



planetmath.org

Math for the people, by the people.

finite projective plane

Canonical name	FiniteProjectivePlane
Date of creation	2013-03-22 15:11:15
Last modified on	2013-03-22 15:11:15
Owner	Mathprof (13753)
Last modified by	Mathprof (13753)
Numerical id	11
Author	Mathprof (13753)
Entry type	Topic
Classification	msc 51E15
Classification	msc 51A35
Classification	msc 05B25
Related topic	ProjectivePlane2
Related topic	IncidenceStructures
Related topic	Geometry
Related topic	DeBruijnErdHosTheorem
Defines	prime power conjecture
Defines	planar ternary ring
Defines	PTR

Finite projective planes from axioms

Let us start from the beginning and assume we are given a set of n things called POINTS and a set of ν things called LINES, with an incidence relation between them (a POINT is incident with a LINE iff the LINE is incident with the POINT) that satisfies only two **axioms**, the two unique incidence properties:

- For any two distinct POINTS, there is exactly one LINE through both of them.
- For any two distinct LINES, there is exactly one POINT on both of them.

Given these <http://planetmath.org/node/6940> projective plane axioms we can apply the De Bruijn–Erdős theorem twice (once with the rôle of POINTS and LINES swapped) which tells us we must have $n = \nu$, and one of two possible configurations:

- One “degenerate” solution has one special line ℓ_0 and $n - 1$ ordinary lines ℓ_i , and a special point P_0 and $n - 1$ ordinary points P_i . Each P_i ($i \neq 0$) is incident with its own ℓ_i and with ℓ_0 ; each ℓ_i ($i \neq 0$) with its own P_i and with P_0 . Now ℓ_0 is incident with every point except ℓ_0 while P_0 is incident with every line except ℓ_0 .
- The other solution is a projective plane:
 - the number of POINTS and the number of LINES are of the form $q^2 + q + 1$ for some integer q ;
 - each POINT is incident with $q + 1$ LINES and each LINE with $q + 1$ POINTS.

One usually avoids the degenerate case by demanding there is a **quadrangle** in the plane: four POINTS no three of which lie on the same LINE. This, or a similar non-triviality clause, can then be adopted as a third axiom. Unfortunately it also has the effect of excluding projective planes of orders $q = 0$ and 1. The <http://planetmath.org/DeBruijnErdHosTheorem> De Bruijn–Erdős theorem actually makes an additional assumption: that no two lines are incident with the same set of points (and when applied dually that no two points are incident with the same set of lines). That is not a problem for a LINE incident with more than one POINT or vice versa, because then the axioms forbid it. We just get some more degenerate cases consisting

of multiple lines intersecting one point or none, or vice versa; the insistence on a quadrangle catches these too.

I will not prove the whole theorem here, but under the assumption that a quadrangle exists it is not hard show the interesting part, that those numbers $q+1$ and q^2+q+1 drop out by necessity. The same construction can also be used to give coordinates to the POINTS and LINES of the plane (see below).

Projective planes as bipartite graphs

Projective planes are, apart from anything else, also **bipartite graphs**: let the $q^2 + q + 1$ POINTS be represented by “black” nodes (vertices) of the graph, and let the $q^2 + q + 1$ LINES *also* be nodes, “white” ones say. Edges will represent incidence between a “black” and a “white” node, so there are $(q^2 + q + 1)(q + 1) = q^3 + 2q^2 + 2q + 1$ edges in all.

- In a bipartite graph, nodes of the same color have even distance. This is 0 for any node and itself and **must be 2** for any two distinct nodes of the same color: for any two POINTS there is a path via the LINE they share, and for any two LINES a path via the POINT they share. So distance 4 does not occur.

For nodes of opposite color we can have 1 (if the POINT lies on the LINE) or 3 (otherwise); we can’t have distance 5 which would imply 4 for some nodes. So the graph has **diameter** (maximum distance) 3.

- In a bipartite graph, all cycles (if any) have even length. We don’t have 2-cycles (this is not a multigraph) but no 4-cycles either, by the following argument: such a cycle $P\ell Qm$ would mean two LINES intersecting in two different POINTS, and vice versa. So the **girth** (minimum cycle length) is 6 (showing there indeed are 6-cycles for $q \geq 2$ is left as exercise for the reader).

