Derangements in primitive permutation groups and applications

Hung P. Tong-Viet

University of Pretoria
Hung.Tong-Viet@up.ac.za

2015 CIMPA Research School on
Algebraic Lie Theory
AIMS
July 28, 2015

(Joint work with Tim Burness)

Table of contents

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.
- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω.

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.
- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω.
- $G_\alpha = \{g \in G : \alpha^g = \alpha\}$: the point stabilizer in G of $\alpha \in \Omega$.

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.
- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω.
- $G_\alpha = \{g \in G : \alpha^g = \alpha\}$: the point stabilizer in G of $\alpha \in \Omega$.
- $x^G = \{x^g : g \in G\}$: a conjugacy class of G containing $x \in G$.

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.
- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω.
- $G_\alpha = \{g \in G : \alpha^g = \alpha\}$: the point stabilizer in G of $\alpha \in \Omega$.
- $x^G = \{x^g : g \in G\}$: a conjugacy class of G containing $x \in G$.
- If $H \leq G$ and $g \in G$, then $H^g := g^{-1}Hg$.

Introduction and Notation

- Let Ω be a finite set of size $n > 1$
- $\mathrm{Sym}(\Omega)$: the group of all permutations on Ω.
- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω.
- $G_\alpha = \{g \in G : \alpha^g = \alpha\}$: the point stabilizer in G of $\alpha \in \Omega$.
- $x^G = \{x^g : g \in G\}$: a conjugacy class of G containing $x \in G$.
- If $H \leq G$ and $g \in G$, then $H^g := g^{-1}Hg$.

Introduction and Notation, cont.

Definition

- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω.
- An element $x \in G$ is a derangement if it has no fixed point on Ω.

Introduction and Notation, cont.

Definition

- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω.
- An element $x \in G$ is a derangement if it has no fixed point on Ω.
- Let $\Delta(G)$ be the set of all derangements in G.

Introduction and Notation, cont.

Definition

- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω.
- An element $x \in G$ is a derangement if it has no fixed point on Ω.
- Let $\Delta(G)$ be the set of all derangements in G.
- We call $d(G) = \frac{|\Delta(G)|}{|G|}$ the proportion of derangements in G.

Introduction and Notation, cont.

Definition

- Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω.
- An element $x \in G$ is a derangement if it has no fixed point on Ω.
- Let $\Delta(G)$ be the set of all derangements in G.
- We call $d(G) = \dfrac{|\Delta(G)|}{|G|}$ the proportion of derangements in G.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.
- $\Delta(G) = x^G \cup y^G$.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.
- $\Delta(G) = x^G \cup y^G$.
- $|x^G| = 4! = 24$ and $|y^G| = 20$.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.
- $\Delta(G) = x^G \cup y^G$.
- $|x^G| = 4! = 24$ and $|y^G| = 20$.
- $|\Delta(G)| = 24 + 20 = 44$.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.
- $\Delta(G) = x^G \cup y^G$.
- $|x^G| = 4! = 24$ and $|y^G| = 20$.
- $|\Delta(G)| = 24 + 20 = 44$.
- $d(G) = \frac{|\Delta(G)|}{|G|} = \frac{44}{120} = \frac{11}{30}$.

Introduction and Notation, cont.

Example

Let $\Omega = \{1, 2, \cdots, 5\}$ and $G = \mathrm{Sym}(\Omega)$. Then

- $x = (1, 2, 3, 4, 5)$ and $y = (1, 2)(3, 4, 5)$ are derangements in G.
- $\Delta(G) = x^G \cup y^G$.
- $|x^G| = 4! = 24$ and $|y^G| = 20$.
- $|\Delta(G)| = 24 + 20 = 44$.
- $d(G) = \dfrac{|\Delta(G)|}{|G|} = \dfrac{44}{120} = \dfrac{11}{30}$.

Introduction and Notation, cont.

Lemma

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $|\Omega| > 1$ and let H be a point stabilizer. Then

$$\Delta(G) = G \setminus \bigcup_{\alpha \in \Omega} G_\alpha = G \setminus \bigcup_{g \in G} H^g.$$

Introduction and Notation, cont.

Lemma

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $|\Omega| > 1$ and let H be a point stabilizer. Then

$$\Delta(G) = G \setminus \bigcup_{\alpha \in \Omega} G_\alpha = G \setminus \bigcup_{g \in G} H^g.$$

In particular, $x \in \Delta(G)$ if and only if $x^G \cap H = \emptyset$.

Introduction and Notation, cont.

Lemma

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $|\Omega| > 1$ and let H be a point stabilizer. Then

$$\Delta(G) = G \setminus \bigcup_{\alpha \in \Omega} G_\alpha = G \setminus \bigcup_{g \in G} H^g.$$

In particular, $x \in \Delta(G)$ if and only if $x^G \cap H = \emptyset$.

Montmort's theorem

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with $|\Omega| = n$.
- Question: What is the probability that a random chosen permutation in the symmetric group S_n is a derangement?

Montmort's theorem

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with $|\Omega| = n$.
- Question: What is the probability that a random chosen permutation in the symmetric group S_n is a derangement?

Theorem (Montmort, 1708)

$$d(\mathrm{S}_n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Montmort's theorem

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with $|\Omega| = n$.
- Question: What is the probability that a random chosen permutation in the symmetric group S_n is a derangement?

Theorem (Montmort, 1708)

$$d(\mathrm{S}_n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

In particular, $d(\mathrm{S}_n) \longrightarrow \frac{1}{e}$ as $n \longrightarrow \infty$.

Montmort's theorem

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with $|\Omega| = n$.
- Question: What is the probability that a random chosen permutation in the symmetric group S_n is a derangement?

Theorem (Montmort, 1708)

$$d(\mathrm{S}_n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

In particular, $d(\mathrm{S}_n) \longrightarrow \frac{1}{e}$ as $n \longrightarrow \infty$.

