p–Ranks of Nets

G. Eric Moorhouse
University of Wyoming

Motivation

A *projective plane* of order n has

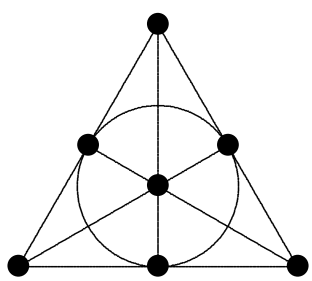
$n^2 + n + 1$ points;

$n^2 + n + 1$ lines;

$n + 1$ points on each line;

$n + 1$ lines through each point.

Example: The projective plane of order $n = 2$



7 points

7 lines

3 points on each line

3 lines through each point

Open Problems

- Must every finite projective plane have prime power order?
- Must every projective plane of prime order $n = p$ be classical? (points = 1-dim subspaces of $\mathbb{F}_p^3$, lines = 2-dim subspaces)

Brief History

Theorem (Bruck and Ryser, 1949). *If there is a projective plane of order $n \equiv 1, 2 \mod 4$, then $n = a^2 + b^2$.*

Proof uses congruence of rational quadratic forms.

Although $10 = 1^2 + 3^2$, we have

Theorem (Lam et al., up through 1989). *There is no projective plane of order 10.*

Proof uses the fact that the extended binary code $\mathcal{C}$ of the plane is self-dual. This restricts the weight enumerator of $\mathcal{C}$. The computer is used extensively to eliminate possibilities for small weight codewords.

These approaches are *global*.

A more *local* approach:

$$\left.\begin{array}{l}\text{proj. plane}\\ \text{of order } n\end{array}\right\} \longleftrightarrow \begin{cases}n{-}1 \text{ mutually}\\ \text{orthogonal}\\ \text{quasigroups on}\\ X=\{1,2,3,\ldots,n\}\end{cases}$$

Two quasigroups $(X,*)$, $(X,\circ)$ are *orthogonal* if the map

$$X\times X\to X\times X, \qquad (x,y)\mapsto(x*y,\,x\circ y)$$

is bijective.

WLOG these quasigroups all have left identity 1:

$$1*x=x \quad \text{for all } x\in X$$

The *left-multiplication group of* $(X, *)$ is the subgroup $G_* \leq Sym(X)$ generated by all permutations

$$\lambda_a : X \to X, \quad x \mapsto a * x$$

for $a \in X$.

Isotopic quasigroups $(X, *)$, $(X, \circ)$ *need not* have equivalent left-multiplication groups.

But if both $(X, *)$, $(X, \circ)$ have left-identity then there exists an isomorphism $\phi : G_* \to G_\circ$ and a bijection $\theta : X \to X$ such that for all $g \in G_*$, the diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad g \quad} & X \\ \theta \big\downarrow & & \big\downarrow \theta \\ X & \xrightarrow{\quad \phi(g) \quad} & X \end{array}$$

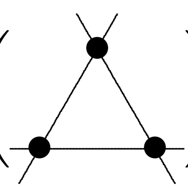
commutes.

The p-rank concept

If A is any matrix with integer entries,

$$\text{rank}_p(A) = \begin{array}{l}\text{rank of } A \\ \text{over any field of} \\ \text{prime characteristic } p\end{array}$$

The p-rank of any point-line incidence structure is the p-rank of its point-line incidence matrix, e.g.

$\text{rank}_p \Big($  $\Big)$

$$= \text{rank}_p \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

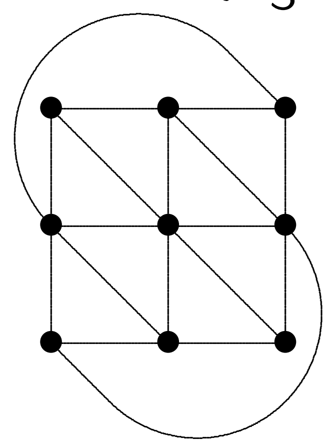
$$= \begin{cases} 2, & \text{if } p = 2; \\ 3, & \text{otherwise.} \end{cases}$$

Typically, the *more 'symmetric'* a structure with given parameters, the *lower* its p-rank for certain choices of the prime p which depend on the parameters.

A quasigroup $(X, *)$ of order n determines a *3-net*, eg.

Quasigroup $(X, *)$ $\longleftrightarrow$ 3-Net $\mathcal{N}_3$

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \longleftrightarrow$$



$n \times n$

n^2 points;

$3n$ lines;

3 parallel classes of n lines each;

n points on each line

Problem: Determine the p-rank of $\mathcal{N}_3$ in terms of algebraic properties of $(X, *)$ or of G_*.

Let $|X| = n = p^a m$, $p \not| m$ (denoted $p^a || n$).

Theorem (1991). $\mathrm{rank}_p \mathcal{N}_3 = 3n - 2 - e$ *where* $e \leq a$ *and*

$$|X/Y| = p^e, \quad Y = \bigcap \{Q : Q \text{ normal in } X, \; X/Q \text{ elem. abel. } p\text{-gp}\}.$$

Theorem (2000). $\mathrm{rank}_p \mathcal{N}_3 = 3n - 2 - e$ *where* $e \leq a$ *and*

$$|G_*/K| = p^e, \quad K = \bigcap \{L : H \leq L \trianglelefteq G_*, \; G_*/L \text{ elem. abel. } p\text{-gp}\};$$

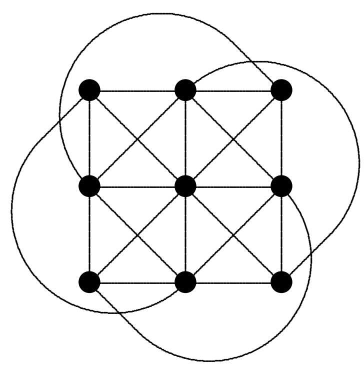
here H *is the stabilizer of an element of* X.