These two conditions, diameter 3 and girth 6, are not only necessary for the graph to represent a projective plane, they are also sufficient, and therefore form an alternative formulation of what it means to be a projective plane.

These graphs could be called the bipartite analogue of Moore graphs of diameter 2 and girth 5; many of the same arguments can be used [?].

Coördinates for finite projective planes

The details on how to impose coordinates on a projective plane can be found in [?, ?], or in <http://planetmath.org/IntroducingCoordinatesInAProjectivePlane> this entry. We summarize it for a finite projective plane below:

Setup: Use a set Q of q different symbols for coordinate values, two of which are 0 and 1. Start with four POINTS O, I, X, Y forming a quadrangle. XY is the “LINE at infinity” ℓ .

Construction: O and I are given coordinates $(0, 0)$ and $(1, 1)$, and the other POINTS on OI (except its intersection with ℓ) arbitrarily (c, c) with unique $c \in Q$. For any POINT P not on ℓ , let YP intersect OI at (a, a) , and let XP intersect OI at (b, b) . Then P will be given (a, b) . For the coordinates of POINTS on ℓ , intersect the LINES joining $(0, 0)$ with $(1, m)$, for all $m \in Q$, with ℓ , calling the intersection (m) . Finally, Y gets coordinate $()$ (instead of (∞) in the literature).

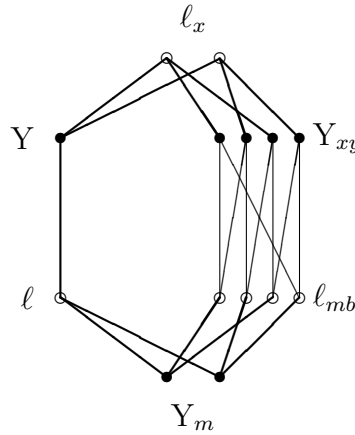
LINES not through Y are given coordinates $[m, k]$ where (m) and $(0, k)$ are their intersections with ℓ and with OY respectively; LINES through Y (other than ℓ) get coordinates $[k]$ going by their intersection $(k, 0)$ with OX . The LINE ℓ gets $[]$ (instead of $[\infty]$ in the literature).

Coordinates from bipartite graphs

The whole business with coordinates becomes a bit more transparent when we try to actually construct the thing as a bipartite graph, starting from one edge, $Y\ell$ say.

There are q more POINTS (other than Y) incident to ℓ , let's call them Y_m where m ranges over the q different values of the set Q . Again, each Y_m is incident to q more LINES (apart from ℓ), let's call those ℓ_{mb} where b is another subscript from Q . Likewise there are q more LINES (other than ℓ) incident to Y , let's call them ℓ_x and to each of them are incident q more POINTS (apart from Y) which we can label Y_{xy} .

This immediately produces the incidence list of the preceding section. Pictorially, for $q = 2$ (with the “to be assessed” portion filled in as thinner lines):



We already have ℓ_0 containing all points Y_{0y} , and in addition if we wanted we could easily arrange for ℓ_{00} to be incident with all the Y_{x0} (just renumber the labels y in the sets Y_{x0} for every x), and for ℓ_{10} to be incident with all the Y_{cc} (just look at which Y_{xy} are incident with ℓ_{10} , then exercise the freedom we still have to relabel all the x , matching each time the corresponding y there). This reproduces the entire coordinatisation.

Projective planes as permutation systems

Five sides of the hexagon are self-evident. On the left we have the single edge $Y\ell$, along the top we fan out in two stages to q and q^2 items, along the bottom we also fan out in two stages to q and q^2 items, and the hard part is the right. We have by now accounted for $2q^2 + 2q + 1$ edges so we know

there must be exactly q^3 more edges, between *some* of those q^2 POINTS and *some* of those q^2 LINES. But where?

For $q = 2$ it is simple enough to avoid 4-cycle clashes (and the diagram shows what is, up to isomorphism, the only solution). In general, it is an open problem to find all possible solutions.

From the projective plane properties it is easy to see that any point Y_{xy} must, for every value of m , be incident to no more than one of the ℓ_{mb} (because if it was incident to two they would intersect both in our Y_{xy} and in their shared Y_m at the bottom). On the other hand, Y_{xy} needs q more mates so it needs to choose exactly one ℓ_{mb} for every value of m .

