Permutation groups, derangements and prime order elements

Tim Burness
University of Southampton

Isaac Newton Institute, Cambridge
April 21, 2009

Overview

1. **Introduction**

2. **Counting derangements:**
   - Jordan's Theorem
   - Cameron-Cohen Theorem
   - Asymptotics and the Boston-Shalev Conjecture

3. **The order of derangements:**
   - Fein-Kantor-Schacher Theorem
   - Elusive permutation groups
   - The Polycirculant Conjecture

4. **Derangements of prime order in simple groups**
   Joint work with Michael Giudici (UWA, Perth)

Introduction

Let G be a permutation group on a set Ω.

An element of G is a **derangement** (or **fixed-point-free**) if it has no fixed points on Ω.

Introduction

Let G be a permutation group on a set Ω.

An element of G is a **derangement** (or **fixed-point-free**) if it has no fixed points on Ω.

Equivalently, if G acts transitively on Ω with point stabilizer H, $x \in G$ is a derangement if and only if $x^G \cap H$ is empty.

Introduction

Let G be a permutation group on a set Ω.

An element of G is a **derangement** (or **fixed-point-free**) if it has no fixed points on Ω.

Equivalently, if G acts transitively on Ω with point stabilizer H, $x \in G$ is a derangement if and only if $x^G \cap H$ is empty.

Some questions

- Does G contain a derangement?
- How many are there?
- Are there restrictions on the possible orders?

A theorem of Jordan

Theorem (Jordan, 1872)

Let G be a transitive permutation group on a finite set Ω with $|\Omega| \geq 2$. Then G contains a derangement.

A theorem of Jordan

Theorem (Jordan, 1872)

Let G be a transitive permutation group on a finite set Ω with $|\Omega| \geq 2$. Then G contains a derangement.

By the Orbit-Counting Lemma we have

$$1 = \frac{1}{|G|} \sum_{x \in G} |\mathrm{fix}(x)|,$$

where $\mathrm{fix}(x) = \{\alpha \in \Omega \mid \alpha x = \alpha\}$.

A theorem of Jordan

Theorem (Jordan, 1872)

Let G be a transitive permutation group on a finite set Ω with $|\Omega| \geq 2$. Then G contains a derangement.

By the Orbit-Counting Lemma we have

$$1 = \frac{1}{|G|} \sum_{x \in G} |\mathrm{fix}(x)|,$$

where $\mathrm{fix}(x) = \{\alpha \in \Omega \mid \alpha x = \alpha\}$.

Since $|\mathrm{fix}(1)| = |\Omega| \geq 2$, there exists $x \in G$ with $|\mathrm{fix}(x)| = 0$.

Infinite permutation groups

Jordan's Theorem does not extend to infinite groups:

Infinite permutation groups

Jordan's Theorem does not extend to infinite groups:

Examples

(i) Every element of the finitary symmetric group G of an infinite set has finite support, so G has no derangements.

Infinite permutation groups

Jordan's Theorem does not extend to infinite groups:

Examples

(i) Every element of the finitary symmetric group G of an infinite set has finite support, so G has no derangements.

(ii) Let G be a transitive permutation group with point stabilizer H. If G has exactly two conjugacy classes and H is non-trivial then every element of G has fixed points.

Infinite permutation groups

Jordan's Theorem does not extend to infinite groups:

Examples

(i) Every element of the finitary symmetric group G of an infinite set has finite support, so G has no derangements.

(ii) Let G be a transitive permutation group with point stabilizer H. If G has exactly two conjugacy classes and H is non-trivial then every element of G has fixed points.

(iii) Let G be a connected algebraic group over an algebraically closed field and let $\Omega = G/B$ be the flag variety of G.

Every element of G belongs to a Borel subgroup and any two Borels are conjugate, so G has no derangements.

Derangements in S_n

The study of derangements can be traced back to the early days of probability theory in the late 17th century.

Derangements in S_n

The study of derangements can be traced back to the early days of probability theory in the late 17th century.

Let $\mathbb{P}(n)$ be the probability of winning the following game of chance:

Take a shuffled deck of n cards, numbered $1, 2, \ldots, n$. Draw one card at a time, without replacement, counting out loud as each card is drawn: "1, 2, 3, ...".

The player 'wins' if he or she can go through the entire deck, never drawing a card bearing the number just called.

