Quasigroup Cohomology and p-Ranks of Nets

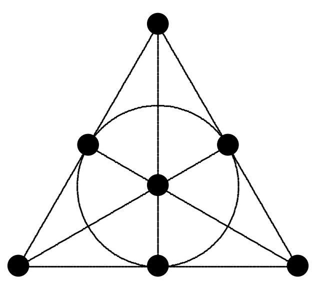
G. Eric Moorhouse
University of Wyoming

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* $n = a^2 + b^2$.

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

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

A *quasigroup* is a finite set X with a binary operation $*$ such that

(i) for all $x \in X$, the map $y \mapsto x*y$ is bijective on X; and

(ii) for all $y \in X$, the map $x \mapsto x*y$ is bijective on X.

We will always take $X = \{1, 2, \ldots, n\}$ and assume 1 is a *left-identity:*

(iii) $1 * x = x$ for all $x \in X$

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

Example: $X = \{1, 2, \ldots, 13\}$, $*$ has multiplication table

eg. $2 * 6 = 7$

$$\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
9 & 4 & 10 & 8 & 2 & 7 & 13 & 6 & 5 & 11 & 1 & 3 & 12 \\
11 & 3 & 12 & 2 & 6 & 13 & 9 & 10 & 1 & 5 & 4 & 8 & 7 \\
5 & 13 & 11 & 7 & 10 & 12 & 8 & 9 & 2 & 4 & 6 & 1 & 3 \\
6 & 8 & 2 & 5 & 12 & 3 & 10 & 4 & 7 & 1 & 13 & 11 & 9 \\
12 & 5 & 6 & 10 & 1 & 11 & 2 & 7 & 3 & 9 & 8 & 13 & 4 \\
8 & 12 & 5 & 13 & 9 & 4 & 3 & 11 & 6 & 2 & 10 & 7 & 1 \\
4 & 6 & 9 & 12 & 7 & 5 & 1 & 13 & 8 & 3 & 2 & 10 & 11 \\
10 & 7 & 13 & 3 & 4 & 1 & 12 & 2 & 11 & 8 & 5 & 9 & 6 \\
3 & 1 & 7 & 9 & 11 & 2 & 4 & 5 & 10 & 13 & 12 & 6 & 8 \\
7 & 11 & 4 & 1 & 8 & 10 & 6 & 3 & 13 & 12 & 9 & 2 & 5 \\
13 & 10 & 8 & 11 & 3 & 9 & 5 & 1 & 12 & 6 & 7 & 4 & 2 \\
2 & 9 & 1 & 6 & 13 & 8 & 11 & 12 & 4 & 7 & 3 & 5 & 10
\end{bmatrix}$$

Here $G \cong PSL(3,3) \leq S_{13}$.

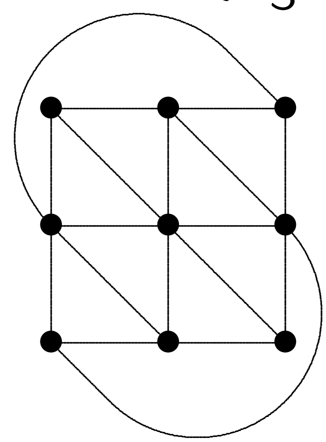
A quasigroup $(X, *)$ of order n determines a *3-net*, eg.

Quasigroup $(X, *)$

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

$n \times n$

3-Net $\mathcal{N}_3$



n^2 points;

$3n$ lines;

3 parallel classes of n lines each;

n points on each line

Problem: Determine the p-rank of $\mathcal{N}_3$ (i.e. of the point-line incidence matrix of $\mathcal{N}_3$) in terms of properties of $(X, *)$ or of G.

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

Theorem (1991). *$\text{rank}_p \mathcal{N}_3 = 3n-2-e$ 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). *$\text{rank}_p \mathcal{N}_3 = 3n-2-e$ 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.

Connection to Projective Planes

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

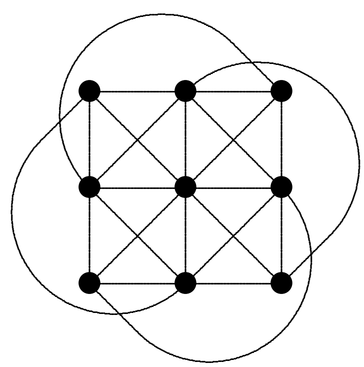
$$X^2 \to X^2, \quad (x,y) \mapsto (x*y, x\circ y)$$

is bijective.

$k-2$ mutually orthogonal quasigroups of order n ($k \le n+1$) $\longleftrightarrow$ 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*

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

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.

Cohomology

Let G be a permutation group on X. Fix a prime field $F = \mathbb{F}_p$.

For $k \geq -1$, a *k-cochain* is a map $f : X^{k+1} \to F$. These form a vector space $C^k(X)$ of dimension n^{k+1} over F.

The *coboundary operator* $\partial : C^k \to C^{k+1}$ is the linear transformation $f \mapsto \partial f$ where

$$(\partial f)(x_0, x_1, \ldots, x_{k+1}) = \sum_{i=0}^{k+1} (-1)^i f(x_0, \ldots, \widehat{x_i}, \ldots, x_k)\,.$$

Then $\partial^2 = 0$, giving the *cochain complex*

$$0 \xrightarrow{0} F \xrightarrow{\partial} C^0(X) \xrightarrow{\partial} C^1(X) \xrightarrow{\partial} C^2(X) \xrightarrow{\partial} \cdots$$

$$Z^k(X) = \mathrm{ker}(\partial : C^k(X) \to C^{k+1}(X))$$
$$= \{k\text{-}\textit{cocycles}\}$$
$$\bigcup\!|$$
$$B^k(X) = \mathrm{im}(\partial : C^{k-1}(X) \to C^k(X))$$
$$= \{k\text{-}\textit{coboundaries}\}$$

$C^k(X)$ is a left G-module via

$$(gf)(x_0, x_1, \ldots, x_k) = f(gx_0, gx_1, \ldots, gx_k)$$

and the action of G commutes with ∂.