By exactly the same reasoning, any ℓ_{mb} needs to be incident with, for every value of x , at most one and then exactly one Y_{xy} . In other words, the projective plane structure takes the form of, for each pair of values x and m , a **bijection** ψ_{xm} between the y indices and the b indices.

This is not yet the only constraint. A closer analysis [?] shows that, in order to prevent any two LINES meeting in more than one POINT or any two POINTS in more than two LINES, all compound bijections of the form

$$\psi_{xm}\psi_{x'm}^{-1}\psi_{x'm'}\psi_{xm'}^{-1}$$

(for $m \neq m'$ and $x \neq x'$) must be **derangements**, i.e. permutations that do not leave any index in place. It is not hard to see this is just a device to prevent 4-cycles. And careful scrutiny of the graph shows that, after arranging 5 of 6 edges along trees fanning out as above, and after recognising there are those bijections along the sixth edge, these derangement shenanigans stop the only remaining gap for 4-cycles to lurk.

This could be called the permutation group interpretation of projective plane structure. The algebraic version appears in the next section.

Planar ternary rings

We've been giving our POINTS and LINES coordinates from a set Q of q different labels. We can give Q the structure of a **ternary ring**, that is, a set with a ternary operation $p \bullet q \circ r$, by defining

$$y = x \bullet m \circ b \iff (x, y) \text{ is on } [m, b] \quad (1)$$

Thus, geometric properties of a projective plane may not be analyzed algebraically. See <http://planetmath.org/TernaryRingOfAProjectivePlane> this entry for more detail. Conversely, every ternary ring determines a projective plane with coordinates as above, so that algebraic properties of the ring can be interpreted geometrically. For more detail on this, see <http://planetmath.org/ProjectivePlane> entry.

Fields and division rings are examples of ternary rings. But there are other classes of algebraic structures intermediate between fields and ternary rings. See [?] for a survey. There are four different projective planes known of order 9, many more of order 16, and so on.

Finding all PTRs in general remains of course just as hard as finding projective planes!

Finite projective planes as incidence structures

Finite projective planes can be defined as (**simple square**) $2-(q^2 + q + 1, q + 1, 1)$ **designs**, or what's the same thing, **Steiner systems** $S(2, q + 1, q^2 + q + 1)$. This way, we already *assume* in the definition that each “block” (LINE) contains exactly $q + 1$ POINTS, from which it follows by calculation that the number of LINES that contain a given POINT is also $q + 1$, and that the total number of LINES equals the total number of POINTS.

Also, the unique incidence property that every two POINTS lie together on exactly one LINE is given, and the dual one that every two LINES meet in exactly one POINT then follows from the numbers and the properties that define a design or Steiner system.

We took a different route to projective planes above: we saw we only need to start with these two unique incidence properties, and can *prove* from them that the number of POINTS on a LINE and the number of LINES through a POINT are both fixed (i.e. that the projective plane and its dual are both designs).

Finite projective planes as incidence matrices

Consider an arbitrary projective plane of order q . We know there are $n = q^2 + q + 1$ points and the same number of lines. Let A be an $n \times n$ matrix of which the rows and columns represent lines and points of the plane, and give the value 1 to entries at intersections where the point (represented by the column) lies on the line (represented by the row), and leave the other entries zeros. Such an A is known as the **incidence matrix** of the plane.

AA^\top has rows and columns both representing lines, and the entries here are the dot products of any two rows of A , i.e. the number of points any two lines l and m have in common, which is $q + 1$ when $l = m$ and 1 otherwise, by the projective plane properties.

$$AA^\top = \begin{pmatrix} q+1 & 1 & 1 & \cdots \\ 1 & q+1 & 1 & \cdots \\ 1 & 1 & q+1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = J + qI$$

where I is the identity matrix (ones along the diagonal, zeros everywhere else) and J is the matrix filled with ones in every entry. Note AA^\top has this same value for *every* projective plane with n points and n lines, while A on its own of course varies if there is more than one plane of the same order, as the plane is fully determined by its incidence matrix. Also, AA^\top having this value is the *only* thing needed to make the plane specified by A satisfy the projective plane properties; it is a fully equivalent formulation of those properties.