Derangements in S_n

The shuffled deck corresponds to a permutation $x \in S_n$, and the player wins if and only if x is a derangement.

Therefore $\mathbb{P}(n)$ is simply the proportion of derangements in S_n.

Derangements in S_n

The shuffled deck corresponds to a permutation $x \in S_n$, and the player wins if and only if x is a derangement.

Therefore $\mathbb{P}(n)$ is simply the proportion of derangements in S_n.

Using the inclusion-exclusion principle, Pierre de Montmort proved the following theorem:

Theorem (Montmort, 1708)

$$\mathbb{P}(n) = \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}.$$

In particular, $\mathbb{P}(n) \to e^{-1}$ *as* $n \to \infty$.

Counting derangements

Let G be a transitive permutation group of degree $n \geq 2$. Let $\delta(G)$ be the **proportion** of derangements in G.

By Jordan's Theorem we have $\delta(G) > 0$.

Counting derangements

Let G be a transitive permutation group of degree $n \geq 2$. Let $\delta(G)$ be the **proportion** of derangements in G.

By Jordan's Theorem we have $\delta(G) > 0$.

Examples

(i) $\delta(S_n) = [n!/e]/n! \approx e^{-1}$ by Montmort's Theorem.

Counting derangements

Let G be a transitive permutation group of degree $n \geq 2$. Let $\delta(G)$ be the **proportion** of derangements in G.

By Jordan's Theorem we have $\delta(G) > 0$.

Examples

(i) $\delta(S_n) = [n!/e]/n! \approx e^{-1}$ by Montmort's Theorem.

(ii) Let q be an odd prime power. Then $\delta(\mathrm{PSL}(2,q)) = \frac{q-1}{2(q+1)}$ with respect to $\Omega = \mathbb{F}_q \cup \{\infty\}$.

Counting derangements

Let G be a transitive permutation group of degree $n \geq 2$. Let $\delta(G)$ be the **proportion** of derangements in G.

By Jordan's Theorem we have $\delta(G) > 0$.

Examples

(i) $\delta(S_n) = [n!/e]/n! \approx e^{-1}$ by Montmort's Theorem.

(ii) Let q be an odd prime power. Then $\delta(\mathrm{PSL}(2,q)) = \frac{q-1}{2(q+1)}$ with respect to $\Omega = \mathbb{F}_q \cup \{\infty\}$.

Theorem (Cameron-Cohen, 1992)

$\delta(G) \geq 1/n$, with equality if and only if G is a Frobenius group of order $n(n-1)$ with n a prime power.

More on $\delta(G)$

There are various extensions of the Cameron-Cohen Theorem.

For example, using CFSG we get

More on $\delta(G)$

There are various extensions of the Cameron-Cohen Theorem.

For example, using CFSG we get

Theorem (Guralnick-Wan, 1997)

One of the following holds:

(i) $\delta(G) \geq 2/n$;

(ii) G *is a Frobenius group of order* $n(n-1)$ *with* n *a prime power;*

(iii) $(G, n, \delta(G)) = (S_4, 4, 3/8)$ *or* $(S_5, 5, 11/30)$.

More on $\delta(G)$

There are various extensions of the Cameron-Cohen Theorem.

For example, using CFSG we get

Theorem (Guralnick-Wan, 1997)

One of the following holds:

(i) $\delta(G) \geq 2/n$;

(ii) G *is a Frobenius group of order* $n(n-1)$ *with* n *a prime power;*

(iii) $(G, n, \delta(G)) = (S_4, 4, 3/8)$ *or* $(S_5, 5, 11/30)$.

Guralnick and Wan use this to investigate the number of distinct values taken by a polynomial $f(X) \in \mathbb{F}_q[X]$ as X runs over $\mathbb{F}_q$.

Asymptotics

We can consider the asymptotic behaviour of $\delta(G)$ for various families of permutation groups.

Asymptotics

We can consider the asymptotic behaviour of $\delta(G)$ for various families of permutation groups.

Examples

(i) Recall that $\delta(S_n) \to e^{-1}$ as $n \to \infty$. In particular, we have $\delta(S_n) \geq 1/3$ for all n.

(ii) Similarly, $\delta(A_n) \geq 1/3$ for all $n \geq 5$.

Asymptotics

We can consider the asymptotic behaviour of $\delta(G)$ for various families of permutation groups.

