required for all $1 \leq i < j \leq 111$.

In the second condition, suppose that i is the index of a row completely specified by the starting configuration and that j is the index of another row. Then

$$\bigvee_{k:A[i,k]=1} a_{j,k}$$

specifies that row i and j intersect at least once. This clause is well-defined since all entries $A[i, k]$ for $1 \leq k \leq 111$ are known in the starting configuration. We also include similar clauses for each column completely specified by the starting configuration.

Additionally, we used two optimizations of this encoding which in our experiments made the instances easier to solve.

First, we do not include all 111^2 variables in the instances. Instead, we choose a submatrix of A and only encode the constraints arising in that submatrix. The submatrix is experimentally chosen to be small while still ensuring that there are enough constraints to make the instance unsatisfiable. As a rule of thumb, about one third of the entries of A are usually required before the instance becomes unsatisfiable. In our collection of benchmarks the weight 15 instance used 75 columns and 51 rows, the 16-type instances used 65 columns and 80 rows, and the primitive weight 19 instances used up to 54 columns and all 111 rows.

Second, we included symmetry breaking clauses that remove symmetries from the search space. In particular, we enforce a lexicographical order on certain rows and columns that are otherwise identical in the starting configuration. There are also additional symmetries in the 16-type instances broken using a lexicographic method—see [3] for details.

IV. SUMMARY

The benchmarks in this collection naturally arise in the process of solving Lam's problem from finite geometry. They have been selected in order to provide the satisfiability community a collection of instances relevant to solving an interesting and celebrated mathematical problem. They were generated as a part of the MathCheck project and can all be solved in under an hour on a modern desktop using the cube-and-conquer paradigm [7].

REFERENCES

[1] C. W. H. Lam, L. Thiel, and S. Swiercz, "The non-existence of finite projective planes of order 10," *Canadian Journal of Mathematics*, vol. 41, no. 6, pp. 1117–1123, 1989.

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

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

[4] ——, "Nonexistence certificates for ovals in a projective plane of order ten," *Proceedings of the 31st International Workshop on Combinatorial Algorithms*, to appear.

[5] M. Hall Jr., "Configurations in a plane of order ten," in *Annals of Discrete Mathematics*. Elsevier, 1980, vol. 6, pp. 157–174.

[6] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "On the existence of a projective plane of order 10," *Journal of Combinatorial Theory, Series A*, vol. 14, no. 1, pp. 66–78, 1973.

[7] M. J. H. Heule, O. Kullmann, and A. Biere, "Cube-and-conquer for satisfiability," in *Handbook of Parallel Constraint Reasoning*. Springer, 2018, pp. 31–59.