Sharply Transitive Sets of Permutations

Peter Müller (joint with Gábor Nagy)

Vienna, July 6th 2012

Notation

Ω:	Finite set
$\mathrm{Sym}(\Omega)$:	Symmetric group on Ω
$\mathrm{Sym}(n)$:	Symmetric group on $\{1, 2, \ldots, n\}$

Definition

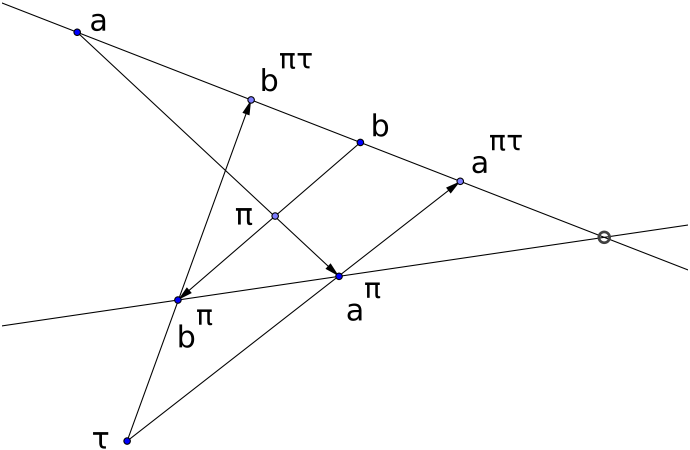
$S \subseteq \mathrm{Sym}(\Omega)$ sharply transitive:
For any $\alpha, \beta \in \Omega$ exactly one $g \in S$ with $\alpha^g = \beta$

Definition

$S \subseteq \mathrm{Sym}(\Omega)$ sharply 2–transitive:
S sharply transitive on pairs (α_1, α_2), $\alpha_1 \neq \alpha_2$

Observation by Ernst Witt:

Projective plane of order n $\Longleftrightarrow$ $S \subseteq \mathrm{Sym}(n)$ sharply 2–transitive



Results by

- Lorimer 1973 (three papers)
- O'Nan 1985
- Grundhöfer & Müller 2009
- Müller & Nagy 2011

yield:

Theorem

Take $S \subseteq Sym(n)$ *sharply 2–transitive, set* $G = <S>$. *Then:*

(a) $n = p^e$, $G \leq \mathrm{AGL}_e(\mathbb{F}_p)$, *or*

(b) $G = Alt(n)$ *or* $Sym(n)$, *or*

(c) $G = M_{24}$

P_g = permutation matrix of g

From

$$S \text{ sharply transitive} \iff \sum_{g \in S} P_g = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

we get

$$G \leq \mathrm{Sym}(\Omega) \text{ contains sharply transitive set}$$

$$\iff$$

$$\sum_{g \in G} x_g P_g = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} \text{ has solution } x_g \in \{0, 1\}$$

Lemma (Contradicting subset lemma)

$S \subseteq Sym(\Omega)$ sharply transitive. $B, C \subseteq \Omega$ arbitrary. Then

$$\sum_{g \in S} |B \cap C^g| = |B||C|$$

Proof.

Count triples $(b, c, g) \in B \times C \times S$ with $b = c^g$! □

Alternating groups

Theorem

$S \subseteq Alt(n)$ sharply 2–transitive. Then $n \equiv 0$ or $1 \pmod 4$

Proof.