Examples

(i) Recall that $\delta(S_n) \to e^{-1}$ as $n \to \infty$. In particular, we have $\delta(S_n) \geq 1/3$ for all n.

(ii) Similarly, $\delta(A_n) \geq 1/3$ for all $n \geq 5$.

(iii) Let q be an odd prime power. Then

$$\delta(\mathrm{PSL}(2,q)) = \frac{q-1}{2(q+1)} \to \frac{1}{2} \text{ as } q \to \infty.$$

In particular, $\delta(\mathrm{PSL}(2,q)) \geq 1/3$ for all $q \geq 5$.

The Boston-Shalev Conjecture

Theorem (Fulman-Guralnick, 2003)

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

The Boston-Shalev Conjecture

Theorem (Fulman-Guralnick, 2003)

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

- This was originally a conjecture of Boston and Shalev. Interestingly, it does not extend to almost simple groups.
- Excluding some known cases, $\delta(G) \to 1$ as $|G| \to \infty$.
- The proof uses CFSG and detailed information on maximal subgroups. It provides an explicit constant $\epsilon = 1/25$, with a finite list of possible exceptions.

Derangements of prescribed order

Jordan's Theorem guarantees the existence of a derangement, but can we find derangements of prescribed order?

Derangements of prescribed order

Jordan's Theorem guarantees the existence of a derangement, but can we find derangements of prescribed order?

For **prime powers** we have

Theorem (Fein-Kantor-Schacher, 1981)

Let G be a transitive permutation group of degree $n \geq 2$. Then G has a derangement of prime power order.

Derangements of prescribed order

Jordan's Theorem guarantees the existence of a derangement, but can we find derangements of prescribed order?

For **prime powers** we have

Theorem (Fein-Kantor-Schacher, 1981)

Let G be a transitive permutation group of degree $n \geq 2$. Then G has a derangement of prime power order.

The problem is first reduced to the simple primitive case, then the various simple groups are analysed in detail, using CFSG.

No CFSG-free proof is known.

Derangements of prime order

Let G be a transitive permutation group of degree n with stabilizer H. Then G is **elusive** if it has no derangements of prime order.

Derangements of prime order

Let G be a transitive permutation group of degree n with stabilizer H. Then G is **elusive** if it has no derangements of prime order.

In particular, G is elusive if

- Every prime dividing n also divides $|H|$; and
- G has a unique class of elements of order p, for each prime p dividing n.

Derangements of prime order

Let G be a transitive permutation group of degree n with stabilizer H. Then G is **elusive** if it has no derangements of prime order.

In particular, G is elusive if

- Every prime dividing n also divides $|H|$; and
- G has a unique class of elements of order p, for each prime p dividing n.

Examples

(i) $\mathrm{M}_{11} < S_{12}$ is elusive since $n = 2^2.3$, $|H| = 2^2.3.5.11$ and M_{11} has a unique class of elements of order 2 or 3.

Derangements of prime order

Let G be a transitive permutation group of degree n with stabilizer H. Then G is **elusive** if it has no derangements of prime order.

In particular, G is elusive if

- Every prime dividing n also divides $|H|$; and
- G has a unique class of elements of order p, for each prime p dividing n.

Examples

(i) $\mathrm{M}_{11} < S_{12}$ is elusive since $n = 2^2.3$, $|H| = 2^2.3.5.11$ and M_{11} has a unique class of elements of order 2 or 3.

(ii) Let p be a Mersenne prime, let $G = \mathrm{AGL}(1, p^2)$ and let Ω be the set of left cosets of $\mathrm{AGL}(1, p)$ in G.

Then G is elusive on Ω since $|\Omega| = p(p+1)$ and all elements of order 2 or p in G are conjugate.

Elusive groups

Every non-trivial normal subgroup of a primitive permutation group is transitive.

The next result determines the elusive examples in a much wider class of permutation groups.

Elusive groups

Every non-trivial normal subgroup of a primitive permutation group is transitive.

The next result determines the elusive examples in a much wider class of permutation groups.

Theorem (Giudici, 2003)

Let G be an elusive permutation group with a transitive minimal normal subgroup. Then $G = \mathrm{M}_{11} \wr K$ acting on 12^t points, with K a transitive subgroup of S_t.

In particular, G is primitive.

Elusive groups

Every non-trivial normal subgroup of a primitive permutation group is transitive.

