Transitive groups, derangements and related problems

Tim Burness

University of Bristol

Algebraic Combinatorics and Group Actions
Herstmonceux Castle
July 11th 2016

Introduction

Let G be a group acting on a set Ω.

An element of 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.

Some natural questions

1. Is $\Delta(G)$ non-empty?
2. How large is $\Delta(G)$ (e.g. relative to the order of G, for G finite)?
3. What sort of elements are contained in $\Delta(G)$?

   Can we find special elements (e.g. derangements of a given order)?
4. How many conjugacy classes are contained in $\Delta(G)$?

etc. etc.

Existence

Theorem (Jordan, 1872)

If G is finite, transitive and non-trivial, then $\Delta(G)$ is non-empty.

- $|\mathrm{fix}_\Omega(1)| \geqslant 2, \ \sum_{x \in G} |\mathrm{fix}_\Omega(x)| = |G| \implies |\mathrm{fix}_\Omega(x)| = 0$ for some $x \in G$
- **J.-P. Serre:** *On a theorem of Jordan*, Bull. AMS, 2003

Jordan's theorem does **not** extend to **infinite** transitive groups, e.g.

- $G = \{x \in \mathrm{Sym}(\Omega) : x \text{ has finite support}\}$, Ω any infinite set
- $G = \mathrm{GL}_n(\mathbb{C})$, $B = \{\text{upper-triangular matrices in } G\}$, $\Omega = G/B$

1. Counting derangements

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group with $|\Omega| = n \geqslant 2$.

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

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

Theorem (Cameron & Cohen, 1992)

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

Let r be the rank of G. Then

$$\begin{aligned}(r-1)|G| &= \sum_{x \in G} (|\mathrm{fix}_\Omega(x)| - 1)(|\mathrm{fix}_\Omega(x)| - n) \\ &\leqslant \sum_{x \in \Delta(G)} (|\mathrm{fix}_\Omega(x)| - 1)(|\mathrm{fix}_\Omega(x)| - n) = n|\Delta(G)|\end{aligned}$$

and thus $d(G) \geqslant (r-1)/n$.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group with $|\Omega| = n \geqslant 2$.

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

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

Theorem (Cameron & Cohen, 1992)

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

Theorem (Guralnick & Wan, 1997)

One of the following holds:

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

Symmetric groups

Fix $1 \leqslant k \leqslant n/2$ and set $d(n,k) = d(S_n)$ with respect to the action of S_n on k-element subsets of $\{1, \dots, n\}$.

- **Montmort, 1708:** $d(n,1) = \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$
- **Dixon, 1992:** $d(n,k) \geqslant \frac{1}{3}$
- **Łuczak & Pyber, 1993:**

$$d(n,k) > 1 - Ck^{-0.01} \text{ for some constant } C > 0$$

- **Eberhard, Ford & Green, 2015:**

$$1 - Ak^{-\delta}(1 + \log k)^{-3/2} < d(n,k) < 1 - Bk^{-\delta}(1 + \log k)^{-3/2}$$

for some constants $A, B > 0$ and $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086$.

Eberhard, Ford & Green, 2015:

$$1 - Ak^{-\delta}(1+\log k)^{-3/2} < d(n,k) < 1 - Bk^{-\delta}(1+\log k)^{-3/2}$$

for some constants $A, B > 0$ and $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086$.

This is closely related to the following theorem on **integer factorisation**:

Ford, 2008: Let $f(n,k)$ be the probability that a random integer in the interval (e^n, e^{n+1}) does not have a divisor in (e^k, e^{k+1}). Then

$$1 - Ak^{-\delta}(1+\log k)^{-3/2} < f(n,k) < 1 - Bk^{-\delta}(1+\log k)^{-3/2}$$

for some constants $A, B > 0$.

Some further asymptotics

Theorem (Łuczak & Pyber, 1993)

Let $T(n)$ be the proportion of elements in S_n contained in a transitive subgroup (other than S_n or A_n). Then $\lim_{n\to\infty} T(n) = 0$.