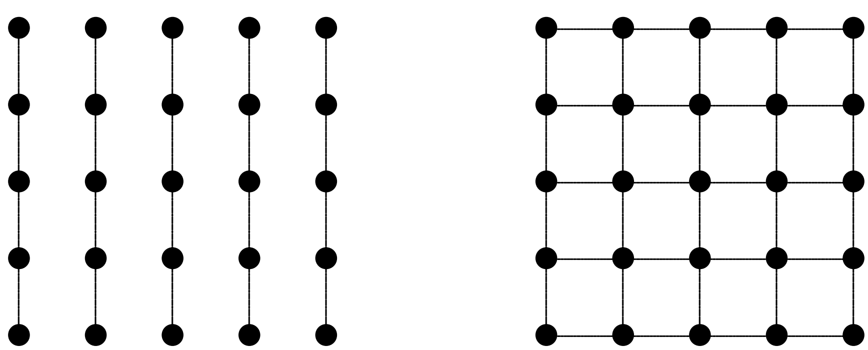
f is *G-invariant*, denoted $f \in C^k(X)^G$, if $gf = f$ for all $g \in G$.

Back to 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 $\mathcal{L}_i = \langle \ell_{i,z} : z \in X \rangle_F$. Clearly
$\dim_F \mathcal{L}_i = n$;
$\dim_F(\mathcal{L}_i + \mathcal{L}_j) = 2n - 1$ for $i \neq j$.



Also

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

Lemma. *The restriction of* $\partial : C^0(X) \to B^1(X)$ *to a certain subspace* $U \cong ((\mathcal{L}_1+\mathcal{L}_2)\cap\mathcal{L}_3)$ *induces an exact sequence*

$$0 \ \to\ Z^0(X)\ \to\ U\ \xrightarrow{\partial|_U}\ B^1(X)^G\ \longrightarrow 0\,.$$

Proof. $(\mathcal{L}_1+\mathcal{L}_2)\cap\mathcal{L}_3$

$$\cong U = \{c \in C^0(X)\ :\ \sum_{x\in X} c(x)\ell_{3,x} = \sum_{x\in X}(a(x)\ell_{1,x} + b(x)\ell_{2,x}), \text{ some } b, c \in C^0(X)\}.$$

Evaluating at $(x,y)-(x,1)-(1,y)+(1,1)$ gives $c \in U$ iff

$$c(x*y) = c(x*1) + c(y) - c(1)$$
for all $x, y \in X$.

This implies that the map $\partial c \in B^1(X)$ is G-invariant:

$$\begin{aligned}(\partial c)(u*x, u*y) &= c(u*y) - c(u*x) \\ &= (c(u*1) + c(y) - c(1)) \\ &\qquad - (c(u*1) + c(x) - c(1)) \\ &= c(y) - c(x) \\ &= (\partial c)(x,y).\end{aligned}$$

Thus $\partial U \subseteq B^1(X)^G$. Conversely, given $\partial c \in B^1(X)^G$ where $c \in C^0(X)$, we take $a(x) = c(x*1)$, $b(x) = c(x) - c(1)$ to get $c \in U$.

Finally, $\ker(\partial|_U) = U \cap Z^0(X) = Z^0(X)$ since $Z^0(X) \cong F$ consists of constant functions $x \mapsto c$; these lie in U since

$$\sum_{x\in X} c\ell_{3,x} = \sum_{x \in X} (c\ell_{1,x} + 0\ell_{2,x}). \qquad \square$$

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

As before, $|X| = n = p^a m$, $p \not| m$.

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

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

here H is the stabilizer of an element of X.

Proof. Denote by V the F-vector space of maps $f : G \to F$ vanishing on H such that

$$f(gh) = f(g) + f(h) \quad \text{for all } g, h \in G.$$

Such maps have $\ker f \supseteq K$ and $\dim V = e$. We construct

$$\phi : B^1(X)^G \xrightarrow{\cong} V$$

as vector spaces over F. Fix $x_0 \in X$. Given $b \in B^1(X)^G$, define

$$\phi b : G \to F, \quad g \mapsto b(x_0, gx_0).$$

Then $\phi b \in V$ since

$$
\begin{aligned}
0 &= (\partial b)(x_0, gx_0, ghx_0) \\
&= b(gx_0, ghx_0) - b(x_0, ghx_0) + b(x_0, gx_0) \\
&= b(x_0, hx_0) - b(x_0, ghx_0) + b(x_0, gx_0) \\
&= (\phi b)(h) - (\phi b)(gh) + (\phi b)(g).
\end{aligned}
$$

Clearly $\phi(a+b) = \phi a + \phi b$, and if $\phi b = 0$ then

$$b(gx_0, hx_0) = b(x_0, g^{-1}hx_0) = (\phi b)(g^{-1}h) = 0$$

and the transitivity of G on X gives $b = 0$.

To show ϕ is onto: Let $f \in V$. Define $c_f \in C^0(X)$ by

$$c_f(gx_0) = f(g).$$

This is well-defined since f vanishes on H, the stabilizer of x_0. Now

$$
\begin{aligned}
(\partial c_f)(x_0, gx_0) &= c_f(gx_0) - c_f(x_0) \\
&= f(g) - f(1) = f(g)
\end{aligned}
$$

gives $\phi(\partial c_f) = f$.

Finally, K has p^e equal-sized orbits on X, so $p^e | n$ and $e \leq a$. $\square$