The next result determines the elusive examples in a much wider class of permutation groups.

Theorem (Giudici, 2003)

Let G be an elusive permutation group with a transitive minimal normal subgroup. Then $G = \mathrm{M}_{11} \wr K$ acting on 12^t points, with K a transitive subgroup of S_t.

In particular, G is primitive.

Various other infinite families of elusive groups have since been constructed.

The Polycirculant Conjecture

Let G be a permutation group on a finite set Ω. The 2-**closure** of G, denoted by $G^{(2)}$, is the largest subgroup of $\mathrm{Sym}(\Omega)$ which preserves the orbits of G on $\Omega \times \Omega$.

The Polycirculant Conjecture

Let G be a permutation group on a finite set Ω. The 2-**closure** of G, denoted by $G^{(2)}$, is the largest subgroup of $\mathrm{Sym}(\Omega)$ which preserves the orbits of G on $\Omega \times \Omega$.

For example, if G is 2-transitive then

$$\{(\alpha, \alpha) \mid \alpha \in \Omega\}, \quad \{(\alpha, \beta) \mid \alpha, \beta \in \Omega, \alpha \neq \beta\}$$

are the orbits of G on $\Omega \times \Omega$, so $G^{(2)} = \mathrm{Sym}(\Omega)$.

The Polycirculant Conjecture

Let G be a permutation group on a finite set Ω. The 2-**closure** of G, denoted by $G^{(2)}$, is the largest subgroup of $\mathrm{Sym}(\Omega)$ which preserves the orbits of G on $\Omega \times \Omega$.

For example, if G is 2-transitive then

$$\{(\alpha, \alpha) \mid \alpha \in \Omega\}, \quad \{(\alpha, \beta) \mid \alpha, \beta \in \Omega, \alpha \neq \beta\}$$

are the orbits of G on $\Omega \times \Omega$, so $G^{(2)} = \mathrm{Sym}(\Omega)$.

We say that G is 2-**closed** if $G = G^{(2)}$.

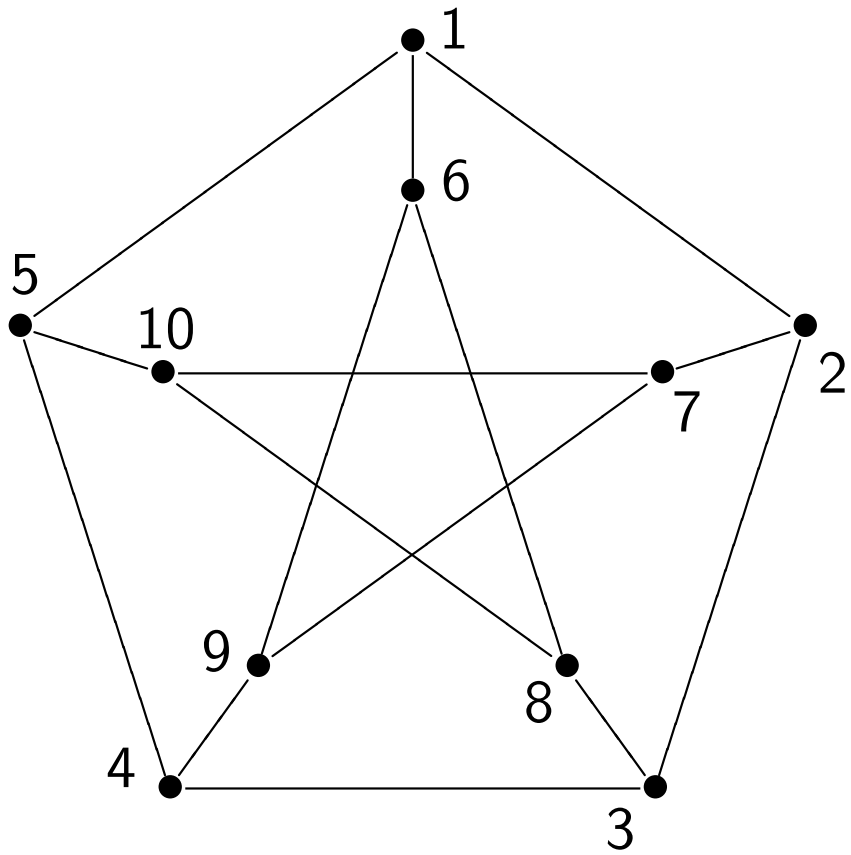
For example, the automorphism group of a finite graph is 2-closed (acting on the set of vertices).

