

Permutation groups, primitivity and derangements

Tim Burness

University of Bristol

Pure Mathematics Colloquium
University of St Andrews
March 12th 2015



Introduction

Let $G \leq \text{Sym}(\Omega)$ be a permutation group on a set Ω .

An element x in G is a **derangement** if it has no fixed points on Ω .

Let $\Delta(G)$ be the set of derangements in G .

If G is transitive and H is a point stabilizer, then

$$\Delta(G) = G \setminus \bigcup_{\alpha \in \Omega} G_{\alpha} = G \setminus \bigcup_{g \in G} g^{-1}Hg$$

In particular, $x \in G$ is a derangement iff $x^G \cap H$ is empty.

Notation. $G_{\alpha} = \{x \in G : x \cdot \alpha = \alpha\}$, $x^G = \{g^{-1}xg : g \in G\}$

Jordan's theorem

Theorem (Jordan, 1872)

Every (nontrivial) finite transitive permutation group has a derangement.

Let $G \leq \text{Sym}(\Omega)$ be such a group. By the **Orbit-Counting Lemma**

$$\frac{1}{|G|} \sum_{x \in G} |\text{fix}_\Omega(x)| = 1$$

where $\text{fix}_\Omega(x) = \{\alpha \in \Omega : x \cdot \alpha = \alpha\}$.

Since $|\text{fix}_\Omega(1)| = |\Omega| \geq 2$, we must have $|\text{fix}_\Omega(x)| = 0$ for some x in G .

J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc., 2003

Infinite groups

Jordan's theorem does **not** extend to transitive actions of **infinite** groups:

Examples

- Let $G = \text{FSym}(\Omega) = \{x \in \text{Sym}(\Omega) : x \text{ has finite support}\}$ be the **finitary symmetric group** on an infinite set Ω .
- Let $G = 1 \cup x^G$ be an infinite group with two conjugacy classes and set $\Omega = x^G$ (here $H = C_G(x)$ and $\bigcup_{g \in G} g^{-1}Hg = G$).
- Let $G = \text{GL}(V)$, where V is an n -dimensional vector space over \mathbb{C} , and let Ω be the set of complete flags of V , i.e. subspace chains

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V_n = V$$

where V_k is k -dimensional.

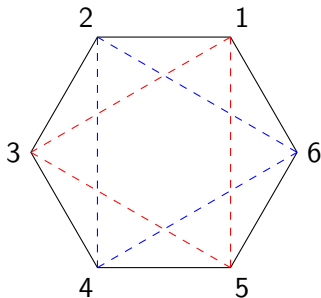
Primitivity

Let $G \leq \text{Sym}(\Omega)$ be a transitive group with point stabilizer H .

Definition. G is **imprimitive** if there exists a G -invariant partition of Ω , other than $\{\Omega\}$ and $\{\{\alpha\} : \alpha \in \Omega\}$. Otherwise, G is **primitive**.

Equivalently, G is primitive iff H is a maximal subgroup of G .

An example



$G = D_{12}$ is a transitive permutation group on $\Omega = \{1, 2, 3, 4, 5, 6\}$, and

$$\Omega = \{1, 3, 5\} \cup \{2, 4, 6\}$$

is a G -invariant partition, so G is imprimitive.

Primitivity

Let $G \leq \text{Sym}(\Omega)$ be a transitive group with point stabilizer H .

Definition. G is **imprimitive** if there exists a G -invariant partition of Ω , other than $\{\Omega\}$ and $\{\{\alpha\} : \alpha \in \Omega\}$. Otherwise, G is **primitive**.

Equivalently, G is primitive iff H is a maximal subgroup of G .

The structure of a finite primitive group is restricted, e.g. it has at most two minimal normal subgroups.

