Finite Projective Planes

Thomas Cohn

11/1/18

Yesterday we prove that if $(X, \mathscr{L})$ is a finite projective plane, then

- $(n+1)$ lines through every $x \in X$
- $(n+1)$ points on every line $\ell \in \mathscr{L}$
- $|X| = |\mathscr{L}| = n^2 + n + 1$
- n is the order of the finite projective plane

Defn: If $(X, \mathscr{L})$ is a FPP, then its dual (Y, τ) has a point y_ℓ for every $\ell \in \mathscr{L}$ and a line t_x for every point $x \in X$, and $x \in \ell \Leftrightarrow y_\ell \in t_x$.

Thm: (Y, τ) is also a FPP.
Proof: Let (Y, τ) be the dual of $(X, \mathscr{L})$. Properties P1 and P2 obviously hold by the definition of the dual. So it is enough to show the property P0 holds.
By P0 for $(X, \mathscr{L})$, we have points $\{a, b, c, d\} \subset X$ s.t. $\forall \ell \in \mathscr{L}, |\ell \cap F| \leq 2$. Consider

$$\begin{array}{cccc} \overline{ab} & \overline{cd} & \overline{ad} & \overline{bc} \\ \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow \\ y_{\overline{ab}} & y_{\overline{cd}} & y_{\overline{ad}} & y_{\overline{bc}} \end{array}$$

Then for $\overline{F} = \left\{y_{\overline{ab}}, y_{\overline{cd}}, y_{\overline{ad}}, y_{\overline{bc}}\right\}$; for each point in $\overline{F}$, no line could intersect more than 2 points, or else we would have a line in $\mathscr{L}$ which intersects more than 2 points.
Therefore, property P0 holds, so (Y, τ) is a FPP. $\square$

Construct a bipartite graph from $(X, \mathscr{L})$.

- Let A, B be 2 sets with $|A| = |B| = |X| = |\mathscr{L}|$.
- $a \in A$ is adjacent to $b \in B$ if and only if $x_a \in \ell_b$.

Then $|A| = |B| = n^2 + n + 1$, and for every $a \in A$, every $b \in B$ has degree $n + 1$.

The dual of $(X, \mathscr{L})$ is the one with A and B flipped.

Existence and construction

Existence: $2, 3, 4, 5, \cancel{6}, 7, 8, 9, \cancel{10}, 11, \ldots$
Can we find a pattern? It seems like numbers which are prime or only have one prime factor have a projective plane, but numbers with more than one prime factor do not.
Uniqueness: $2, 3, 4, 5, 7, 8$. 9 does not satisfy uniqueness – there are 3 finite projective planes.

Thm: If n is a prime power, there is a fpp of order n.

Open question: We do not know if there exists a finite projective plane for a non-prime power order.

Defn: A field F is a set with 2 operations $+, \cdot$ with the following rules:

- $a + (b + c) = (a + b) + c$ (+ associativity)
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c)$ ($\cdot$ associativity)
- $a + b = b + a$ (+ commutativity)
- $a \cdot b = b \cdot a$ ($\cdot$ commutativity)
- $a + 0_F = a$ (Existence of the additive identity 0_F)
- $a \cdot 1_F = a$ (Existence of the multiplicative identity 1_F)
- $\forall a \in F, \exists(-a) \in F$ s.t. $a + (-a) = 0_F$ (existence of an additive inverse)
- $\forall a \in F, \exists a^{-1} \in F$ s.t. $a \cdot a^{-1} = 1_F$ (existence of a multiplicative inverse)
- $0_F \neq 1_F$

Ex: $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ are all fields

Ex: $F_2 = \{0_{F_2}, 1_{F_2}\}$, where $1_{F_2} + 1_{F_2} = 0$
$F_3 = \{-1_{F_2}, 0_{F_2}, 1_{F_2}\}$ with the usual multiplication, and $1_{F_2} + 1_{F_2} = -1_{F_2}$, $-1_{F_2} + (-1_{F_2}) = 1_{F_2}$
For prime p, $F_p = \{0, 1, \ldots, p-1\}$ where $i + j = (i + j \pmod p)$ and $i \cdot j = (i \cdot j \pmod p)$.

Thm: If $q = p^k$ for some prime p, then there is a unique finite field F_q with q elements, up to isomorphism.

If q is *not* a prime power, there is not a finite field with q elements.

Constructing a finite projective plane from a finite field:

1. Consider a field F. Let $V = F^3 = F \times F \times F$, a vector space on the field F.
2. Let X be the set of 1-dimensional subspaces in V.
3. Let $\mathscr{L}$ be the set of 2-dimensional subspaces in V.

Then we claim that $(X, \mathscr{L})$ forms a finite projective plane, with $x \in \ell \Leftrightarrow S_x \subset T_\ell$.

Goal: $|X| = q^2 + q + 1$.
$F_q^3 = \{(x, y, z) : x, y, z \in F_q\}$. So there are $q^3 - 1$ non-zero points in F_q^3. But there are q points in every 1-dimensional subspace, so we need to divide by $q - 1$. This gives us $|X| = \frac{q^3-1}{q-1} = q^2 + q + 1$

Thm: If G on n vertices has no $K_{2,2}$ subgraphs, then $|E| \leq \frac{1}{2}(n^{3/2} + n)$. We proved this previously.

Thm: For infinitely many values m, there is a $K_{2,2}$-free graph on m vertices, with at least $0.35m^{3/2}$ edges.

Proof: Let $q = p^k$. Then consider $(X, \mathscr{L})$ of order q. Construct a bipartite graph: $\overline{x\ell} \leftrightarrow x \in \ell$.
Then there are $m = |X| + |\mathscr{L}| = 2(q^2 + q + 1)$ vertexes.
And there are $|E| = (q^2 + q + 1)(q + 1)$ edges.

$$|E| = (q^2 + q + 1)(q + 1) \geq (q^2 + q + 1)\sqrt{q^2 + q + 1} = (q^2 + q + 1)^{3/2} = \left(\frac{m}{2}\right)^{3/2} \approx 0.35m^{3/2} \quad . \square$$

The 0.35 can be improved to 0.5. The "sharp" asymptotics is $\frac{1}{2}m^{3/2}$.