Can We Trust the Machine? Auditing Computer-Assisted Proofs

Curtis Bright
University of Waterloo

August 5, 2026

MathFest 2026

Computers and Combinatorics

Part I:
Lam's Problem

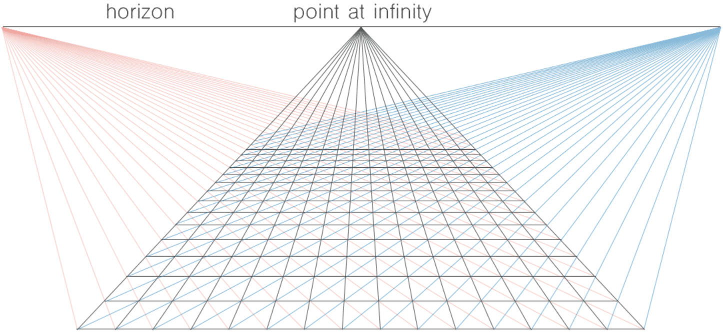
and the projective plane of order ten

Projective Planes

A collection of points and lines is a *projective plane* when

1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.

The real projective plane satisfies these axioms.



Projective Planes

A collection of points and lines is a *projective plane* when

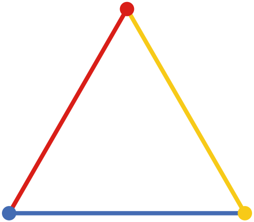
1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.

Do finite projective planes exist?

Projective Planes

A collection of points and lines is a *projective plane* when

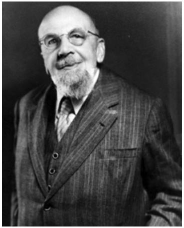
1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.



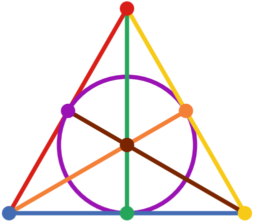
Projective Planes

A collection of points and lines is a *projective plane* when

1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.



Gino Fano

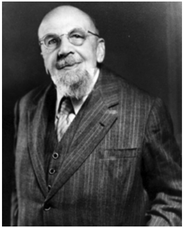


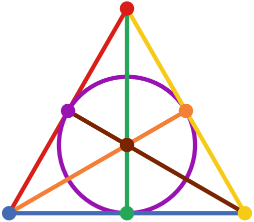
The Fano plane (1892)

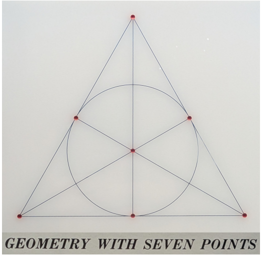
Projective Planes

A collection of points and lines is a *projective plane* when

1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.


Gino Fano


The Fano plane (1892)



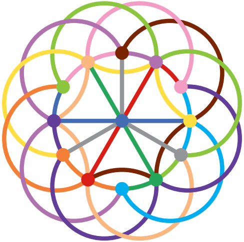
Museum of Science (Boston)

Projective Planes

A collection of points and lines is a *projective plane* when

1. every pair of lines meet in a unique point, and
2. there is a unique line through every pair of points.

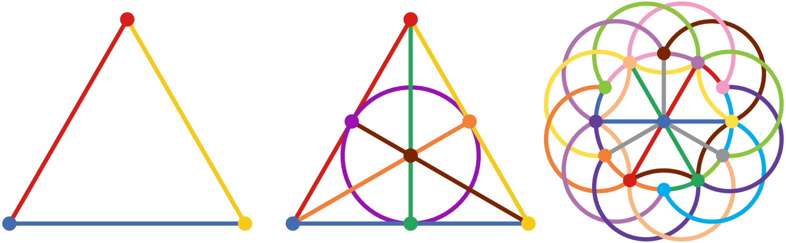
Oswald Veblen



13 points, 13 lines (1906)

The Order of a Plane

A projective plane is said to be of *order* n if all lines pass through exactly $n+1$ points.



PP(1) PP(2) PP(3)

Projective Plane Existence

Veblen and Bussey (1906) constructed projective planes in all prime power orders.

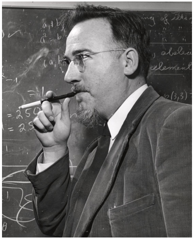
Many more have been constructed since. Moorhouse (2010) found over 309,000 planes of order 49.

The *prime power conjecture* says that projective planes only exist in prime power orders. It is still open and considered the "holy grail" of finite geometry.

Projective Plane Nonexistence

Theorem (Bruck and Ryser, 1949)

If n is not the sum of two integer squares and $n \equiv 1, 2 \pmod 4$ then a $\mathrm{PP}(n)$ *does not exist.*



Projective Plane Orders

6 is not the sum of two squares, so a PP(6) does not exist.