O'Nan-Scott Theorem (1979): Five families of finite primitive groups:

1. Affine
2. Almost simple
3. Diagonal type
4. Product type
5. Twisted product type

Affine and almost simple groups

Let p be a prime and let $\text{AGL}(V) = \text{GL}(V) \ltimes V$ be the group of affine transformations of $V = (\mathbb{F}_p)^d$:

$$\varphi_{x,u} : v \mapsto xv + u \quad (\text{for } x \in \text{GL}(V), u \in V)$$

Then $G \leq \text{Sym}(V)$ is **affine** if

$$V \leq G \leq \text{AGL}(V)$$

G is primitive iff $G_0 \leq \text{GL}(V)$ is irreducible

A transitive group $G \leq \text{Sym}(\Omega)$ is **almost simple** if there is a nonabelian finite simple group T such that

$$T \leq G \leq \text{Aut}(T)$$

G is primitive iff $G_\alpha < G$ is a maximal subgroup

Variations on Jordan's theorem

Let $G \leq \text{Sym}(\Omega)$ be a **finite** transitive permutation group.

Jordan's theorem: G contains a derangement

Q1. *How many derangements does G contain?*

Q2. *Does G contain derangements with special properties?*

Counting derangements

Let $G \leq \text{Sym}(\Omega)$ be a finite transitive group with $|\Omega| = n$.

Let $d(G) = |\Delta(G)|/|G|$ be the **proportion** of derangements in G .

Jordan's theorem: $d(G) > 0$

Theorem (Cameron & Cohen, 1992)

$d(G) \geq 1/n$, with equality iff G is sharply 2-transitive.

Here G is **2-transitive** if the natural action of G on

$$\Gamma = \{(\alpha, \beta) : \alpha, \beta \in \Omega, \alpha \neq \beta\}$$

is transitive. Further, G is **sharply 2-transitive** if $G_t = 1$ for $t \in \Gamma$.

e.g. If $V = \mathbb{F}_q$, then $\text{AGL}(V)$ is sharply 2-transitive

Counting derangements

Let $G \leq \text{Sym}(\Omega)$ be a finite transitive group with $|\Omega| = n$.

Let $d(G) = |\Delta(G)|/|G|$ be the **proportion** of derangements in G .

Jordan's theorem: $d(G) > 0$

Theorem (Cameron & Cohen, 1992)

$d(G) \geq 1/n$, with equality iff G is sharply 2-transitive.

Theorem (Guralnick & Wan, 1997)

One of the following holds:

- $d(G) \geq 2/n$
- G is sharply 2-transitive
- $(G, n, d(G)) = (S_4, 4, 3/8)$ or $(S_5, 5, 11/30)$

Montmort's theorem

In a highly influential book on probability,

Essay d'analyse sur les jeux de hazard

Pierre de Montmort calculated $d(S_n)$ (w.r.t. $\Omega = \{1, \dots, n\}$):

Theorem (Montmort, 1708)

$$d(S_n) = \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}, \text{ so } d(S_n) \rightarrow 1/e \text{ as } n \rightarrow \infty$$

Let E_i be the event that a randomly chosen element of S_n fixes i .

$$\begin{aligned} 1 - d(S_n) &= \mathbb{P}(E_1 \cup \dots \cup E_n) \\ &= \sum_i \mathbb{P}(E_i) - \sum_{i < j} \mathbb{P}(E_i \cap E_j) + \dots + (-1)^{n+1} \mathbb{P}(E_1 \cap \dots \cap E_n) \end{aligned}$$

Simple groups

There are similar formulae for $d(A_n)$ and $d(\mathrm{PSL}_2(q))$ (w.r.t. the natural actions). In both cases, $d(G) \geq 1/3$ for all $n, q \geq 5$.

Theorem (Fulman & Guralnick, 2014)

There exists an absolute constant $\epsilon > 0$ such that $d(G) > \epsilon$ for any simple transitive group G .

- The constant ϵ is undetermined: is $\epsilon = 2/7$ optimal?
- The conclusion does **not** extend to almost simple groups

Remark. By a theorem of Boston et al. (1993), the subset

$$\{d(G) : G \text{ is a finite primitive group}\} \subset (0, 1)$$

is dense.