Montmort's theorem - proof

The number of permutations of $\Omega = \{1, 2, \cdots, n\}$ fixing a given set of k points is $(n-k)!$.

By the Inclusion-Exclusion principle, we have

$$|\Delta(\mathrm{S}_n)| = \sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)!$$

Montmort's theorem - proof

The number of permutations of $\Omega = \{1, 2, \cdots, n\}$ fixing a given set of k points is $(n-k)!$.

By the Inclusion-Exclusion principle, we have

$$|\Delta(\mathrm{S}_n)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!$$

$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!(n-k)!} (n-k)!$$

Montmort's theorem - proof

The number of permutations of $\Omega = \{1, 2, \cdots, n\}$ fixing a given set of k points is $(n-k)!$.

By the Inclusion-Exclusion principle, we have

$$\begin{aligned} |\Delta(\mathrm{S}_n)| &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!(n-k)!} (n-k)! \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \end{aligned}$$

Montmort's theorem - proof

The number of permutations of $\Omega = \{1, 2, \cdots, n\}$ fixing a given set of k points is $(n-k)!$.

By the Inclusion-Exclusion principle, we have

$$
\begin{aligned}
|\Delta(\mathrm{S}_n)| &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\
&= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!(n-k)!} (n-k)! \\
&= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.
\end{aligned}
$$

Observation: The proportion $d(\mathrm{S}_n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ is the truncation of the Taylor series for e^x at $x = -1$.

Montmort's theorem - proof

The number of permutations of $\Omega = \{1, 2, \cdots, n\}$ fixing a given set of k points is $(n-k)!$.

By the Inclusion-Exclusion principle, we have

$$
\begin{aligned}
|\Delta(\mathrm{S}_n)| &= \textstyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\
&= \textstyle\sum_{k=0}^{n} (-1)^k \dfrac{n!}{k!(n-k)!} (n-k)! \\
&= n! \textstyle\sum_{k=0}^{n} \dfrac{(-1)^k}{k!}.
\end{aligned}
$$

Observation: The proportion $d(\mathrm{S}_n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ is the truncation of the Taylor series for e^x at $x = -1$.

Montmort's theorem - Applications

Card shuffling

Suppose you have a deck of n cards, numbered $1, 2, \cdots, n$. After shuffling, draw one card at a time without replacement, counting out loud as each card is drawn: '$1, 2, 3, \cdots$'.

Question: What is the probability that there will be no coincidence?

Montmort's theorem - Applications

Card shuffling

Suppose you have a deck of n cards, numbered $1, 2, \cdots, n$. After shuffling, draw one card at a time without replacement, counting out loud as each card is drawn: '$1, 2, 3, \cdots$'.

Question: What is the probability that there will be no coincidence?

This game is also called 'Treize', 'Rencontres' or 'Montmort's matching problem'.

Montmort's theorem - Applications

Card shuffling

Suppose you have a deck of n cards, numbered $1, 2, \cdots, n$. After shuffling, draw one card at a time without replacement, counting out loud as each card is drawn: '$1, 2, 3, \cdots$'.

Question: What is the probability that there will be no coincidence?

This game is also called 'Treize', 'Rencontres' or 'Montmort's matching problem'.

Secretary problem

If a secretary types n letters and addresses the envelopes, then puts the letters in envelopes at random.

Montmort's theorem - Applications

Card shuffling

Suppose you have a deck of n cards, numbered $1, 2, \cdots, n$. After shuffling, draw one card at a time without replacement, counting out loud as each card is drawn: '$1, 2, 3, \cdots$'.
Question: What is the probability that there will be no coincidence?

This game is also called 'Treize', 'Rencontres' or 'Montmort's matching problem'.

Secretary problem

If a secretary types n letters and addresses the envelopes, then puts the letters in envelopes at random.
Question: What is the probability that nobody gets their correct letter?

Montmort's theorem - Applications

Card shuffling

Suppose you have a deck of n cards, numbered $1, 2, \cdots, n$. After shuffling, draw one card at a time without replacement, counting out loud as each card is drawn: '$1, 2, 3, \cdots$'.
Question: What is the probability that there will be no coincidence?

This game is also called 'Treize', 'Rencontres' or 'Montmort's matching problem'.

Secretary problem

If a secretary types n letters and addresses the envelopes, then puts the letters in envelopes at random.
Question: What is the probability that nobody gets their correct letter?

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Orbit-Counting Lemma (Burnside's Lemma)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite permutation group. Then the number of orbits of G on Ω is the average number of fixed points of elements of G.

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Orbit-Counting Lemma (Burnside's Lemma)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite permutation group. Then the number of orbits of G on Ω is the average number of fixed points of elements of G.

Let $\mathcal{F}\mathrm{ix}(x) = \mathcal{F}\mathrm{ix}_{\Omega}(x) = \{\alpha \in \Omega : \alpha^x = \alpha\}$.

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Orbit-Counting Lemma (Burnside's Lemma)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite permutation group. Then the number of orbits of G on Ω is the average number of fixed points of elements of G.

Let $\mathcal{F}\mathrm{ix}(x) = \mathcal{F}\mathrm{ix}_\Omega(x) = \{\alpha \in \Omega : \alpha^x = \alpha\}$.

Let m be the number of G-orbits on Ω. Then

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Orbit-Counting Lemma (Burnside's Lemma)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite permutation group. Then the number of orbits of G on Ω is the average number of fixed points of elements of G.

Let $\mathcal{F}\mathrm{ix}(x) = \mathcal{F}\mathrm{ix}_{\Omega}(x) = \{\alpha \in \Omega : \alpha^x = \alpha\}$.

Let m be the number of G-orbits on Ω. Then

$$m = \frac{1}{|G|}\sum_{g \in G} |\mathcal{F}\mathrm{ix}_{\Omega}(g)|.$$

Jordan's theorem

Theorem (Jordan, 1872)

Every finite transitive permutation group of degree $n \geq 2$ contains a derangement.