$10 = 1^2 + 3^2$ is the sum of two squares, so the Bruck–Ryser theorem does not apply.

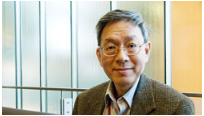
1	2	3	4	5	6	7	8	9	10
✓	✓	✓	✓	✓	✗	✓	✓	✓	?

Lam's Problem

Does a PP(10) *exist?*

No theoretical obstruction is known. If a PP(10) exists, it has

- exactly 111 lines and 111 points, and with
- every line passing through exactly 11 points.



Clement Lam was a PhD student at Caltech in the early 1970s. He was interested in working on this problem...

Incidence Matrices

A PP(n) is equivalent to a $(0, 1)$-matrix with $n + 1$ ones in each row and column that is quad-free (contains no rectangle with 1s in the corners).

1	1	0
1	0	1
0	1	1

PP(1)

1	1	0	1	0	0	0
0	1	1	0	1	0	0
0	0	1	1	0	1	0
0	0	0	1	1	0	1
1	0	0	0	1	1	0
0	1	0	0	0	1	1
1	0	1	0	0	0	1

PP(2)

1	0	0	0	1	0	0	0	1	1	0	0	0
0	0	1	1	0	0	0	1	0	1	0	0	0
0	1	0	0	0	1	1	0	0	1	0	0	0
1	0	0	0	0	1	0	1	0	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	0	0
0	0	1	0	1	0	1	0	0	0	1	0	0
1	0	0	1	0	0	1	0	0	0	0	1	0
0	1	0	0	1	0	0	1	0	0	0	1	0
0	0	1	0	0	1	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1
0	0	0	0	0	0	1	1	1	0	0	0	1
1	1	1	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	1	1	1	1

PP(3)

Coding Theory

The *code* of a PP(n) is the row space of its incidence matrix over $\mathbb{F}_2 = \{0, 1\}$.

Edward Assmus gave a talk at Oberwolfach (1970) where he derived properties of the code generated by a PP(10), e.g., the code is a subspace of $\mathbb{F}_2^{111}$ of dimension 56, assuming it exists.

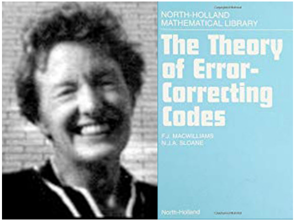
Weight Distribution

The *weight* of an $\mathbb{F}_2$-vector is the number of 1s it contains.

Assmus and Mattson use MacWilliams' identity (1961) to show the striking and strange equation

$$w_{19} = 141w_{12} - 27w_{15} + 7w_{16} + 24675, \qquad \textbf{(!?)}$$

where w_i counts how many vectors of weight i are in the code of a PP(10).



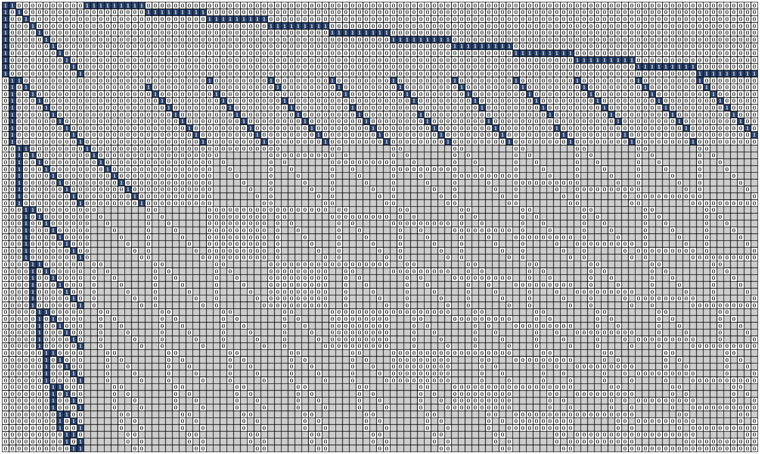
Computer-Assisted Proof

So far, everything could be done "by hand" but we've seemingly reached the limits of human analysis.

Under the assumption $w_{12} > 0$, a computer program explored all possible ways of filling in the unknown entries of the incidence matrix. (Lam, Thiel, Swiercz, McKay 1983)

A Nightmare “Sudoku”

Fill in the gray entries with 1 (blue) or 0 (white) so every row has eleven 1s and the matrix is quad-free. . .



After running for 183 days on a VAX 11/780, Lam et al.'s program determined there was no way of filling in the unknown entries—like a Sudoku with no solution.