The Polycirculant Conjecture

A graph Γ is a **polycirculant** if there exists $1 \neq x \in \mathrm{Aut}(\Gamma)$ which permutes the vertices of Γ in cycles of equal length.

Example: The Petersen graph

Let Γ be the **Petersen graph**:



Then Γ is a polycirculant since

$$(1,2,3,4,5)(6,7,8,9,10) \in \mathrm{Aut}(\Gamma).$$

The Polycirculant Conjecture

A graph Γ is a **polycirculant** if there exists $1 \neq x \in \mathrm{Aut}(\Gamma)$ which permutes $V(\Gamma)$ in cycles of equal length.

Marušič (1981): Is every vertex-transitive graph a polycirculant?

Of course, if $\mathrm{Aut}(\Gamma)$ contains a derangement of prime order then Γ is a polycirculant.

The Polycirculant Conjecture

A graph Γ is a **polycirculant** if there exists $1 \neq x \in \mathrm{Aut}(\Gamma)$ which permutes $V(\Gamma)$ in cycles of equal length.

Marušič (1981): Is every vertex-transitive graph a polycirculant?

Of course, if $\mathrm{Aut}(\Gamma)$ contains a derangement of prime order then Γ is a polycirculant.

Conjecture (Klin, 1997)

Let G be a transitive 2-closed permutation group on a finite set Ω. Then G has a derangement of prime order.

The conjecture is still open, although various special cases have been confirmed.

The Polycirculant Conjecture

If $G = \mathrm{M}_{11} \wr K$, as in Giudici's theorem, then $G^{(2)} \neq G$.

Therefore all minimal normal subgroups of a counterexample to the conjecture must be intransitive.

The Polycirculant Conjecture

If $G = \mathrm{M}_{11} \wr K$, as in Giudici's theorem, then $G^{(2)} \neq G$.

Therefore all minimal normal subgroups of a counterexample to the conjecture must be intransitive.

A 2-**arc** in a graph Γ is a triple (v_0, v_1, v_2) of vertices such that $v_0 \sim v_1 \sim v_2$ and $v_0 \neq v_2$. Then Γ is 2-**arc transitive** if $\mathrm{Aut}(\Gamma)$ is transitive on the set of 2-arcs in Γ.

The Polycirculant Conjecture

If $G = \mathrm{M}_{11} \wr K$, as in Giudici's theorem, then $G^{(2)} \neq G$.

Therefore all minimal normal subgroups of a counterexample to the conjecture must be intransitive.

A 2-**arc** in a graph Γ is a triple (v_0, v_1, v_2) of vertices such that $v_0 \sim v_1 \sim v_2$ and $v_0 \neq v_2$. Then Γ is 2-**arc transitive** if $\mathrm{Aut}(\Gamma)$ is transitive on the set of 2-arcs in Γ.

Theorem (Giudici-Xu, 2007)

The automorphism group of any 2-arc transitive graph has a derangement of prime order.

The more general arc-transitive case remains open.

Almost simple primitive groups

A finite group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0.

Using the O'Nan-Scott Theorem, many general questions about finite permutation groups can be reduced to the almost simple primitive case.

Almost simple primitive groups

A finite group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0.

Using the O'Nan-Scott Theorem, many general questions about finite permutation groups can be reduced to the almost simple primitive case.

As a corollary to Giudici's earlier theorem we get:

Corollary

Let G be an elusive almost simple primitive permutation group. Then $G = \mathrm{M}_{11}$ acting on 12 points.

Almost simple primitive groups

A finite group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0.

Using the O'Nan-Scott Theorem, many general questions about finite permutation groups can be reduced to the almost simple primitive case.

As a corollary to Giudici's earlier theorem we get:

Corollary

Let G be an elusive almost simple primitive permutation group. Then $G = \mathrm{M}_{11}$ acting on 12 points.

This is strictly an existence result; if $G \neq \mathrm{M}_{11}$ on 12 points then there exists a derangement of prime order.

Almost simple primitive groups

The problem

Let G be a non-elusive almost simple primitive permutation group. Determine the primes r such that G has a derangement of order r.

This is work in progress, joint with Michael Giudici.