The proof of Jordan's theorem is based on the following lemma:

Orbit-Counting Lemma (Burnside's Lemma)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite permutation group. Then the number of orbits of G on Ω is the average number of fixed points of elements of G.

Let $\mathcal{F}\mathrm{ix}(x) = \mathcal{F}\mathrm{ix}_\Omega(x) = \{\alpha \in \Omega : \alpha^x = \alpha\}$.

Let m be the number of G-orbits on Ω. Then

$$m = \frac{1}{|G|} \sum_{g \in G} |\mathcal{F}\mathrm{ix}_\Omega(g)|.$$

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.
- So Δ has $|G|$ edges and Γ has $m|G|$ edges.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.
- So Δ has $|G|$ edges and Γ has $m|G|$ edges.
- For $g \in G$, there are exactly $|\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.
- So Δ has $|G|$ edges and Γ has $m|G|$ edges.
- For $g \in G$, there are exactly $|\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.
- So Γ has $\sum_{g \in G} |\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.
- So Δ has $|G|$ edges and Γ has $m|G|$ edges.
- For $g \in G$, there are exactly $|\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.
- So Γ has $\sum_{g\in G} |\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.
- Therefore, $\sum_{g\in G} |\mathcal{F}\mathrm{ix}_\Omega(g)| = m|G|$.

A proof of Orbit-Counting Lemma

- Consider the bipartite graph Γ with vertex set $\Omega \cup G$ and there is an edge between $\alpha \in \Omega$, $g \in G$ iff $\alpha^g = \alpha$.
- Count the number of edges of Γ in two different ways.
- Let Δ be a G-orbit on Ω and $\alpha \in \Delta$.
- The number of edges going through α is $|G_\alpha| = \dfrac{|G|}{|\Delta|}$.
- So Δ has $|G|$ edges and Γ has $m|G|$ edges.
- For $g \in G$, there are exactly $|\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.
- So Γ has $\sum_{g \in G} |\mathcal{F}\mathrm{ix}_\Omega(g)|$ edges.
- Therefore, $\sum_{g \in G} |\mathcal{F}\mathrm{ix}_\Omega(g)| = m|G|$.

Jordan's theorem-Variations

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group.
- By Jordan's theorem, G always contains a derangement.

Jordan's theorem-Variations

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group.
- By Jordan's theorem, G always contains a derangement.

Questions

- What is the proportion of derangements in G?

Jordan's theorem-Variations

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group.
- By Jordan's theorem, G always contains a derangement.

Questions

- What is the proportion of derangements in G?
- Does G contain derangements with special properties?

Jordan's theorem-Variations

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group.
- By Jordan's theorem, G always contains a derangement.

Questions

- What is the proportion of derangements in G?
- Does G contain derangements with special properties?
- What is the structure of G if we impose some restrictions on $\Delta(G)$?

Jordan's theorem-Variations

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group.
- By Jordan's theorem, G always contains a derangement.

Questions

- What is the proportion of derangements in G?
- Does G contain derangements with special properties?
- What is the structure of G if we impose some restrictions on $\Delta(G)$?

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.
- If $G = \mathrm{D}_8 \leq \mathrm{Sym}(\Omega)$ is the group of symmetries of a square with vertex set $\Omega = \{1, 2, 3, 4\}$, then $\{1, 3\}$ is a nontrivial block of G.

Primitivity

- Let $G \le \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.
- If $G = \mathrm{D}_8 \le \mathrm{Sym}(\Omega)$ is the group of symmetries of a square with vertex set $\Omega = \{1, 2, 3, 4\}$, then $\{1, 3\}$ is a nontrivial block of G.

Definition

A transitive group $G \le \mathrm{Sym}(\Omega)$ is imprimitive if G has a nontrivial block.

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.
- If $G = \mathrm{D}_8 \leq \mathrm{Sym}(\Omega)$ is the group of symmetries of a square with vertex set $\Omega = \{1, 2, 3, 4\}$, then $\{1, 3\}$ is a nontrivial block of G.

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is imprimitive if G has a nontrivial block. Otherwise, G is primitive.

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.
- If $G = \mathrm{D}_8 \leq \mathrm{Sym}(\Omega)$ is the group of symmetries of a square with vertex set $\Omega = \{1, 2, 3, 4\}$, then $\{1, 3\}$ is a nontrivial block of G.

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is imprimitive if G has a nontrivial block. Otherwise, G is primitive.

Equivalently, G is primitive if and only if the point stabilizer G_α is a maximal subgroup of G.

Primitivity

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H.
- A nonempty subset $\Delta \subseteq \Omega$ is a block of G if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.
- Ω and $\{\alpha\}$ for $\alpha \in \Omega$ are trivial blocks of G.
- If $G = \mathrm{D}_8 \leq \mathrm{Sym}(\Omega)$ is the group of symmetries of a square with vertex set $\Omega = \{1, 2, 3, 4\}$, then $\{1, 3\}$ is a nontrivial block of G.

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is imprimitive if G has a nontrivial block. Otherwise, G is primitive.

Equivalently, G is primitive if and only if the point stabilizer G_α is a maximal subgroup of G.

Almost simple and Affine groups

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is almost simple if there exists a nonabelian simple group T such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$.

G is primitive if and only if G_α is maximal in G.

Almost simple and Affine groups

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is almost simple if there exists a nonabelian simple group T such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$.

G is primitive if and only if G_α is maximal in G.

Definition

Let p be a prime and let $V = \mathbb{Z}_p^d$. Let $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ be the group of affine transformations of V :

$$\tau_{x,u}(v) = vx + u \text{ (for } x \in \mathrm{GL}(V), u \in V).$$

Almost simple and Affine groups

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is almost simple if there exists a nonabelian simple group T such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$.