Special derangements

Let G be a finite transitive permutation group.

Q. Does G contain derangements with special properties?

Theorem (Fein, Kantor & Schacher, 1981)

G contains a derangement of prime power order.

- Let G be a minimal counterexample. We may assume G is primitive.
If $1 \neq N \triangleleft G$, then N is transitive, so minimality implies that $N = G$, so G is simple. Now use CFSG...
- No “elementary” proof is known

Theorem. *Let L/K be a nontrivial finite extension of global fields. Then the relative Brauer group $B(L/K)$ is infinite.*

Elusivity

Q. *Does G contain a derangement of prime order?*

A. Not always!

e.g. Take $G = M_{11}$ and $\Omega = G/H$ with $H = \text{PSL}_2(11)$ (here $|\Omega| = 12$)

A transitive group is **elusive** if it has no derangement of prime order.

Theorem (Giudici, 2003)

Let $G \leq \text{Sym}(\Omega)$ be a finite primitive elusive group.

Then $G = M_{11} \wr L$ acting with its product action on $\Omega = \Gamma^k$, where $k \geq 1$, $L \leq S_k$ is transitive and $|\Gamma| = 12$.

Conjecture (Marušič, 1981)

If Γ is a finite vertex-transitive graph, then $\text{Aut}(\Gamma)$ is non-elusive.

Extremal permutation groups

Joint work with Hung Tong-Viet (Pretoria)

Conjugacy classes

Let $G \leq \text{Sym}(\Omega)$ be a finite transitive group with point stabilizer H .

Let $k(G)$ be the number of conjugacy classes in $\Delta(G)$.

Jordan's theorem: $k(G) \geq 1$

Theorem (B & Tong-Viet, 2014)

Let G be a finite primitive group of degree n . Then

$$k(G) = 1 \iff G \text{ is sharply 2-transitive, or} \\ (G, n) = (A_5, 6) \text{ or } (\text{Aut}(\text{PSL}_2(8)), 28)$$

- “Primitive” can be replaced by “transitive” [Guralnick, 2015]
- For almost simple groups G , we show that $k(G) \rightarrow \infty$ as $|G| \rightarrow \infty$

Proof: The reduction

Suppose $\Delta(G) = x^G$ and let N be a minimal normal subgroup of G .

1. N is regular: Here $H \cap N = 1$, $G = HN$ and $N = 1 \cup x^G$.

If N is non-abelian then $|N|$ is divisible by at least 3 primes, which is not possible. Therefore N is abelian, so $N \leq C_G(x)$,

$$|\Delta(G)| = |G : C_G(x)| \leq |G : N| = |H| = |G|/n$$

and thus $d(G) \leq 1/n$, where $n = |G : H|$.

But **Cameron-Cohen** implies that $d(G) \geq 1/n$, with equality iff G is sharply 2-transitive.

2. N is non-regular: A longer and more technical argument shows that G is almost simple.

Proof: Groups of Lie type

The basic strategy:

(a) Identify two conjugacy classes, say x_1^G and x_2^G , such that

$$\mathcal{M} = \{M < G \text{ maximal} : x_1^G \cap M \neq \emptyset \text{ or } x_2^G \cap M \neq \emptyset\}$$

is very restricted.

(b) We may assume that $H \in \mathcal{M}$. Work directly with these subgroups...

If x^G is one of the classes in (a) then

$$\mathbb{P}(G = \langle x, y \rangle : y \in G) \gg 0$$

so these classes arise naturally in problems on **random generation**.

Application: Character theory

Let $G \leq \text{Sym}(\Omega)$ be a finite transitive group with point stabilizer H .

Let $\chi = 1_H^G$ be the corresponding **permutation character**, so

$$\chi(g) = |\text{fix}_\Omega(g)| \text{ for all } g \in G$$

Jordan's theorem: $\chi(g) = 0$ for some $g \in G$

Let G be a finite group and let $\chi \in \text{Irr}(G)$ be non-linear.