Almost simple primitive groups

The problem

Let G be a non-elusive almost simple primitive permutation group. Determine the primes r such that G has a derangement of order r.

This is work in progress, joint with Michael Giudici.

- Does G contain a derangement of order 2?
- Is there a derangement of odd prime order?
- Is there a derangement of order the largest prime dividing the degree?
- If G is a group of Lie type in characteristic p then does G contain a derangement of order p?

Preliminaries

Let G be a non-elusive almost simple primitive permutation group of degree n with point stabilizer H and socle G_0.

Let r be a prime divisor of $n = |G : H|$. To determine if G has a derangement of order r we may as well assume r also divides $|H|$.

Preliminaries

Let G be a non-elusive almost simple primitive permutation group of degree n with point stabilizer H and socle G_0.

Let r be a prime divisor of $n = |G : H|$. To determine if G has a derangement of order r we may as well assume r also divides $|H|$.

Since G is primitive, H is a maximal subgroup of G and so we can analyse the possibilities for H using powerful theorems of

- O'Nan-Scott (G_0 alternating);
- Aschbacher (G_0 classical);
- Liebeck-Seitz (G_0 exceptional);
- Wilson et al. (G_0 sporadic).

Preliminaries

Let G be a non-elusive almost simple primitive permutation group of degree n with point stabilizer H and socle G_0.

Let r be a prime divisor of $n = |G : H|$. To determine if G has a derangement of order r we may as well assume r also divides $|H|$.

Since G is primitive, H is a maximal subgroup of G and so we can analyse the possibilities for H using powerful theorems of

- O'Nan-Scott (G_0 alternating);
- Aschbacher (G_0 classical);
- Liebeck-Seitz (G_0 exceptional);
- Wilson et al. (G_0 sporadic).

This is part of a wider study of maximal subgroups and conjugacy classes in almost simple groups.

Alternating groups

Theorem (O'Nan-Scott, 1980)

Let G be a primitive permutation group with socle A_n and point stabilizer H. Then one of the following holds:

(i) *H is a 'known' subgroup of G, e.g. $(S_k \times S_{n-k}) \cap G$ or $(S_k \wr S_t) \cap G$ (with $n = kt$);*

(ii) *H is almost simple and primitive on $\{1, \ldots, n\}$.*

Alternating groups

Theorem (O'Nan-Scott, 1980)

Let G be a primitive permutation group with socle A_n and point stabilizer H. Then one of the following holds:

(i) *H is a 'known' subgroup of G, e.g. $(S_k \times S_{n-k}) \cap G$ or $(S_k \wr S_t) \cap G$ (with $n = kt$);*

(ii) *H is almost simple and primitive on $\{1, \ldots, n\}$.*

Proposition (B-Giudici, 2008)

Let G be a primitive permutation group on Ω with socle A_n. Let r be a prime divisor of $|\Omega|$. Then one of the following holds:

(i) G contains a derangement of order r;

(ii) (G, Ω, r) belongs to a short list of known exceptions.

Alternating groups

Proposition

Suppose $G = A_n$ or S_n, $H = G_\alpha$ is primitive on $\{1, \ldots, n\}$ and r is a prime divisor of $|\Omega|$. Then either

(i) G contains a derangement of order r; or

(ii) $r = 2$ and $(G, H) = (A_5, D_5)$ or $(A_6, \mathrm{PSL}(2, 5))$.

Proposition

Suppose $G = A_n$ or S_n, $H = G_\alpha$ is primitive on $\{1, \ldots, n\}$ and r is a prime divisor of $|\Omega|$. Then either

(i) G contains a derangement of order r; or

(ii) $r = 2$ and $(G, H) = (A_5, D_5)$ or $(A_6, \mathrm{PSL}(2, 5))$.

The case $r \neq 2$:

Let $x \in G$ be an r-cycle. If $r < n - 2$ then a theorem of Jordan implies that H does not contain a r-cycle, so x is a derangement.

If $r \geq n - 2$ then r^2 does not divide $|G|$, so r does not divide $|H|$ and thus x is a derangement.

Sporadic groups

Proposition (B-Giudici, 2008)

Let $G \neq \mathbb{M}$ be an almost simple sporadic primitive permutation group on Ω and let r be a prime divisor of $|\Omega|$. Then either

(i) G contains a derangement of order r;

(ii) (G, Ω, r) belongs to a list of known exceptions.