G is primitive if and only if G_α is maximal in G.

Definition

Let p be a prime and let $V = \mathbb{Z}_p^d$. Let $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ be the group of affine transformations of V :

$$\tau_{x,u}(v) = vx + u \text{ (for } x \in \mathrm{GL}(V), u \in V).$$

$G \leq \mathrm{Sym}(V)$ is affine if $V \trianglelefteq G \leq \mathrm{AGL}(V)$.

Almost simple and Affine groups

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is almost simple if there exists a nonabelian simple group T such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$.

G is primitive if and only if G_α is maximal in G.

Definition

Let p be a prime and let $V = \mathbb{Z}_p^d$. Let $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ be the group of affine transformations of V :

$$\tau_{x,u}(v) = vx + u \text{ (for } x \in \mathrm{GL}(V), u \in V).$$

$G \leq \mathrm{Sym}(V)$ is affine if $V \trianglelefteq G \leq \mathrm{AGL}(V)$.

G is primitive if and only if $G_0 \leq \mathrm{GL}(V)$ is irreducible.

Almost simple and Affine groups

Definition

A transitive group $G \leq \mathrm{Sym}(\Omega)$ is almost simple if there exists a nonabelian simple group T such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$.

G is primitive if and only if G_α is maximal in G.

Definition

Let p be a prime and let $V = \mathbb{Z}_p^d$. Let $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ be the group of affine transformations of V :

$$\tau_{x,u}(v) = vx + u \text{ (for } x \in \mathrm{GL}(V), u \in V).$$

$G \leq \mathrm{Sym}(V)$ is affine if $V \trianglelefteq G \leq \mathrm{AGL}(V)$.

G is primitive if and only if $G_0 \leq \mathrm{GL}(V)$ is irreducible.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.
2. G is of affine type.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.
2. G is of affine type.
3. G is of diagonal type.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.
2. G is of affine type.
3. G is of diagonal type.
4. G is of product type.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.
2. G is of affine type.
3. G is of diagonal type.
4. G is of product type.
5. G is of twisted wreath product type.

O'Nan-Scott-Aschbacher Theorem

Theorem

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then one of the following holds:

1. G is almost simple.
2. G is of affine type.
3. G is of diagonal type.
4. G is of product type.
5. G is of twisted wreath product type.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Theorem (Cameron-Cohen, 1992)

$d(G) \geq \frac{1}{n}$ with equality if and only if G is sharply 2-transitive.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Theorem (Cameron-Cohen, 1992)

$d(G) \geq \frac{1}{n}$ with equality if and only if G is sharply 2-transitive.

- G is 2-transitive if the natural action of G on $\Gamma = \{(\alpha, \beta) : \alpha \neq \beta \in \Omega\}$ is transitive.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Theorem (Cameron-Cohen, 1992)

$d(G) \geq \frac{1}{n}$ with equality if and only if G is sharply 2-transitive.

- G is 2-transitive if the natural action of G on $\Gamma = \{(\alpha, \beta) : \alpha \neq \beta \in \Omega\}$ is transitive.
- It is sharply 2-transitive if furthermore, $G_{(\alpha,\beta)} = 1$ for some $(\alpha, \beta) \in \Gamma$.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Theorem (Cameron-Cohen, 1992)

$d(G) \geq \frac{1}{n}$ with equality if and only if G is sharply 2-transitive.

- G is 2-transitive if the natural action of G on $\Gamma = \{(\alpha, \beta) : \alpha \neq \beta \in \Omega\}$ is transitive.
- It is sharply 2-transitive if furthermore, $G_{(\alpha,\beta)} = 1$ for some $(\alpha, \beta) \in \Gamma$.
- This bound is best possible but we can get better bounds by allowing more exceptions.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.
- We have $d(G) > 0$ by Jordan's theorem.

Theorem (Cameron-Cohen, 1992)

$d(G) \geq \frac{1}{n}$ with equality if and only if G is sharply 2-transitive.

- G is 2-transitive if the natural action of G on $\Gamma = \{(\alpha, \beta) : \alpha \neq \beta \in \Omega\}$ is transitive.
- It is sharply 2-transitive if furthermore, $G_{(\alpha,\beta)} = 1$ for some $(\alpha, \beta) \in \Gamma$.
- This bound is best possible but we can get better bounds by allowing more exceptions.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.

Theorem (Guralnick-Wan, 1997)

One of the following holds.

- $d(G) \geq 2/n$.
- G is sharply 2-transitive.
- $(G, n, d(G)) = (\mathrm{S}_5, 5, 11/30)$ or $(\mathrm{S}_4, 4, 3/8)$.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.

Theorem (Guralnick-Wan, 1997)

One of the following holds.

- $d(G) \geq 2/n$.
- G is sharply 2-transitive.
- $(G, n, d(G)) = (\mathrm{S}_5, 5, 11/30)$ or $(\mathrm{S}_4, 4, 3/8)$.

- The proof uses the classification of 2-transitive groups.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.

Theorem (Guralnick-Wan, 1997)

One of the following holds.

- $d(G) \geq 2/n$.
- G is sharply 2-transitive.
- $(G, n, d(G)) = (\mathrm{S}_5, 5, 11/30)$ or $(\mathrm{S}_4, 4, 3/8)$.

- The proof uses the classification of 2-transitive groups.
- This result has applications to algebraic curves over finite fields.

Bounding $d(G)$ in terms of the degree

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with $n = |\Omega| \geq 2$.

Theorem (Guralnick-Wan, 1997)

One of the following holds.

- $d(G) \geq 2/n$.
- G is sharply 2-transitive.
- $(G, n, d(G)) = (\mathrm{S}_5, 5, 11/30)$ or $(\mathrm{S}_4, 4, 3/8)$.

- The proof uses the classification of 2-transitive groups.
- This result has applications to algebraic curves over finite fields.

