The Projective Plane That Wasn't There: How Lam's Problem Was Solved

Curtis Bright
University of Windsor

May 21, 2025

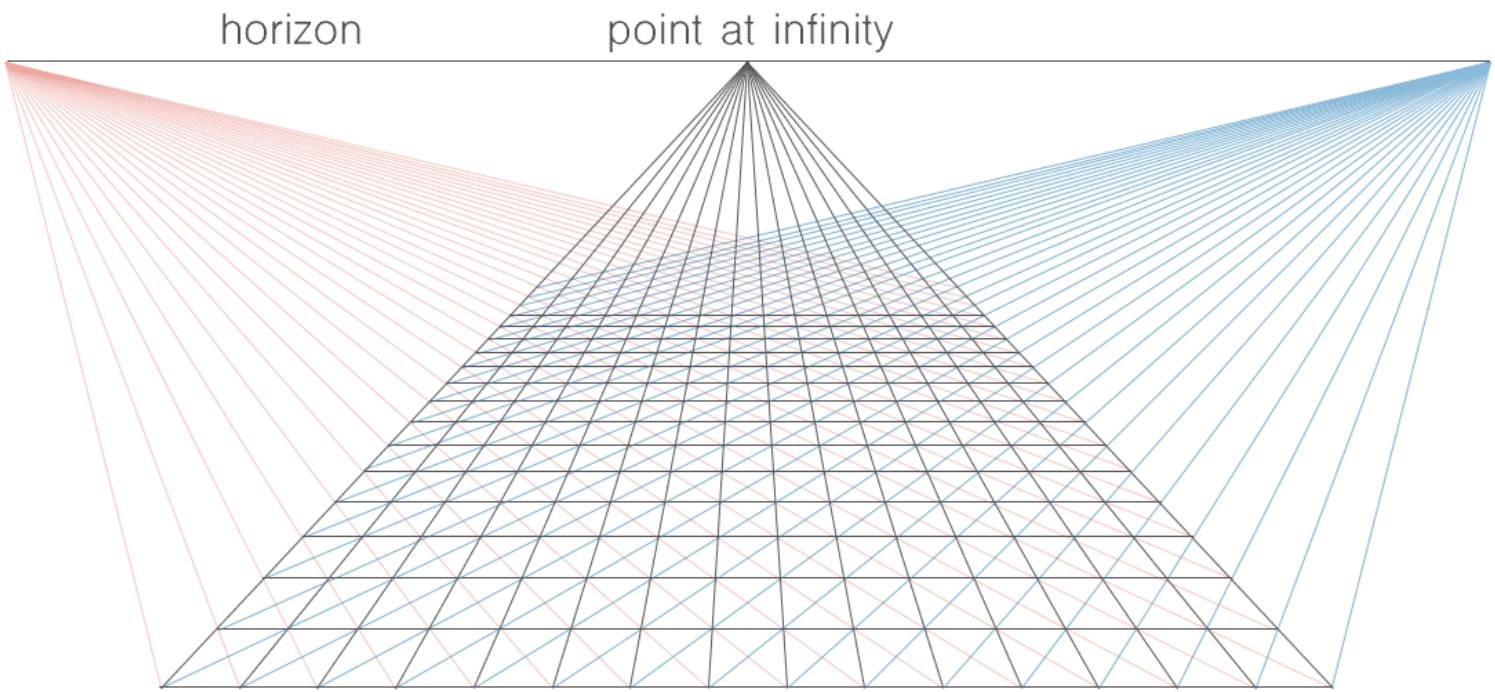
CanaDAM 2025

How Many? The Art and Craft of Counting

Projective Geometry

In the *Euclidean plane*, **any two points define a unique line**, but two lines may or may not meet.

In a *projective plane*, any two points define a unique line, but additionally **any two lines meet at a unique point**.



Finite 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. every pair of points define a unique line.

Similar to how once one knows about infinite fields like $\mathbb{Q}$ or $\mathbb{R}$ one can ask about *field fields*, we can now ask the question:

Do finite projective planes exist?