Sporadic groups

Proposition (B-Giudici, 2008)

Let $G \neq \mathbb{M}$ be an almost simple sporadic primitive permutation group on Ω and let r be a prime divisor of $|\Omega|$. Then either

(i) G contains a derangement of order r;

(ii) (G, Ω, r) belongs to a list of known exceptions.

- The proof uses a combination of computational and character-theoretic methods.

Sporadic groups

Proposition (B-Giudici, 2008)

Let $G \neq \mathbb{M}$ be an almost simple sporadic primitive permutation group on Ω and let r be a prime divisor of $|\Omega|$. Then either

(i) G contains a derangement of order r;

(ii) (G, Ω, r) belongs to a list of known exceptions.

- The proof uses a combination of computational and character-theoretic methods.
- Work on the Monster $\mathbb{M}$ is in progress...

  This group is difficult to study computationally since its smallest faithful permutation representation has degree approximately 9.3×10^{13}(!)

Classical groups: Subgroup structure

Let G be an almost simple classical group over $\mathbb{F}_q$ with natural module V, e.g. $\mathrm{PGL}(n,q)$, $\mathrm{PSp}(n,q)$, $\mathrm{Aut}(\mathrm{P}\Omega^+(n,q)), \ldots$

Classical groups: Subgroup structure

Let G be an almost simple classical group over $\mathbb{F}_q$ with natural module V, e.g. $\mathrm{PGL}(n,q)$, $\mathrm{PSp}(n,q)$, $\mathrm{Aut}(\mathrm{P}\Omega^+(n,q)), \ldots$

Theorem (Aschbacher, 1984)

Let H be a maximal subgroup of G. Then either

(i) *H belongs to one of eight 'natural' subgroup collections; or*

(ii) *H is almost simple and acts irreducibly on V.*

Classical groups: Subgroup structure

Let G be an almost simple classical group over $\mathbb{F}_q$ with natural module V, e.g. $\mathrm{PGL}(n,q)$, $\mathrm{PSp}(n,q)$, $\mathrm{Aut}(\mathrm{P}\Omega^+(n,q)), \ldots$

Theorem (Aschbacher, 1984)

Let H be a maximal subgroup of G. Then either

(i) *H belongs to one of eight 'natural' subgroup collections; or*

(ii) *H is almost simple and acts irreducibly on V.*

The 'natural' subgroup collections include:

- Stabilizers of subspaces of V;
- Stabilizers of direct and tensor product decompositions of V;
- Stabilizers of non-degenerate forms on V;
- Subfield subgroups.

Classical groups: Elements of prime order

Let $G = \mathrm{GL}(n, q)$ and let $x \in G$ be an element of prime order r. Write $p = \mathrm{char}(\mathbb{F}_q)$.

Classical groups: Elements of prime order

Let $G = \mathrm{GL}(n, q)$ and let $x \in G$ be an element of prime order r. Write $p = \mathrm{char}(\mathbb{F}_q)$.

Case 1. $r = p$**:**

Here x is G-conjugate to a block-diagonal matrix of the form $[J_p^{a_p}, \ldots, J_1^{a_1}]$, where $a_k \geq 0$ and J_i denotes a standard Jordan block of size i.

Classical groups: Elements of prime order

Let $G = \mathrm{GL}(n, q)$ and let $x \in G$ be an element of prime order r. Write $p = \mathrm{char}(\mathbb{F}_q)$.

Case 1. $r = p$**:**

Here x is G-conjugate to a block-diagonal matrix of the form $[J_p^{a_p}, \ldots, J_1^{a_1}]$, where $a_k \geq 0$ and J_i denotes a standard Jordan block of size i.

Case 2. $r \neq p$**:**

Let $i \geq 1$ be minimal such that r divides $q^i - 1$.

Then x is G-conjugate to a matrix of the form $[I_\ell, A_1, \ldots, A_t]$, where $\ell \geq 0$ and each $A_k \in \mathrm{GL}(i, q)$ is irreducible of order r.

Classical groups

Let G be an almost simple primitive classical permutation group on Ω, with point stabilizer H.

If H is a 'natural' subgroup of G then we have precise results in most cases.

Classical groups

Let G be an almost simple primitive classical permutation group on Ω, with point stabilizer H.

If H is a 'natural' subgroup of G then we have precise results in most cases.