The **determinant** of A is best evaluated via that of AA^\top , because $(\det A)^2 = (\det A)(\det A^\top) = \det AA^\top$, and we know every entry of AA^\top . The **eigenvalues** of any $n \times n$ matrix of the form $J + qI$ are easily seen to be

- $q + n$ (once) with eigenvector \mathbf{x} for which $x_0 = x_1 = x_2 \dots$
- q (multiplicity $n-1$) for the complementary eigenspace $x_0 + x_1 + x_2 \dots = 0$

by letting the matrix act on these eigenvectors. This gives

$$\det AA^\top = q^{n-1} (q + n)$$

which in our case ($n = q^2 + q + 1$) amounts to

$$\det AA^\top = q^{q^2+q} (q^2 + 2q + 1)$$

As $q^2 + q$ is even and the other factor a square, we get an integer

$$\det A = \pm q^{\frac{q^2+q}{2}} (q+1) = \pm q^{\binom{q+1}{2}} (q+1)$$

where the sign is moot, as A has no correspondence between its columns and rows.

Existence

The **Bruck–Ryser theorem** [?] states that

If q is the order of a projective plane, and $q \equiv 1$ or $2 \pmod{4}$, then q is the sum of two integer squares (one of which can be 0^2).

It can be proven [?, ?] using the incidence matrix A , by a clever rearrangement of $\mathbf{x}A A^T \mathbf{x}$ (plus one extra term) for an arbitrary vector \mathbf{x} , on which gradually constraints are imposed four components at a time using the fact that each integer is a sum of four squares. The argument only works when $q^2 + q + 1 = n \equiv -1 \pmod{4}$, hence the constraint on $q \pmod{4}$.

Interestingly, there is a partial converse [?]: whenever q is allowed by the theorem (either congruent 0 or 3 $\pmod{4}$, or congruent 1 or 2 $\pmod{4}$ and a sum of two squares), there always is a **rational** $n \times n$ matrix A (where $n = q^2 + q + 1$) such that $AA^T = M$. Of course, the matrix is only a proper incidence matrix if that rational matrix only has entries 0 and 1.

The theorem doesn't rule out any potential projective plane orders $q \equiv 0$ or $3 \pmod{4}$, but does rule out a large number of $q \equiv 1$ or $2 \pmod{4}$, starting with $n = 6, 14, 21, 22 \dots$. Note in passing that it is easy to prove no prime power falls foul of Bruck–Ryser, which is just as well, as (classical) planes exist for all those orders.

The only other order ruled out to date is 10, via an epic computer search by Lam, Swiercz and Thiel (read <http://www.cecm.sfu.ca/organics/papers/lam/index.html> for Lam's account).

All projective planes actually found to date, even the non-classical ones, have an order q that is the power of a prime. The **prime power conjecture** says this is the case for all projective planes. It is still open.

References

- [BR49] R. H. BRUCK & H. J. RYSER, “The non-existence of certain finite projective planes” *Can. J. Math.* **12** (1949) pp 189–203
- [HR54] M. HALL, JR. & H. J. RYSER, “Normal completions of incidence matrices” *Amer. J. Math.* **76** (1954) pp 581–9
- [Hal59] MARSHALL HALL, JR., *The Theory of Groups*, Macmillan 1959
- [Cam94] PETER J. CAMERON, *Combinatorics: topics, techniques, algorithms*, Camb. Univ. Pr. 1994, ISBN 0 521 45761 0
<http://www.maths.qmul.ac.uk/~pjc/comb/>
<http://www.maths.qmul.ac.uk/~pjc/com>
 (solutions, errata &c.)
- [CD96] CHARLES J. COLBOURN and JEFFREY H. DINITZ, eds.
The CRC Handbook of Combinatorial Designs,
 CRC Press 1996, ISBN 0 8493 8948 8
<http://www.emba.uvm.edu/~dinitz/hcd.html>
<http://www.emba.uvm.edu/~dinitz/h>
 (errata, new results)
the reference work on designs incl. Steiner systems, proj. planes
- [dRe96] MARIALUISA J. DE RESMINI, “Projective Planes, Nondesarguesian”, pp 708–718 in the previous reference
- [vG03] MARIJKE VAN GANS, M.Phil.(Qual.) thesis, Birmingham 2003