On permutation codes in given permutation groups

ALCOMA10, Thurnau, 2010

Gábor Péter Nagy, University of Szeged (Hungary)

Joint work with Peter Müller (Univ. of Würzburg, Germany)

April 12, 2010

Overview

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $x = [2\,3\,1\,4\,5]$, $y = [5\,3\,4\,2\,1]$.

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $x = [2\,\mathbf{3}\,1\,4\,5]$, $y = [5\,\mathbf{3}\,4\,2\,1]$. $d(x, y) = 4$.

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $$x = \begin{pmatrix} 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix}, \; y = \begin{pmatrix} 0\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,1\,0\,0\,0 \\ 1\,0\,0\,0\,0 \end{pmatrix}.$$

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $x = \begin{pmatrix} 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix}, y = \begin{pmatrix} 0\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,1\,0\,0\,0 \\ 1\,0\,0\,0\,0 \end{pmatrix}. \; d = 4$

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $x = (123)$, $y = (234)(15)$.

Permutations

Definition: Permutation

A permutation of degree n is a bijection of the set Ω of cardinality n onto itself. (Usually, $\Omega = \{1, 2, \ldots, n\}$.)
A permutation can be represented either by an n-tuple, or by a permutation matrix, or in cyclic form.

Definition: Hamming distance of permutations

Let x, y permutations of degree n. Then, $d(x, y) = |\{i \mid i^x \neq i^y\}|$.

Example: $x = (123)$, $y = (234)(15)$. $xy^{-1} = (1435)$, $d = 4$.

Permutation codes and Latin squares

Definition: Permutation codes (or arrays)

A permutation code (or array) of length n and distance d is a set T of permutations from some fixed set of n symbols such that the Hamming distance between each distinct $x, y \in T$ is at least d.

An example with $n = 3$ and $d = 2$ in matrix form: $\begin{pmatrix} 1\,1\,2\,2\,3\,3 \\ 2\,3\,1\,3\,1\,2 \\ 3\,2\,3\,1\,2\,1 \end{pmatrix}$.

Proposition (folklore)

$|T| \le d(d+1)\cdots n.$

Proof. Put $t = n - d + 1$ and look at the first t rows. Then, all columns give different arrangement of length t; $|T| \le \frac{n!}{(n-t)!}$. $\square$

Permutation codes and sharply multiply transitive sets

Definition: Sharply t-transitive sets of permutations

The set S of permutations of degree n is sharply t-transitive, if for any t-tuples $(i_1, \ldots, i_t), (j_1, \ldots, j_t)$ there is a unique element $s \in S$ such that $i_k^s = j_k$ for all k. $(1 \leq i_k, j_k \leq n.)$

- Notice that for a sharply t-transitive set S, we have $d(x, y) \geq n - t + 1$ for all $x, y \in S$.
- Thus, sharply t-transitive sets are precisely the permutation codes of maximal size with parameter $d = n - t + 1$.
- If S is a sharply t-transitive set of degree n, then it is a sharply 1-transitive set on

$$\Omega = \{(i_1, \ldots, i_t) \mid i_k \neq i_\ell \text{ if } k \neq \ell\}.$$

Sharply 1 and 2-transitive sets

- Sharply 1-transitive sets of permutations are Latin squares. $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,1\,4\,5\,3 \\ 3\,5\,1\,2\,4 \\ 4\,3\,5\,1\,2 \\ 5\,4\,2\,3\,1 \end{pmatrix}$.
- Let $\mathbb{F}$ be a field and consider the set

$$S = \{x \mapsto ax + b \mid a \in \mathbb{F}^*, b \in \mathbb{F}\}$$

  of $\mathbb{F} \to \mathbb{F}$ maps. Then, S is a sharply 2-transitive set of permutations.
- It is well known that a sharply 2-transitive set of degree n corresponds to an affine plane of order n. [Witt, 1938]
- MAIN PROBLEM: Construct 2-transitive sets of **not** prime power degree!!!

Finite 2-transitive permutation groups

Program from the 1970's (Lorimer, O'Nan, Grundhöfer, Müller)

Show for classes of 2-transitive finite groups that they don't contain sharply 2-transitive sets.

The classification of finite 2-transitive permutation groups uses the CTFSG.

1. Groups of affine type. Such groups are vector spaces + matrix groups over a finite field. The degree is prime power.
2. Almost simple groups. Groups with deep combinatorial and finite geometric structure.
3. "No structure" at all: A_n, S_n.

- Hard nuts: Mathieu and other sporadic groups, $PSp(2n, 2)$.
- Still open: A_n, S_n, M_{24}.