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

- Let π be the permutation character of G.

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

- Let π be the permutation character of G.
- Observe that $(\pi, \pi) = r$ and $\pi(g) = 0$ for all $g \in \Delta(G)$. We have

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

- Let π be the permutation character of G.
- Observe that $(\pi, \pi) = r$ and $\pi(g) = 0$ for all $g \in \Delta(G)$. We have

$$r|G| = \sum_{g \in G} \pi(g)^2 = \sum_{g \in G \setminus \Delta(G)} \pi(g)^2 \geq \frac{1}{|G| - |\Delta(G)|}\Big(\sum_{g \in G \setminus \Delta(G)} \pi(g)\Big)^2.$$

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

- Let π be the permutation character of G.
- Observe that $(\pi, \pi) = r$ and $\pi(g) = 0$ for all $g \in \Delta(G)$. We have

$$r|G| = \sum_{g \in G} \pi(g)^2 = \sum_{g \in G \setminus \Delta(G)} \pi(g)^2 \geq \frac{1}{|G| - |\Delta(G)|} \Big(\sum_{g \in G \setminus \Delta(G)} \pi(g) \Big)^2.$$

- As $(\pi, 1_G) = 1$ we have $|G| = \sum_{g \in G} \pi(g) = \sum_{g \in G \setminus \Delta(G)} \pi(g)$.
- So $r|G| \geq \frac{|G|^2}{|G| - |\Delta(G)|}$ and the first part holds.

Bounding $d(G)$ in terms of the rank

- Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group with $n = |\Omega| \geq 2$.
- The rank of G is the number of orbits of G on $\Omega \times \Omega$.

Theorem (Guralnick-Isaacs-Spiga, 2015)

$d(G) \leq 1 - \frac{1}{r}$ with equality if and only if G acts regularly.

- Let π be the permutation character of G.
- Observe that $(\pi, \pi) = r$ and $\pi(g) = 0$ for all $g \in \Delta(G)$. We have

$$r|G| = \sum_{g \in G} \pi(g)^2 = \sum_{g \in G \setminus \Delta(G)} \pi(g)^2 \geq \frac{1}{|G| - |\Delta(G)|}\Big(\sum_{g \in G \setminus \Delta(G)} \pi(g)\Big)^2.$$

- As $(\pi, 1_G) = 1$ we have $|G| = \sum_{g \in G} \pi(g) = \sum_{g \in G \setminus \Delta(G)} \pi(g)$.
- So $r|G| \geq \frac{|G|^2}{|G| - |\Delta(G)|}$ and the first part holds.

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?
- $d(\mathrm{A}_n) \geq \frac{1}{3}$ and $d(\mathrm{PSL}_2(q)) \geq \frac{1}{3}$ for all $n, q \geq 5$.

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?
- $d(\mathrm{A}_n) \geq \frac{1}{3}$ and $d(\mathrm{PSL}_2(q)) \geq \frac{1}{3}$ for all $n, q \geq 5$.

Theorem (Fulman-Guralnick, 2014)

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

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?
- $d(\mathrm{A}_n) \geq \frac{1}{3}$ and $d(\mathrm{PSL}_2(q)) \geq \frac{1}{3}$ for all $n, q \geq 5$.

Theorem (Fulman-Guralnick, 2014)

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

- The absolute constant ϵ is unknown.

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?
- $d(\mathrm{A}_n) \geq \frac{1}{3}$ and $d(\mathrm{PSL}_2(q)) \geq \frac{1}{3}$ for all $n, q \geq 5$.

Theorem (Fulman-Guralnick, 2014)

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

- The absolute constant ϵ is unknown.
- This confirms a conjecture due to Boston et al. (1993) and Shalev.

Simple groups

- Montmort's theorem: $d(\mathrm{S}_n) \geq \frac{1}{e}$.
- Question: what is the asymptotic behavior of $d(G)$ for other infinite families of groups?
- $d(\mathrm{A}_n) \geq \frac{1}{3}$ and $d(\mathrm{PSL}_2(q)) \geq \frac{1}{3}$ for all $n, q \geq 5$.

Theorem (Fulman-Guralnick, 2014)

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

- The absolute constant ϵ is unknown.
- This confirms a conjecture due to Boston et al. (1993) and Shalev.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.
- We can assume that G is primitive.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.
- We can assume that G is primitive.
- Let $1 \neq N \trianglelefteq G$. Then N is transitive. So by the minimality of $|G|$, we can assume $N = G$. Thus G is a simple group.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.
- We can assume that G is primitive.
- Let $1 \neq N \trianglelefteq G$. Then N is transitive. So by the minimality of $|G|$, we can assume $N = G$. Thus G is a simple group.

Question: Find a proof of FKS-theorem without using the classification.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.
- We can assume that G is primitive.
- Let $1 \neq N \trianglelefteq G$. Then N is transitive. So by the minimality of $|G|$, we can assume $N = G$. Thus G is a simple group.

Question: Find a proof of FKS-theorem without using the classification.

Theorem

Let L/K be a finite extension of global fields with $L \neq K$. Then the relative Brauer group $B(L/K)$ is infinite.

Derangements of prime power order

Question: Does G contain derangements of prime power order?

Theorem (Fein, Kantor, Schacher, 1981)

Every transitive group contains a derangement of prime power order.

- Let G be a counterexample with $|G|$ minimal.
- We can assume that G is primitive.
- Let $1 \neq N \trianglelefteq G$. Then N is transitive. So by the minimality of $|G|$, we can assume $N = G$. Thus G is a simple group.

Question: Find a proof of FKS-theorem without using the classification.

Theorem

Let L/K be a finite extension of global fields with $L \neq K$. Then the relative Brauer group $B(L/K)$ is infinite.

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.
- Then every element in $\Delta(G)$ has order 4 or 8.

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.
- Then every element in $\Delta(G)$ has order 4 or 8.