Nets

$k-2$ mutually orthogonal quasigroups of order n ($k \leq n+1$) $\longleftrightarrow$ k-net $\mathcal{N}_k$ of order n:

- n^2 points, nk lines;
- k parallel classes of n lines each;
- n points on each line

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \longleftrightarrow$$



eg. 4-net (affine plane) of order 3

$n-1$ mutually orthogonal quasigroups of order n $\longleftrightarrow$ $(n-1)$-net $\mathcal{N}_{n-1}$ of order n (affine plane)

$\longleftrightarrow$ projective plane of order n

Conjecture (1991). *If $p||n$ then*

$$\mathrm{rank}_p\mathcal{N}_k - \mathrm{rank}_p\mathcal{N}_{k-1} \geq n-k+1.$$

If this Conjecture holds then every projective plane of *squarefree* order n, or order $n \equiv 2 \bmod 4$, is classical with $n = p =$ prime.

The conjecture holds for

(i) $k \leq 3$;

(ii) translation nets with an abelian translation group (in particular equality holds in the classical case);

(iii) 4-nets of prime order with a central translation (i.e. 4-nets constructible from $3 \times p$ difference matrices over a group of prime order p);

(iv) direct products of smaller nets which also satisfy the conjecture.

Proof techniques:

loop ‘characters’ or group theory;

group algebras over $\mathbb{F}_p$, in particular Jennings’ 1941 study of the powers of the augmentation ideal.

This suggests using quasigroup algebras over $\mathbb{F}_p$ in the general case.

Back to 3-nets. . .

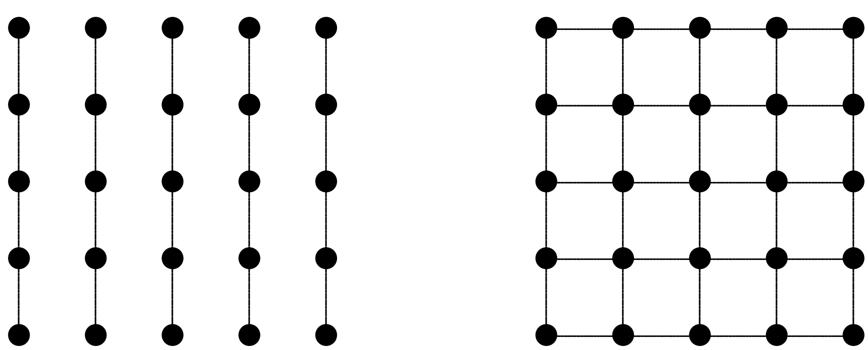
Consider the 3-net $\mathcal{N}_3$ corresponding to a quasi-group $(X,*)$ of order n. This has three parallel classes of lines:

$$\ell_{1,a} = \{(a,y) : y \in X\};$$
$$\ell_{2,b} = \{(x,b) : x \in X\};$$
$$\ell_{3,c} = \{(x,y) : x * y = c\}.$$

Let $\mathcal{L}_i = \langle \ell_{i,z} : z \in X\rangle_F$, $F = \mathbb{F}_p$. Clearly

$\dim_F \mathcal{L}_i = n$;

$\dim_F(\mathcal{L}_i + \mathcal{L}_j) = 2n-1$ for $i \neq j$.



Also

$$\begin{aligned}\dim(\mathcal{L}_1+\mathcal{L}_2+\mathcal{L}_3) &= \dim(\mathcal{L}_1+\mathcal{L}_2) + \dim \mathcal{L}_3 \\ &\qquad - \dim((\mathcal{L}_1+\mathcal{L}_2) \cap \mathcal{L}_3) \\ &= 3n-1 - \dim((\mathcal{L}_1+\mathcal{L}_2) \cap \mathcal{L}_3)\end{aligned}$$

Lemma. *We have an exact sequence*

$$0 \to F \to (\mathcal{L}_1+\mathcal{L}_2)\cap\mathcal{L}_3 \xrightarrow{\partial} B^1(X)^{G_*} \longrightarrow 0$$

where $B^1(X)^{G_*}$ is the set of all maps $X \times X \to F$ of the form $(x,y) \mapsto f(y) - f(x)$ which are G_*-invariant, i.e.

$$f(y) - f(x) = f(gy) - f(gx) \quad \text{for all } g \in G_*\,.$$

Corollary. $\mathrm{rank}_p \mathcal{N}_3 = 3n - 2 - \dim B^1(X)^{G_*}\,.$

More generally, let G be a transitive permutation group on X, $|X| = n = p^a m$, $p \nmid m$.

Theorem. $\dim B^1(X)^G = e \le a$ *where*

$$|G/K| = p^e, \qquad K = \bigcap \{L : H \le L \trianglelefteq G,\ G/L \text{ elem. abel. } p\text{-gp}\};$$

here H is the stabilizer of an element of X.