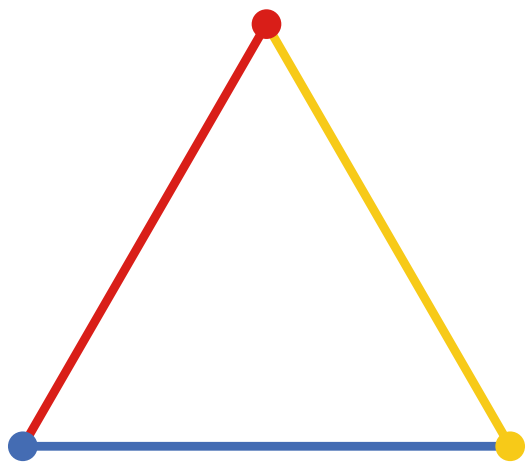
Finite Projective Planes

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

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

Similar to how once one knows about infinite fields like $\mathbb{Q}$ or $\mathbb{R}$ one can ask about *field fields*, we can now ask the question:

Do finite projective planes exist?



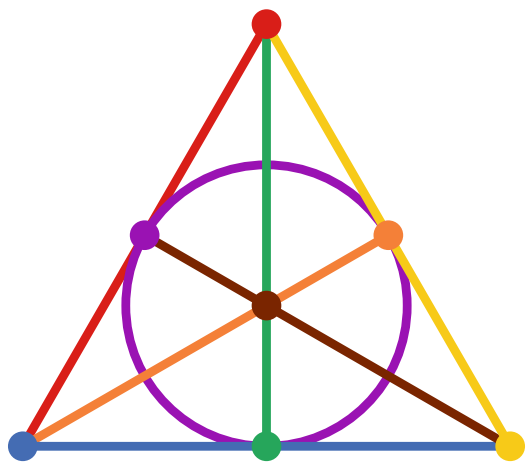
Finite Projective Planes

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

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

Similar to how once one knows about infinite fields like $\mathbb{Q}$ or $\mathbb{R}$ one can ask about *field fields*, we can now ask the question:

Do finite projective planes exist?



The Fano plane

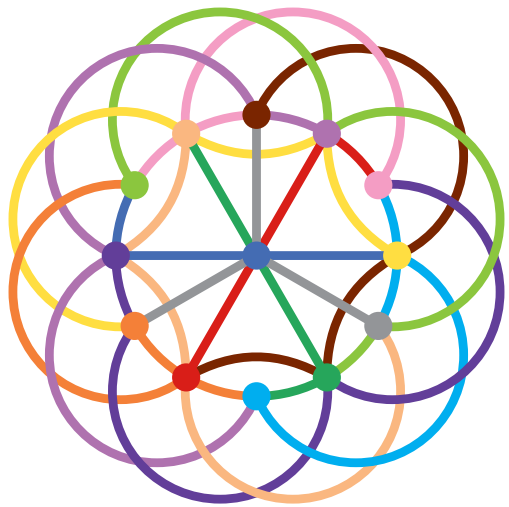
Finite Projective Planes

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

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

Similar to how once one knows about infinite fields like $\mathbb{Q}$ or $\mathbb{R}$ one can ask about *field fields*, we can now ask the question:

Do finite projective planes exist?



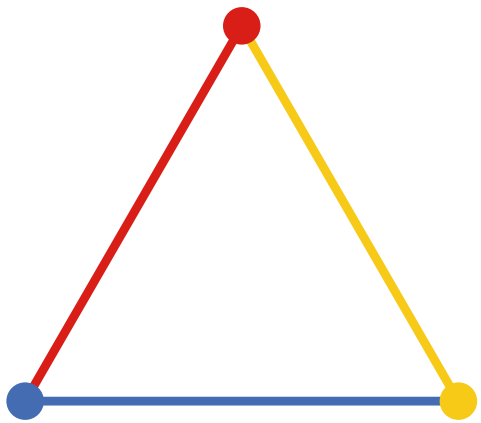
The Order of a Plane

In a projective plane all lines will pass through the same number of points, and a plane is said to be of *order* n if all lines pass through exactly $n + 1$ points.

A projective plane of order n will have exactly $n^2 + n + 1$ points (and the same number of lines).