Burnside, 1911: $\chi(g) = 0$ for some $g \in G$

Malle, Navarro & Olsson, 2000: $\chi(g) = 0$ for some $g \in G$ of prime power order

Application: Character theory

Let G be a finite group and let $\chi \in \text{Irr}(G)$ be non-linear.

Let $n(\chi) \geq 1$ be the number of classes on which χ vanishes.

Problem

Investigate the groups G with $n(\chi) = 1$ for some non-linear $\chi \in \text{Irr}(G)$

Suppose $\chi = \varphi_H^G$ is **induced**, where $H < G$ and $\varphi \in \text{Irr}(H)$. Then

$$n(\chi) = 1 \implies G \setminus \bigcup_{g \in G} g^{-1}Hg = x^G$$

for some $x \in G$.

If H is core-free, our theorem applies. In the general case, we can give detailed information on the normal structure of G .

Prime powers

Let $G \leq \text{Sym}(\Omega)$ be a finite transitive group.

Fein, Kantor & Schacher: G has a derangement of prime power order

Theorem (Isaacs, Keller, Lewis & Moretó, 2006)

If every derangement in G is an involution, then either

- *G is an elementary abelian 2-group; or*
- *G is a Frobenius group with kernel an elementary abelian 2-group.*

Q. *What about odd primes and prime powers?*

Let $G \leq \text{Sym}(\Omega)$ be a finite primitive group with point stabilizer H .

Property (\star): Every derangement in G is an r -element, for some fixed prime r

Theorem (B & Tong-Viet, 2014)

If (\star) holds, then G is either almost simple or affine.

The almost simple groups with property (\star)

| G | H | Conditions |
|-------------------------|-------------------------|---|
| $\mathrm{PSL}_3(q)$ | P_1, P_2 | $q^2 + q + 1 = (3, q - 1)r$ $q^2 + q + 1 = 3r^2$ |
| $\Gamma\mathrm{L}_2(q)$ | $N_G(D_{2(q+1)})$ | $r = q - 1$ Mersenne prime |
| $\Gamma\mathrm{L}_2(8)$ | $N_G(P_1), N_G(D_{14})$ | $r = 3$ |
| $\mathrm{PGL}_2(q)$ | $N_G(P_1)$ | $r = 2, q = 2^{e+1} - 1$ Mersenne |
| $\mathrm{PSL}_2(q)$ | P_1 | $q = 2r^e - 1$ |
| | $P_1, D_{2(q-1)}$ | $r = q + 1$ Fermat prime |
| | $D_{2(q+1)}$ | $r = q - 1$ Mersenne prime |
| $\mathrm{PSL}_2(8)$ | P_1, D_{14} | $r = 3$ |
| M_{11} | $\mathrm{PSL}_2(11)$ | $r = 2$ |

Let $G \leq \text{Sym}(\Omega)$ be a finite primitive group with point stabilizer H .

Property (\star) : Every derangement in G is an r -element, for some fixed prime r

Theorem (B & Tong-Viet, 2014)

- *If (\star) holds, then G is either almost simple or affine.*
- *If $G \leq \text{AGL}(V)$ is affine with $V = (\mathbb{F}_p)^d$, then (\star) holds iff $r = p$ and every two-point stabilizer in G is an r -group.*

The affine groups with this property have been extensively studied:

- **Guralnick & Wiegand, 1992:** Structure of Galois field extensions
- **Fleischmann, Lempken & Tiep, 1997:** r' -semiregular pairs

Some open problems

1. Determine the primitive groups such that every derangement has prime power order.
2. Determine the **strongly non-elusive** groups: every derangement has prime order.
3. Determine an explicit constant in the Fulman-Guralnick Theorem. Is $2/7$ optimal?
4. Prove Marušič's conjecture on vertex-transitive graphs!
5. Study the proportion of conjugacy classes containing derangements. For almost simple groups, is it bounded away from zero?
6. **J.G. Thompson:** G primitive $\implies \Delta(G)$ is a transitive subset of G ?