Other Searches

There was no PP(10) under the assumption $w_{12} > 0$, so it must be the case that $w_{12} = 0$.

Other similar searches run in the 1970s and 1980s showed $w_{15} = w_{16} = w_{19} = 0$, contradicting the previous weight distribution equation. Thus, a PP(10) does not exist.

Determining $w_{19} = 0$ used around 2 years on a VAX 11/780 and 3 months on a Cray 1A.

Computer Search Solves an Old Math Problem

A math problem with roots that reach back 200 years has been solved by means of a massive computer search

Science, Dec. 16, 1988

Is a Math Proof a Proof If No One Can Check It?

The New York Times, Dec. 20, 1988

“Only An Experimental Result” –Lam

It is particularly difficult to write *optimized* code that is bug-free, and the enormity of Lam’s problem seems to require optimized code.

An independent double-check was performed on a cluster of desktop computers and used around 4 CPU years in 2011.*
Some discrepancies in Lam’s reported results were discovered.

---

*Roy. Confirmation of the non-existence of a projective plane of order 10. Master’s thesis, 2011.

Satisfiability (SAT)

In 2020, I reduced Lam's problem into a problem in Boolean logic.† The advantage of this is twofold:

- We use a highly optimized "SAT solver" (already written) to solve Lam's problem.
- The solver produces a long but auditable *proof log* that can be verified for correctness by relatively simple software.

Check out Bernardo Subercaseaux's talk (Friday 10:40) on applying SAT to mathematical problems, as well as his webpage sat4math.com!

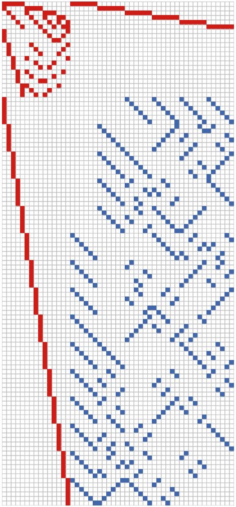
†Bright et al. A SAT-based Resolution of Lam's Problem. AAAI 2021.

Discrepancies

The SAT solver found discrepancies in the reported results of *both* PP(10) prior searches.

On the right is a 51-column partial projective plane found by the SAT solver.

The double-check of Lam's problem purported to show the stronger result that this partial plane does not exist—yet it does.



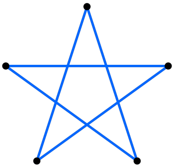
Part II: Ramsey Theory

an audit of $R(3,8) = 28$ *and* $R(3,9) = 36$

Ramsey (p, q)-graphs

A Ramsey (p, q)-graph has no p mutually connected vertices and also no q mutually **un**connected vertices.

The pentagram is a $(3, 3)$-graph.



Ramsey (1930) proved that arbitrarily large (p, q)-graphs do not exist. The pentagram is the largest $(3, 3)$-graph.

Ramsey Numbers

The *Ramsey number* $R(p, q)$ is the first integer for which (p, q)-graphs with $R(p, q)$ vertices stop existing.

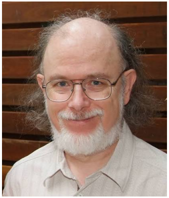
$R(3, 3) = 6$ because the pentagram is the largest $(3, 3)$-graph.

Finding the exact value of Ramsey numbers is a notoriously difficult problem. $R(5, 5)$ is unknown.

$R(3,8)$

Grinstead and Roberts (1972) found a $(3,8)$-graph of order 27. Thus, $R(3,8) > 27$, and this is easy to check.

McKay and Zhang (1992) used a search to prove that there exist no $(3,8)$-graphs of order 28, so $R(3,8) \leq 28$, but we have to take the computer's word for it.



Auditable Proof that $R(3,8) = 28$

A SAT solver starts from "there exists a 28-vertex $(3,8)$-graph" and produces an auditable sequence of logical deductions ending with a contradiction.

This implies $R(3,8) \leq 28$.

$R(3,8) > 27$ is easily auditable, so this gives a complete auditable proof that $R(3,8) = 28$.[‡]

[‡] Li, Duggan, Bright, Ganesh. Verified Certificates via SAT and Computer Algebra Systems for the Ramsey $R(3,8)$ and $R(3,9)$ Problems. IJCAI 2025.

Summary

Using SAT solvers, we generated...

- A 5.8 GiB proof that $R(3, 8) = 28$, verified in 6 hours.
- A 289 GiB proof that $R(3, 9) = 36$, verified in 6 days.
- A 110 TiB proof for Lam's problem, verified in 3.8 years.

No search code is trusted. However, currently the SAT encodings need to be trusted. Eventually, we hope the encodings are verified in a theorem prover like Lean.