Set $B = \{(i,j) \mid i < j\},\ C = \{(i,j) \mid i > j\}$

$$|B \cap C^g| = \text{number of } i < j \text{ with } i^{g^{-1}} > j^{g^{-1}} \text{ is even}$$

Thus

$$(\frac{n(n-1)}{2})^2 = |B||C| = \sum_{g \in S} |B \cap C^g|$$

is even

□

Symmetric block designs

Theorem (O'Nan)

$P\Gamma L(m,q)$, $m \geq 3$, has no sharply 2–transitive subset

Remark

$\mathrm{P\Gamma L}(m,q)$ is automorphism group of symmetric block design

Symmetric (ν, k, λ)–design

- ν: number of points
- k: size of a block
- λ: size of intersection of two distinct blocks

$$\boxed{(\nu-1)\lambda = k^2 - k} \quad \boxed{k(\nu-k) = (k-\lambda)(\nu-1)}$$

Theorem

Let $\Omega \cup \{x\}$ be the points of symmetric (ν, k, λ)–design. Then Aut(*Design*) *contains no sharply transitive set on Ω.*

Proof.

S sharply transitive on $\Omega \implies |S| = |\Omega| = \nu - 1$

(i) $B = C \subseteq \Omega$ is block, hence $|B \cap C^g| = k$ or $\lambda \Rightarrow$
$ak + (\nu - 1 - a)\lambda = \sum_{g \in S} |B \cap C^g| = |B||C| = k^2 \Rightarrow$
$a(k - \lambda) = k$

(ii) $B \cup \{x\} = C \cup \{x\}$ is block, hence $|B \cap C^g| = k - 1$ or $\lambda - 1$
$b(k-1) + (\nu - 1 - b)(\lambda - 1) = (k-1)^2 \Rightarrow$
$b(k - \lambda) = \nu - k$

$$\left.\begin{array}{c|l} k - \lambda & \nu \\ (k-\lambda)^2 & k(\nu - k) = (k-\lambda)(\nu - 1) \end{array}\right\} \Rightarrow k - \lambda = 1$$

Hence $k = 1$ or $\nu - 1$ (trivial design) □

Unfortunately ...

$$\sum_{g\in G} x_g P_g = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} \tag{1}$$

has integral solutions in many interesting cases:

- $G = M_{24}$ of degree $23 \cdot 24$, or
- $G = \mathrm{Sym}(n)$ of degree $(n-1)n$ (not confirmed)

Too naive?

Use additional equation

$$\sum_{g\in G} x_g^2 = n \tag{2}$$

Every integral solution of (1) and (2) is $\{0,1\}$–solution

Size of complete subgraphs, Lovász and Schrijver bounds

Definition

Given a graph. Consider real symmetric matrix $A = (a_{ij})$ with

$$a_{ij} = \begin{cases} 1 \text{ or } \geq 1 \text{ arbitrary}, & \text{if } i = j \text{ or } (i,j) \text{ is edge} \\ \text{arbitrary}, & \text{otherwise} \end{cases}$$

Theorem (Lovász, Schrijver)

S complete subgraph. If $\rho E - A$ positive semidefinite, then $|S| \leq \rho$.

Proof.

v = characteristic vector of S:

$$v^t(\rho E - A)v \geq 0, \text{ hence}$$

$$\rho v^t v \geq v^t A v = \sum_{i,j \in S} a_{ij} \geq |S|^2 = |S| v^t v$$

□

Example

Fixed point free elements

$S \subseteq G$ sharply transitive, $\pi(g) =$ number of fixed points of g

(a) $\pi(g/h) = 0$ for all $g \neq h \in S$

(b) Pick any $s \in S$. Then Ss^{-1} is sharply transitive too

Set $G^\star = \{g \in G | \pi(g) = 0\}$. May assume $S \subseteq \{e\} \cup G^\star$.

Plane of order 6

$G = \mathrm{Sym}(6)$ on $5 \cdot 6 = 30$ points.

- Vertices $= G^\star$
- Edges $=$ pairs (g, h) if $\pi(g/h) = 0$

S complete subgraph. Need to show: $|S| \leq 28$.

Lovász:	$\lvert S\rvert \leq \rho_{\min} =$	$28.004469596\ldots$
Schrijver:	$\lvert S\rvert \leq \rho_{\min} =$	$24.722717988\ldots$
Indeed:	$\lvert S\rvert \leq$	17