Incidence Matrices

The *incidence matrix* of a plane is the binary matrix containing a 1 in the (i, j)th entry exactly when line i goes through point j.



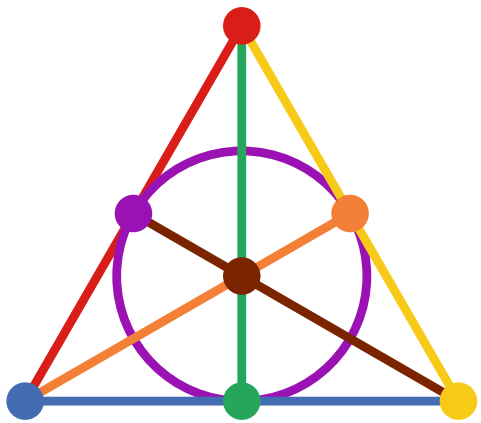
1	1	0
1	0	1
0	1	1

order $n = 1$ (3 lines, 3 points)

Any two incidence matrix rows have an inner product of 1.

Incidence Matrices

The *incidence matrix* of a plane is the binary matrix containing a 1 in the (i, j)th entry exactly when line i goes through point j.



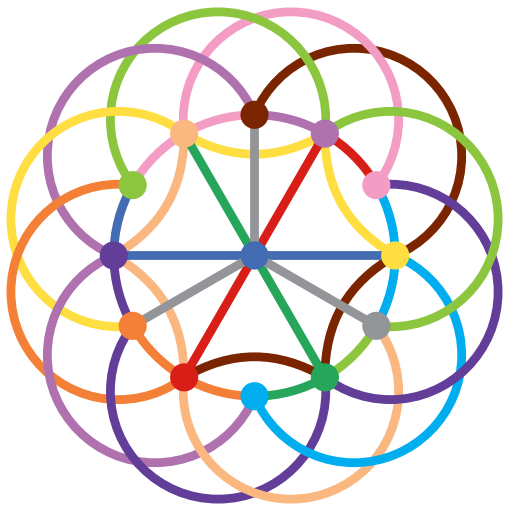
1	1	1	0	0	0	0
1	0	0	1	1	0	0
1	0	0	0	0	1	1
0	1	0	1	0	1	0
0	1	0	0	1	0	1
0	0	1	1	0	0	1
0	0	1	0	1	1	0

order $n = 2$ (7 lines, 7 points)

Any two incidence matrix rows have an inner product of 1.

Incidence Matrices

The *incidence matrix* of a plane is the binary matrix containing a 1 in the (i, j)th entry exactly when line i goes through point j.



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

order $n = 3$ (13 lines, 13 points)

Any two incidence matrix rows have an inner product of 1.

Projective Plane Existence

Projective planes can be constructed in all prime power orders.

The Bruck–Ryser theorem provides nonexistence in some other orders.

Theorem (Bruck and Ryser, 1949)

If $n \equiv 1, 2 \pmod 4$ *and* n *is not the sum of two integer squares then* n *is not the order of a projective plane.*

Projective Plane Orders

Because 6 is not the sum of two squares, 6 cannot be the order of a projective plane.

But $10 = 1^2 + 3^2$ 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 projective plane of order ten exist?

If so, it would contain 111 lines and 111 points. Every line would pass through exactly 11 points and its incidence matrix would be a binary 111×111 matrix A with

$$AA^T = \begin{array}{|c|c|c|c|c|c|}\hline 11 & 1 & 1 & 1 & & 1 \\ \hline 1 & 11 & 1 & 1 & & 1 \\ \hline 1 & 1 & 11 & 1 & & 1 \\ \hline 1 & 1 & 1 & 11 & & 1 \\ \hline & & & & \ddots & \\ \hline 1 & 1 & 1 & 1 & & 11 \\ \hline \end{array}.$$

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

Coding Theory

If A is an $N \times N$ matrix, the linear span of its rows over $\mathbb{F}_2$ is a *binary code* $C = \text{rowspace}(A) \subseteq \mathbb{F}_2^N$.

Theorem (Assmus and Mattson, 1970)

If A is the incidence matrix of a projective plane of order 2 (mod 4) then its code C has dimension $\lceil \#\text{rows}(A)/2 \rceil$.