Methods

Existing methods, used for some specific permutation action of 2-transitive permutation groups:

- Enumeration methods by Lorimer (1973) deals with the groups of Ree type, $PU(3, q^2)$ and the Suzuki groups.
- O'Nan's contradicting subgroup method (1985) was used to exclude the groups $P\Gamma L(m, q)$ ($m \geq 3$ or $q \geq 5$), and the Higman-Sims sporadic simple group.
- The character theoretical method by Grundhöfer and P. Müller (2008) deals with $PSp(2d, 2)$ and the Conway group Co_3.
- Computational methods using Östergård's CLIQUER and Soicher's GRAPE programs.

The main lemma

Main Lemma

Let G be a permutation group on a finite set Ω. Assume that there are subsets B, C of Ω and a prime p such that $p \nmid |B||C|$ and $p \mid |B \cap C^g|$ for all $g \in G$. Then G contains no sharply transitive set of permutations.

Proof. Assume $S \subseteq G$ is a sharply transitive set. By double counting the set

$$\{(b, c, s) \mid b \in B, c \in C, s \in S, c^s = b\},$$

we obtain $|B||C| = \sum_{s \in S} |B \cap C^s| \equiv 0 \pmod{p}$.
Contradiction. $\square$

1st application: Sharply 1-transitive sets in M_{22}

Theorem 1

In its natural permutation representation of degree 22, the Mathieu group M_{22} does not contain a sharply transitive set of permutations.

Proof.

- Let $\Omega' = \{1, \dots, 23\}$, $\Omega = \{1, \dots, 22\}$ and $G = M_{22}$ be the stabilizer of $23 \in \Omega'$.
- Let $B \subset \Omega$ be a block of the Witt design $\mathcal{W}_{23}$, and, $C = \Omega \setminus B$.
- Then, $|B| = 7, |C| = 15$ and for all $g \in G$, $|B \cap C^g| = 0, 4$ or 6.
- The Main Lemma implies the result with $p = 2$. $\square$

2nd application: Sharply 1-transitive sets in $Sp(2n, 2^m)$

Theorem 2

Let n, m be positive integers, $n \geq 2$, $q = 2^m$. Let $G = Sp(2n, q)$ be the permutation group in its natural permutation actions on $\Omega = \mathbb{F}_q^{2n} \setminus \{0\}$. Then, G does not contain a sharply transitive set of permutations.

Proof.

- Let $\mathcal{E}$ be an elliptic quadric of $PG(2n-1, q)$ whose quadratic equation polarizes to the invariant symplectic form $\langle ., . \rangle$ of G.
- Let ℓ be a line of $PG(2n-1, q)$ which is nonsingular with respect to $\langle ., . \rangle$.
- Then for any $g \in G$, ℓ^g is nonsingular and $|\mathcal{E} \cap \ell^g| = 0$ or 2.
- Furthermore, both $|\mathcal{E}|$ and $|\ell|$ are odd for $n \geq 2$. We apply the Main Lemma with $B = \mathcal{E}$, $C = \ell$ and $p = 2$. $\square$

3rd applitation: Sharply 2-transitive sets in A_n

Theorem 3

If $n \equiv 2, 3 \pmod 4$ then the alternating group A_n does not contain a sharply 2-transitive set of permutations.

Proof.

- Put $B = \{(i,j) \mid i < j\}, \qquad C = \{(i,j) \mid i > j\}.$
- By the assumption on n, $|B| = |C| = n(n-1)/2$ is odd.
- For any permutation $g \in S_n$, we have

$$|\{(i,j) \mid i < j,\ i^g > j^g\}| \equiv \mathrm{sgn}(g) \pmod 2.$$

- This implies $|B \cap C^g| \equiv 0 \pmod 2$ for all $g \in A_n$. □

Corollary

The Mathieu group M_{23} does not contain a sharply 2-transitive set.

A combinatorial proof of O'Nan's theorem

Theorem (Lorimer, 1973)

If $k \geq 2$ and $q \geq 5$, then $G = P\Gamma L(k, q)$ does not contain a sharply 2-transitive set of permutations.

Theorem (O'Nan, 1985)

$G = P\Gamma L(k, q)$ does not contain a sharply 2-transitive set of permutations unless $k = 2$ and $q = 2, 3, 4$.

Proof. Uses character theory. $\square$ Sharp.

Theorem (Peter Müller, GN, 2009)

The automorphism group G of a nontrivial symmetric design D does not contain a sharply 2-transitive set of permutations.

Proof. Combinatorial. $\square$ Put $D = PG(k-1, q)$ for $k \geq 3$.