Corollary

Let (G_i) be a sequence of transitive permutation groups, where $G_i = S_{n_i}$ has point stabilizer H_i. Assume each H_i is transitive and $n_i \to \infty$ with i.

Then

$$1 - d(G_i) = |\bigcup_{g\in G_i} g^{-1}H_i g|/|G_i| \leqslant T(n_i)$$

and thus $\lim_{i\to\infty} d(G_i) = 1$.

Simple groups

Similar asymptotics hold for alternating groups G, which show that $d(G)$ is bounded away from zero.

Theorem (Fulman & Guralnick, 2015)

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

- This was a conjecture of Boston and Shalev (early 1990s)
- The proof is 100+ pages long (in a series of 4 papers)
- The result does **not** extend to almost simple groups, e.g.

$$G = \mathrm{PGL}_2(p^r){:}\langle\phi\rangle,\ \Omega = \phi^G \implies d(G) \leqslant \frac{1}{r}$$

for any primes p, r with $\gcd(p(p^2-1), r) = 1$.

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

- **FG:** $\epsilon \geqslant .016$ up to finitely many exceptions
- If $G = {}^2F_4(2)'$ and $G_\alpha = 2^2.[2^8].S_3$ then $\epsilon = 89/325 \approx .273$

Conjecture. Let (G_n) be a sequence of finite simple transitive groups s.t. $|G_n| \to \infty$ as $n \to \infty$. Then $\liminf_{n\to\infty} d(G_n) \geqslant \alpha$, where

$$\alpha = \prod_{k=1}^{\infty}(1 - 2^{-k}) \approx .288$$

- This is work in progress... It holds for alternating groups and simple groups of Lie type of bounded rank.

- **Neumann & Praeger, 1998:** $\lim_{n\to\infty} d(G_n) = \alpha$ for $G_n = \mathrm{SL}_n(2)$ on 1-dimensional subspaces of $(\mathbb{F}_2)^n$.

2. Orders of derangements

Theorem (Fein, Kantor & Schacher, 1981)

Every finite transitive group contains a derangement of prime power order.

- Let G be a minimal counterexample. We can assume G is primitive.

  If $1 \neq N \trianglelefteqslant G$ then N is transitive, so minimality implies that $N = G$, so G is simple. Now use CFSG...

- No "elementary" proof is known.

- It is equivalent to the following theorem in number theory:

Theorem. *The relative Brauer group of any non-trivial finite extension of global fields is infinite.*

Elusive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be transitive with $|\Omega| = n \geqslant 2$. We say G is **elusive** if it has no derangement of prime order.

e.g. Take $G = \mathrm{M}_{11}$ and $\Omega = G/H$ with $H = \mathrm{PSL}_2(11)$

Giudici, 2003: G is primitive and elusive iff $G = \mathrm{M}_{11} \wr L$ acting with its product action on $\Omega = \Gamma^k$, where $k \geqslant 1$, $L \leqslant S_k$ is transitive and $|\Gamma| = 12$.

Let r be a prime divisor of n. Then G is ***r*-elusive** if it does not contain a derangement of order r.

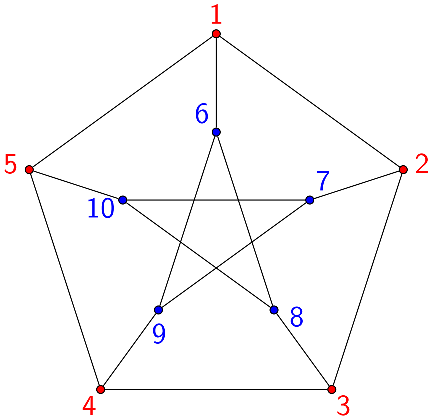
- **B, Giudici & Wilson, 2011:** We determined all the r-elusive almost simple primitive groups with an **alternating** or **sporadic** socle.
- **B & Giudici, 2015:** An in-depth analysis of r-elusivity for primitive almost simple **classical** groups.