If A is the incidence matrix of the Fano plane, its associated code C is a linear subspace of $\mathbb{F}_2^7$ of dimension $\lceil 7/2 \rceil = 4$.

The Fano Plane's Code

Since $\dim(C) = 4$ and we are working over $\mathbb{F}_2$, the code C contains $2^4 = 16$ elements (called *codewords*) given below:

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

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

Weight

The *weight* of a codeword is its number of nonzero entries.

Let w_i count the number of vectors in of weight i in C. The *weight enumerator* of C is the polynomial

$$W_C(x) = \sum_{i \geq 0} w_i x^i.$$

For the Fano code, $W_C(x) = 1 + 7x^3 + 7x^4 + x^7$.

Careful Counting

Let C be the code of a projective plane of order ten. This is a subspace of $\mathbb{F}_2^{111}$ of dimension $\lceil 111/2 \rceil = 56$.

Assmus and Mattson show

- $w_0 = 1$,
- $w_i = 0$ for $1 \leq i \leq 10$,
- $w_{11} = 111$,
- $w_i = 0$ for $i \equiv 1, 2 \pmod 4$,
- $w_i = w_{111-i}$ for all i.

Putting these together, there are *only 22 unknowns* in $W_C(x)$:

$$w_{12}, w_{15}, w_{16}, w_{19}, w_{20}, \ldots, w_{55}.$$

The MacWilliams Identity

The *dual code* $C^\perp$ is the orthogonal complement of C (the set of vectors orthogonal to all codewords in C).

Assmus–Mattson show if C is the code associated with a projective plane of order 2 (mod 4), then $C^\perp$ consists of the codewords of C of even weight.

Theorem (MacWilliams, 1961)

If $C \subseteq \mathbb{F}_2^N$ is a linear code then

$$W_{C^\perp}(x) = \frac{(1+x)^N}{|C|} W_C\left(\frac{1-x}{1+x}\right).$$

Letting C be the code of a projective plane of order ten, we can write both sides of the above as a polynomial in x with coefficients in terms of the 22 unknowns $w_{12}, \ldots, w_{55}$.

Then a Miracle Occurs...

Equating coefficients on matching powers of x in MacWilliams' identity and simplifying, all coefficients of $W_C(x)$ can be written in terms of only w_{12}, w_{15}, and w_{16}.

For example, the coefficient of x^{19} is

$$w_{19} = 24675 + 141w_{12} - 27w_{15} + 7w_{16}.$$

This surprising count restricts the number of codewords of small weights 12, 15, 16, and 19.