For example, suppose $G = \mathrm{PSL}(n, q) = \mathrm{PSL}(V)$ and Ω is the set of d-dimensional subspaces of V where $d < n/2$. Then

$$|\Omega| = \frac{(q^n - 1) \cdots (q^{n-d+1} - 1)}{(q^d - 1) \cdots (q - 1)}.$$

Let r be a prime divisor of $|\Omega|$ and let $i \geq 1$ be minimal such that r divides $q^i - 1$.

The case $r > 2$, $i > d$:

Let $n - d < j \leq n$ be maximal such that r divides $q^j - 1$. Set $x = [I_{n-j}, A^{j/i}] \in G$, where $A \in \mathrm{SL}(i, q)$ is irreducible of order r.

Then x is a derangement of order r.

The case $r > 2$, $i > d$:

Let $n - d < j \leq n$ be maximal such that r divides $q^j - 1$. Set $x = [I_{n-j}, A^{j/i}] \in G$, where $A \in \mathrm{SL}(i, q)$ is irreducible of order r.

Then x is a derangement of order r.

Proposition

G contains a derangement of order r iff one of the following holds:

(i) $r > 2$ and $i > d$;

(ii) $r > 2$, $i = 1$, r divides n, $\gcd(d, r) = 1$ and $(q-1)_r < d_r$;

(iii) $r > 2$, $2 \leq i \leq d$ and $k < l$, where $n \equiv k\,(i)$ and $d \equiv l\,(i)$;

(iv) $r = 2$, n is even, d odd and either $q \equiv 3\,(4)$ or $(q-1)_2 < d_2$.

Classical groups

Now suppose H is almost simple and irreducible on V. In general, the possibilities for H are not known.

Classical groups

Now suppose H is almost simple and irreducible on V. In general, the possibilities for H are not known.

For $x \in \mathrm{PGL}(n, q)$ let $\nu(x)$ denote the codimension of the largest eigenspace of $\hat{x} \in \mathrm{GL}(n, \bar{\mathbb{F}}_q)$ on the natural $\mathrm{GL}(n, \bar{\mathbb{F}}_q)$-module.

Classical groups

Now suppose H is almost simple and irreducible on V. In general, the possibilities for H are not known.

For $x \in \mathrm{PGL}(n,q)$ let $\nu(x)$ denote the codimension of the largest eigenspace of $\hat{x} \in \mathrm{GL}(n,\bar{\mathbb{F}}_q)$ on the natural $\mathrm{GL}(n,\bar{\mathbb{F}}_q)$-module.

Theorem (Guralnick-Saxl, 2003)

If $n \geq 6$ then either $\nu(x) > \max(2, \sqrt{n}/2)$ for all non-trivial $x \in H \cap \mathrm{PGL}(V)$, or (G,H) is a known exception.

Classical groups

Now suppose H is almost simple and irreducible on V. In general, the possibilities for H are not known.

For $x \in \mathrm{PGL}(n,q)$ let $\nu(x)$ denote the codimension of the largest eigenspace of $\hat{x} \in \mathrm{GL}(n,\bar{\mathbb{F}}_q)$ on the natural $\mathrm{GL}(n,\bar{\mathbb{F}}_q)$-module.

Theorem (Guralnick-Saxl, 2003)

If $n \geq 6$ then either $\nu(x) > \max(2, \sqrt{n}/2)$ for all non-trivial $x \in H \cap \mathrm{PGL}(V)$, or (G,H) is a known exception.

Consequently, ignoring the exceptions, any $x \in G \cap \mathrm{PGL}(V)$ with $\nu(x) \leq \max(2, \sqrt{n}/2)$ is a derangement.

For example, $[J_2^2, I_{n-4}] \in G$ is a derangement of order p, while $[-I_2, I_{n-2}] \in G$ is a derangement of order 2 if $p > 2$.

A question of Thompson

Question (J.G. Thompson)

Let G be a primitive permutation group on a finite set Ω. Is the set of derangements in G transitive on Ω?

A question of Thompson

Question (J.G. Thompson)

Let G be a primitive permutation group on a finite set Ω. Is the set of derangements in G transitive on Ω?

- The primitivity hypothesis is necessary.
- The answer is yes if G is 2-transitive on Ω.
- Giudici has reduced it to the almost simple case.
- No almost simple counterexample is known.