Graphs and elusivity

Conjecture (Marušič, 1981)

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

Example: The Petersen graph



$(1,2,3,4,5)(6,7,8,9,10) \in \mathrm{Aut}(\Gamma)$ is a derangement of order 5

Graphs and elusivity

Conjecture (Marušič, 1981)

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

- The conjecture has been verified in several special cases

  e.g. Cayley graphs, distance-transitive graphs, 2-arc transitive graphs, graphs of valency 3 or 4...

- **Giudici, 2003:** If Γ is a counterexample, then every minimal normal subgroup of $\mathrm{Aut}(\Gamma)$ is intransitive.

There is a natural extension to 2-**closed** permutation groups:

Conjecture (Klin, 1997)

Every finite transitive 2-closed permutation group is non-elusive.

3. Conjugacy classes

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

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

Jordan's theorem: $\ell(G) \geqslant 1$

Theorem (B & Tong-Viet, 2015)

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

$$\ell(G) = 1 \iff G \text{ is sharply 2-transitive, or } (G, n) = (A_5, 6) \text{ or } (\mathrm{PSL}_2(8).3, 28)$$

- **Guralnick, 2016:** "Primitive" can be replaced by "transitive"
- For almost simple G, we determine the cases with $\ell(G) = 2$, and we show that $\ell(G) \to \infty$ as $|G| \to \infty$

Proof: The reduction

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

Set $n = |\Omega| = |G : H|$.

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

- N non-abelian $\implies \pi(N) \geqslant 3$, a contradiction
- N abelian $\implies N \leqslant C_G(x)$, so $d(G) = 1/|C_G(x)| \leqslant 1/|N| = 1/n$

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

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

Proof: Groups of Lie type

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 typically

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

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

Application: Character theory

Let G be a finite group, let $\chi \in \mathrm{Irr}(G)$ and let $n(\chi)$ be the number of conjugacy classes on which χ vanishes.

Burnside, 1903: If χ is non-linear then $n(\chi) \geqslant 1$

Problem

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

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

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

for some $x \in G$.

We obtain structural information on G in terms of $N = \mathrm{Core}_G(H)$, G/N and H/N.

4. Prime powers revisited

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

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

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

Every derangement in G has order 2 if and only if

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

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

Let $G \leqslant \mathrm{Sym}(\Omega)$ 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, 2016)

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

The almost simple groups with property ($\star$)

G	H	Conditions
$\mathrm{PSL}_3(q)$	$\mathrm{P}_1, \mathrm{P}_2$	$q^2+q+1=(3,q-1)r$
		$q^2+q+1=3r^2$
$\mathrm{P\Gamma L}_2(q)$	$\mathrm{N}_G(\mathrm{D}_{2(q+1)})$	$r=q-1$ Mersenne prime
$\mathrm{PGL}_2(q)$	$\mathrm{N}_G(\mathrm{P}_1)$	$r=2$, q Mersenne prime
$\mathrm{PSL}_2(q)$	P_1	$q=2r^e-1$
	$\mathrm{P}_1, \mathrm{D}_{2(q-1)}$	$r=q+1$ Fermat prime
	$\mathrm{D}_{2(q+1)}$	$r=q-1$ Mersenne prime
$\mathrm{P\Gamma L}_2(8)$	$\mathrm{N}_G(\mathrm{P}_1)$, $\mathrm{N}_G(\mathrm{D}_{14})$	$r=3$
$\mathrm{PSL}_2(8)$	$\mathrm{P}_1, \mathrm{D}_{14}$	$r=3$
M_{11}	$\mathrm{PSL}_2(11)$	$r=2$

Let $G \leqslant \mathrm{Sym}(\Omega)$ 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, 2016)

- *If $(\star)$ holds, then G is either almost simple or affine.*
- *If $G \leqslant \mathrm{AGL}(V)$ 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