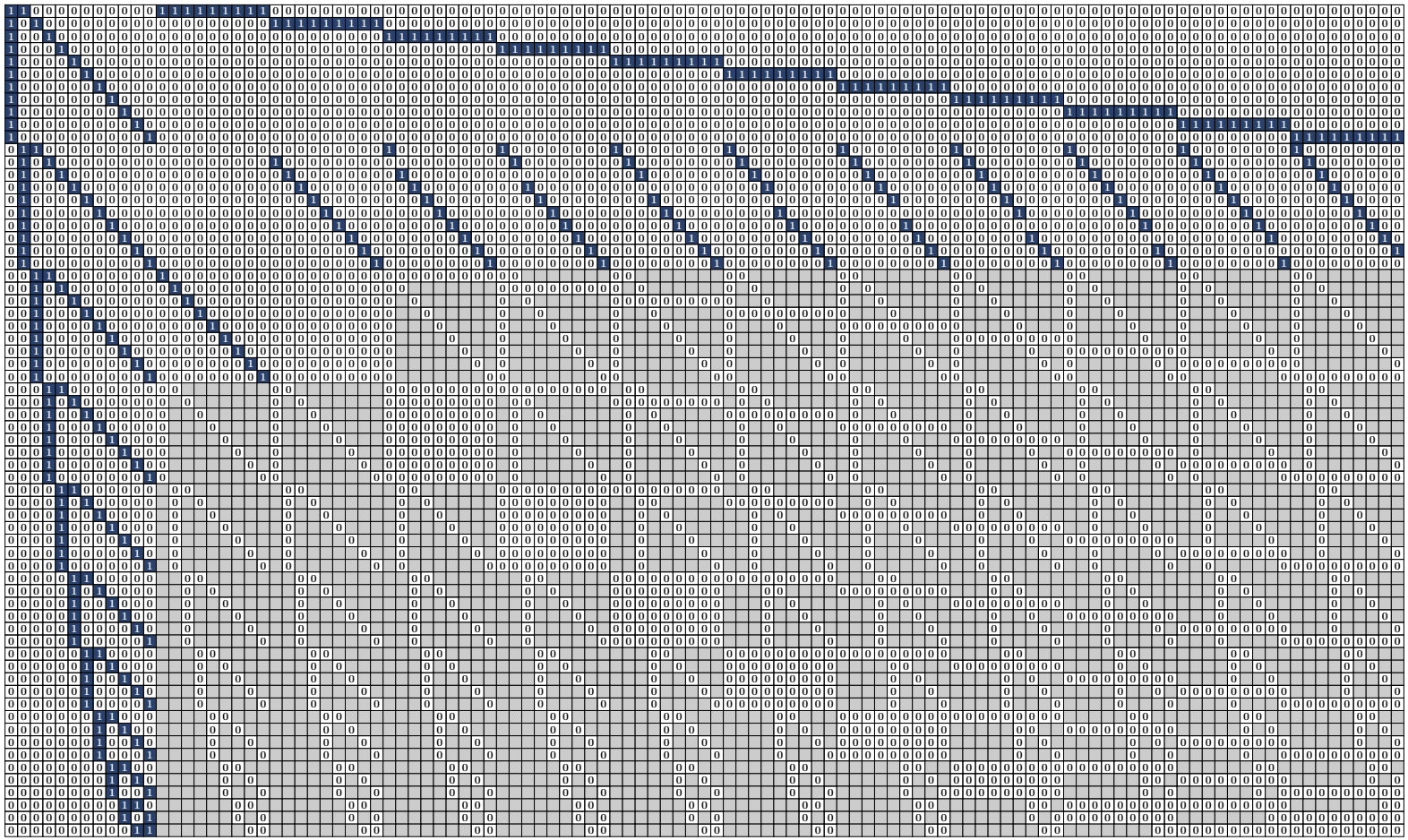
Computer-Assisted Mathematics

So far, everything could feasibly be done "by hand" but we've seemingly reached the limits of theoretical 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 pair of rows has an inner product of 1...



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 solution under the assumption $w_{12} > 0$, so it must be the case that $w_{12} = 0$.

Other similar searches were run in the 1970s and 1980s, assuming the existence of codewords of small weights:

Weight	**Compute Time***	**Publication**
12	4,400 hours	Lam et al. 1983
15	2 hours	MacWilliams et al. 1973
16	3,200 hours	Carter 1974, Lam et al. 1986
19	320,000 hours	Lam, Thiel, Swiercz 1989

*Estimated time on a VAX (one million instructions per second).

Resolution of Lam's Problem

The searches imply that $w_{12} = w_{15} = w_{16} = w_{19} = 0$, resulting in an inconsistent weight enumerator $W_C(x)$, so the projective plane of order ten does not exist.

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

Can We Trust Lam's Result?

Unfortunately, almost all computer programs are full of bugs. This is particularly problematic for programs that purport to show nonexistence.

In 2020, I reduced Lam's problem into logical satisfiability (SAT) problems and used a "SAT solver" to show nonexistence.[†]

This is significantly less error-prone, and we found a few inconsistencies in Lam's original search and an independent verification.[‡]

[†] C. Bright, B. Stevens, K. Cheung, I. Kotsireas, V. Ganesh. 2021.

[‡] D. Roy, Master's Thesis 2011.

The End, For Now

Moreover, SAT solvers produce certificates of nonexistence that can be verified by automatic proof verifiers.

Proof verifiers are trustworthy, and some come with formal proofs of correctness. However, our scripts generating the SAT instances don't have formal proofs.

Eventually, we are hoping to verify the entire proof, including the SAT instances, in a theorem prover.