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

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.
- Then every element in $\Delta(G)$ has order 4 or 8.

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

Theorem (Giudici, 2003)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive elusive group. Then $G = \mathrm{M}_{11} \wr L$ acting with its product action on $\Omega = \Gamma^k$, where $k \geq 1, L \leq \mathrm{S}_k$ is transitive and $|\Gamma| = 12$.

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.
- Then every element in $\Delta(G)$ has order 4 or 8.

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

Theorem (Giudici, 2003)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive elusive group. Then $G = \mathrm{M}_{11} \wr L$ acting with its product action on $\Omega = \Gamma^k$, where $k \geq 1, L \leq \mathrm{S}_k$ is transitive and $|\Gamma| = 12$.

Conjecture (Marušič, 1981)

Every finite vertex-transitive digraph contains a derangement of prime order.

Elusive groups

Question: Does transitive group contain derangements of prime order?

- Let $G = \mathrm{M}_{11}, H = \mathrm{PSL}_2(11)$ and $\Omega = G/H$.
- Then every element in $\Delta(G)$ has order 4 or 8.

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

Theorem (Giudici, 2003)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive elusive group. Then $G = \mathrm{M}_{11} \wr L$ acting with its product action on $\Omega = \Gamma^k$, where $k \geq 1, L \leq \mathrm{S}_k$ is transitive and $|\Gamma| = 12$.

Conjecture (Marušič, 1981)

Every finite vertex-transitive digraph contains a derangement of prime order.

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

- G is sharply 2-transitive or

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

- G is sharply 2-transitive or
- $(G, n) = (\mathrm{A}_5, 6)$ or $(\mathrm{Aut}(\mathrm{PSL}_2(8)), 28)$.

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

- G is sharply 2-transitive or
- $(G, n) = (\mathrm{A}_5, 6)$ or $(\mathrm{Aut}(\mathrm{PSL}_2(8)), 28)$.

- 'Primitivity' was replaced by 'transitivity' by (Guralnick, 2015).

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

- G is sharply 2-transitive or
- $(G, n) = (\mathrm{A}_5, 6)$ or $(\mathrm{Aut}(\mathrm{PSL}_2(8)), 28)$.

- 'Primitivity' was replaced by 'transitivity' by (Guralnick, 2015).
- For almost simple groups G, we have $\kappa(G) \to \infty$ when $|G| \to \infty$.

Conjugacy classes

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group with point stabilizer H.
- Let $\kappa(G)$ be the number of conjugacy classes in $\Delta(G)$.
- (Jordan's theorem) $\kappa(G) \geq 1$.

Theorem (Burness &T-V, 2014)

Let G be a finite primitive group of degree n. Then $\kappa(G) = 1$ if and only if

- G is sharply 2-transitive or
- $(G, n) = (\mathrm{A}_5, 6)$ or $(\mathrm{Aut}(\mathrm{PSL}_2(8)), 28)$.

- 'Primitivity' was replaced by 'transitivity' by (Guralnick, 2015).
- For almost simple groups G, we have $\kappa(G) \to \infty$ when $|G| \to \infty$.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case** N **is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case N is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.
- If N is nonabelian, then $|N|$ is divisible by at least 3 primes. Thus N is abelain and so $N \leq \mathrm{C}_G(x)$.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case N is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.
- If N is nonabelian, then $|N|$ is divisible by at least 3 primes. Thus N is abelain and so $N \leq \mathrm{C}_G(x)$.
- $|\Delta(G)| = |G : \mathrm{C}_G(x)| \leq |G : N| = |H| = |G|/n$. Thus $d(G) \leq \frac{1}{n}$.

1

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case N is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.
- If N is nonabelian, then $|N|$ is divisible by at least 3 primes. Thus N is abelain and so $N \leq \mathrm{C}_G(x)$.
- $|\Delta(G)| = |G : \mathrm{C}_G(x)| \leq |G : N| = |H| = |G|/n$. Thus $d(G) \leq \frac{1}{n}$.
- However, Cameron-Cohen implies that $d(G) \geq \frac{1}{n}$ with equality iff G is sharply 2-transitive.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case N is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.
- If N is nonabelian, then $|N|$ is divisible by at least 3 primes. Thus N is abelain and so $N \leq \mathrm{C}_G(x)$.
- $|\Delta(G)| = |G : \mathrm{C}_G(x)| \leq |G : N| = |H| = |G|/n$. Thus $d(G) \leq \frac{1}{n}$.
- However, Cameron-Cohen implies that $d(G) \geq \frac{1}{n}$ with equality iff G is sharply 2-transitive.
- **Case N is not regular**: G is almost simple.

Proof

Theorem (Reduction)

Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group. Then $\kappa(G) = 1$ if and only if G is almost simple or G is sharply 2-transitive.

- Suppose $\Delta(G) = x^G$.
- Let $N \trianglelefteq G$ and $H = G_\alpha$. Then N is transitive and $G = HN$.
- **Case N is regular**: $H \cap N = 1$ and $N = \{1\} \cup x^G$.
- If N is nonabelian, then $|N|$ is divisible by at least 3 primes. Thus N is abelain and so $N \leq \mathrm{C}_G(x)$.
- $|\Delta(G)| = |G : \mathrm{C}_G(x)| \leq |G : N| = |H| = |G|/n$. Thus $d(G) \leq \frac{1}{n}$.
- However, Cameron-Cohen implies that $d(G) \geq \frac{1}{n}$ with equality iff G is sharply 2-transitive.
- **Case N is not regular**: G is almost simple.

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;
- a finite simple group of Lie type.

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;
- a finite simple group of Lie type.

- Use GAP or ATLAS for sporadic simple groups.

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;
- a finite simple group of Lie type.

- Use GAP or ATLAS for sporadic simple groups.
- (Jordan's theorem) If G is a primitive group of degree n containing a cycle of prime length fixing at least 3 points, then $\mathrm{A}_n \leq G$.

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;
- a finite simple group of Lie type.

- Use GAP or ATLAS for sporadic simple groups.
- (Jordan's theorem) If G is a primitive group of degree n containing a cycle of prime length fixing at least 3 points, then $\mathrm{A}_n \leq G$.
- For groups of Lie type G with simple socle T, choose two distinct conjugacy classes x_1^G and x_2^G, where $x_i \in T$ such that both x_i's lie in a small number of maximal subgroups of G.

Proof - Almost simple groups

Theorem (CFSG)

Every non-abelian finite simple group is one of the following:

- one of the 26 sporadic simple groups;
- an alternating group A_n wih $n \geq 5$;
- a finite simple group of Lie type.

- Use GAP or ATLAS for sporadic simple groups.
- (Jordan's theorem) If G is a primitive group of degree n containing a cycle of prime length fixing at least 3 points, then $\mathrm{A}_n \leq G$.
- For groups of Lie type G with simple socle T, choose two distinct conjugacy classes x_1^G and x_2^G, where $x_i \in T$ such that both $x_i' s$ lie in a small number of maximal subgroups of G.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.
- (Burnside's theorem, 1911): $\chi(g) = 0$ for some $g \in G$.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.
- (Burnside's theorem, 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.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.
- (Burnside's theorem, 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.
- Let $n(\chi)$ be the number of G-classes on which G vanishes.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.
- (Burnside's theorem, 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.
- Let $n(\chi)$ be the number of G-classes on which G vanishes.

Problem

Classify all the pairs (G, χ) with $n(\chi) = 1$ for some nonlinear $\chi \in \mathrm{Irr}(G)$.

Zeros of characters

- Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G.
- Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$.
- (Burnside's theorem, 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.
- Let $n(\chi)$ be the number of G-classes on which G vanishes.

Problem

Classify all the pairs (G, χ) with $n(\chi) = 1$ for some nonlinear $\chi \in \mathrm{Irr}(G)$.

Zeros of characters

- If χ is imprimitive, i.e., $\chi = \theta^G$ for some $\theta \in \mathrm{Irr}(H)$ with $H < G$, then $n(\chi) = 1$ implies that $G \setminus \cup_{g \in G} H^g = x^G$ for some $g \in G$.
- If H is core-free, then our theorem applies.

Zeros of characters

- If χ is imprimitive, i.e., $\chi = \theta^G$ for some $\theta \in \mathrm{Irr}(H)$ with $H < G$, then $n(\chi) = 1$ implies that $G \setminus \cup_{g \in G} H^g = x^G$ for some $g \in G$.
- If H is core-free, then our theorem applies.
- In general, we obtain some restriction on the normal structure of G.

Zeros of characters

- If χ is imprimitive, i.e., $\chi = \theta^G$ for some $\theta \in \mathrm{Irr}(H)$ with $H < G$, then $n(\chi) = 1$ implies that $G \setminus \cup_{g \in G} H^g = x^G$ for some $g \in G$.
- If H is core-free, then our theorem applies.
- In general, we obtain some restriction on the normal structure of G.

Remarks

- If $G \leq \mathrm{Sym}(\Omega)$ is primitive and $\kappa(G) = 2$, then G is either almost simple or affine.

Zeros of characters

- If χ is imprimitive, i.e., $\chi = \theta^G$ for some $\theta \in \mathrm{Irr}(H)$ with $H < G$, then $n(\chi) = 1$ implies that $G \setminus \cup_{g \in G} H^g = x^G$ for some $g \in G$.
- If H is core-free, then our theorem applies.
- In general, we obtain some restriction on the normal structure of G.

Remarks

- If $G \leq \mathrm{Sym}(\Omega)$ is primitive and $\kappa(G) = 2$, then G is either almost simple or affine.
- If $\Delta(G) = x^G$, then every element in $\Delta(G)$ has the same order which is a power of some prime.

Zeros of characters

- If χ is imprimitive, i.e., $\chi = \theta^G$ for some $\theta \in \mathrm{Irr}(H)$ with $H < G$, then $n(\chi) = 1$ implies that $G \setminus \cup_{g \in G} H^g = x^G$ for some $g \in G$.
- If H is core-free, then our theorem applies.
- In general, we obtain some restriction on the normal structure of G.

Remarks

- If $G \leq \mathrm{Sym}(\Omega)$ is primitive and $\kappa(G) = 2$, then G is either almost simple or affine.
- If $\Delta(G) = x^G$, then every element in $\Delta(G)$ has the same order which is a power of some prime.

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): G has a derangement of prime power order.

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): G has a derangement of prime power order.

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

If every derangement in G is an involution, then either

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): 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

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): 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 an elementary abelian 2-group kernel.

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): 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 an elementary abelian 2-group kernel.

Problem 1: Classify transitive groups in which all derangements have prime order $p > 2$.

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): 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 an elementary abelian 2-group kernel.

Problem 1: Classify transitive groups in which all derangements have prime order $p > 2$.

Problem 2: Classify transitive groups whose all derangements are r-elements for some fixed prime r.

Derangements of prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.
- (Fein, Kantor, Schacher, 1981): 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 an elementary abelian 2-group kernel.

Problem 1: Classify transitive groups in which all derangements have prime order $p > 2$.

Problem 2: Classify transitive groups whose all derangements are r-elements for some fixed prime r.

Prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group with point stabilizer H.
- Property (*): Every derangement in G is an r-element for some fixed prime r.

Prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group with point stabilizer H.
- Property (*): Every derangement in G is an r-element for some fixed prime r.

Theorem (Burness & TV, 2014)

- If (*) holds, then G is either almost simple or affine.

Prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group with point stabilizer H.
- Property (*): Every derangement in G is an r-element for some fixed prime r.

Theorem (Burness & TV, 2014)

- If (*) holds, then G is either almost simple or affine.
- The almost simple groups satisfying (*) are completely classified. We have $\mathrm{Soc}(G) = \mathrm{PSL}_2(q), \mathrm{PSL}_3(q)$ for some prime power q or $(G, H) = (\mathrm{M}_{11}, \mathrm{PSL}_2(11))$.

Prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group with point stabilizer H.
- Property (*): Every derangement in G is an r-element for some fixed prime r.

Theorem (Burness & TV, 2014)

- If (*) holds, then G is either almost simple or affine.
- The almost simple groups satisfying (*) are completely classified. We have $\mathrm{Soc}(G) = \mathrm{PSL}_2(q), \mathrm{PSL}_3(q)$ for some prime power q or $(G, H) = (\mathrm{M}_{11}, \mathrm{PSL}_2(11))$.
- If $G \leq \mathrm{AGL(V)}$ is affine with $V = \mathbb{Z}_p^d$, then (*) holds iff $r = p$ and every two point stabilizer in G is an r-group.

Prime power order

- Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive group with point stabilizer H.
- Property (*): Every derangement in G is an r-element for some fixed prime r.

Theorem (Burness & TV, 2014)

- If (*) holds, then G is either almost simple or affine.
- The almost simple groups satisfying (*) are completely classified. We have $\mathrm{Soc}(G) = \mathrm{PSL}_2(q), \mathrm{PSL}_3(q)$ for some prime power q or $(G, H) = (\mathrm{M}_{11}, \mathrm{PSL}_2(11))$.
- If $G \leq \mathrm{AGL(V)}$ is affine with $V = \mathbb{Z}_p^d$, then (*) holds iff $r = p$ and every two point stabilizer in G is an r-group.

Some connections

- The affine groups with property (*) have been studied extensively.
- (Guralnick, Wan, 1992): Structure of Galois field extension

Some connections

- The affine groups with property (*) have been studied extensively.
- (Guralnick, Wan, 1992): Structure of Galois field extension
- (Fleischmann, Lempken, Tiep, 1997): r'-semiregular pairs.

Some connections

- The affine groups with property (*) have been studied extensively.
- (Guralnick, Wan, 1992): Structure of Galois field extension
- (Fleischmann, Lempken, Tiep, 1997): r'-semiregular pairs.

Definition

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

$$m = \max\{|\Gamma^x \setminus \Gamma| : \Gamma \subseteq \Omega, x \in G\}.$$

We say that G has movement m.

Some connections

- The affine groups with property (*) have been studied extensively.
- (Guralnick, Wan, 1992): Structure of Galois field extension
- (Fleischmann, Lempken, Tiep, 1997): r'-semiregular pairs.

Definition

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

$$m = \max\{|\Gamma^x \setminus \Gamma| : \Gamma \subseteq \Omega, x \in G\}.$$

We say that G has movement m.

Theorem (Hassani, Khayaty, Khukhro, Praeger, 1999)

If G is not a 2-group and $n = \lfloor 2mp/(p-1) \rfloor$, where $p \geq 5$ is the least odd prime dividing $|G|$, then $p \mid n$ and every derangement in G has order p.

Some connections

- The affine groups with property (*) have been studied extensively.
- (Guralnick, Wan, 1992): Structure of Galois field extension
- (Fleischmann, Lempken, Tiep, 1997): r'-semiregular pairs.

Definition

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

$$m = \max\{|\Gamma^x \setminus \Gamma| : \Gamma \subseteq \Omega, x \in G\}.$$

We say that G has movement m.

Theorem (Hassani, Khayaty, Khukhro, Praeger, 1999)

If G is not a 2-group and $n = \lfloor 2mp/(p-1) \rfloor$, where $p \geq 5$ is the least odd prime dividing $|G|$, then $p \mid n$ and every derangement in G has order p.

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Conjecture

Let $G = HV \leq \mathrm{AGL}(V)$ be a finite affine primitive group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where p is a prime and $k \geq 1$.

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Conjecture

Let $G = HV \leq \mathrm{AGL}(V)$ be a finite affine primitive group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where p is a prime and $k \geq 1$. Then G has property (*) iff $r = p$ and the following two conditions hold:

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Conjecture

Let $G = HV \leq \mathrm{AGL}(V)$ be a finite affine primitive group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where p is a prime and $k \geq 1$.Then G has property (*) iff $r = p$ and the following two conditions hold:

(i) Every two-point stabilizer in G is an r-group;

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Conjecture

Let $G = HV \leq \mathrm{AGL}(V)$ be a finite affine primitive group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where p is a prime and $k \geq 1$.Then G has property (*) iff $r = p$ and the following two conditions hold:

(i) Every two-point stabilizer in G is an r-group;

(ii) A Sylow r-subgroup of G has exponent r.

Derangements in p-groups

Problem (Mann-Praeger, 1996)

If $G \leq \mathrm{Sym}(\Omega)$ is a transitive p-group for some prime p, then every derangement of G has order p if and only if G has exponent p.

- (Mann-Praeger, 1996): This is true if $p = 2, 3$.

Conjecture

Let $G = HV \leq \mathrm{AGL}(V)$ be a finite affine primitive group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where p is a prime and $k \geq 1$.Then G has property (*) iff $r = p$ and the following two conditions hold:

(i) Every two-point stabilizer in G is an r-group;

(ii) A Sylow r-subgroup of G has exponent r.

Some open problems

- Marušič's conjecture on vertex-transitive graphs (and more general, the polycirculant conjecture).
- Isbell's conjecture: There is a function f_p such that if $n = p^a b$ with $\gcd(b, p) = 1$ and $a > f_p(b)$, then any transitive group of degree n contains a derangement of p-power order.
- (J.G. Thompson) If G is primitive group, then $\Delta(G)$ is a transitive subset of G. (There is a reduction to almost simple groups).