Automorphism orbits of groups and the Monster

Michael Giudici

Centre for the Mathematics of Symmetry and Computation

THE UNIVERSITY OF WESTERN AUSTRALIA

joint work with Alexander Bors and Cheryl E. Praeger

Ischia Group Theory 2020/2021

March 25–26 2021

Introduction

G a finite group, $\mathrm{Aut}(G)$

Introduction

G a finite group, $\mathrm{Aut}(G)$

- $\mathrm{Aut}(G)$ acts transitively on $G \implies G = 1$.

Introduction

G a finite group, $\mathrm{Aut}(G)$

- $\mathrm{Aut}(G)$ acts transitively on $G \implies G = 1$.
- $\mathrm{Aut}(G)$ acts transitively on $G \backslash \{1\} \implies G = C_p^d$.

Let $\omega(G)$ denote the number of orbits of $\mathrm{Aut}(G)$ on G.

3 or 4 orbits

Laffey-MacHale (1986): Suppose that G is not a p-group:

- If $\omega(G) = 3$ then $|G| = p^a q$ for some primes p and q and G has a normal elementary abelian Sylow p-subgroup.

3 or 4 orbits

Laffey-MacHale (1986): Suppose that G is not a p-group:

- If $\omega(G) = 3$ then $|G| = p^a q$ for some primes p and q and G has a normal elementary abelian Sylow p-subgroup.
- If $\omega(G) = 4$ then $G = A_5$ or $|G| = p^a q^b$ or some primes p and q and G has a normal Sylow p-subgroup.

p-groups with $\omega(G) = 3$

Suppose that G is a p-group with $\omega(G) = 3$.

- Shult (1968): If p odd and G has exponent p^2 then G is abelian.
- Mäurer-Stroppel (1997): Give structural information in exponent p case and some examples.
- Bors-Glasby (2019): Classified the 2-groups G with $\omega(G) = 3$.

A different theme

Bors (2019): If $\mathrm{Aut}(G)$ has an orbit of length $> \frac{18|G|}{19}$ then G is soluble.

Conjectures true proportion is $3/7$ as achieved for $\mathrm{PSL}(2, 8)$.

AT-groups

A group is called an AT-group if for all integers k, $\mathrm{Aut}(G)$ acts transitively on the set of elements of G of order k.

AT-groups

A group is called an AT-group if for all integers k, $\mathrm{Aut}(G)$ acts transitively on the set of elements of G of order k.

Zhang (1992):

- Gave a structure theorem for AT-groups
- Only nonabelian simple ones are A_5, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, A_6 and $\mathrm{PSL}_3(4)$.

A variation

Let $o(G)$ denote the number of element orders in G.

Then G is an AT-group if and only if $o(G) = \omega(G)$.

A variation

Let $o(G)$ denote the number of element orders in G.

Then G is an AT-group if and only if $o(G) = \omega(G)$.

Question: How close can they be?

A variation

Define

$$\mathfrak{d}(G) = \omega(G) - o(G) \geqslant 0$$

$$\mathfrak{q}(G) = \frac{\omega(G)}{o(G)} \geqslant 1$$

Also define

$$\mathfrak{m}(G) = \begin{array}{l} \text{maximum over all } k \text{ of number of} \\ \mathrm{Aut}(G)\text{-orbits on set of elements of order } k \end{array}$$

A variation

Define

$$\mathfrak{d}(G) = \omega(G) - o(G) \geqslant 0$$

$$\mathfrak{q}(G) = \frac{\omega(G)}{o(G)} \geqslant 1$$

Also define

$$\mathfrak{m}(G) = \begin{array}{l}\text{maximum over all } k \text{ of number of} \\ \mathrm{Aut}(G)\text{-orbits on set of elements of order } k\end{array}$$

$$\mathfrak{m}(G) = 1 \iff \mathfrak{d}(G) = 0 \iff \mathfrak{q}(G) = 1 \iff G \text{ is an AT-group}$$

$$\mathfrak{q}(G) \leqslant \frac{o(G)\mathfrak{m}(G)}{o(G)} = \mathfrak{m}(G)$$

Bounding order of group

Let $\mathrm{Rad}(G)$ be the largest normal soluble subgroup of G.

Main Theorem I (Bors-Giudici-Praeger): There exist monotonically increasing functions f_1, f_2 such that

1. $|G : \mathrm{Rad}(G)| \leqslant f_1(\mathfrak{d}(G))$
2. $|G : \mathrm{Rad}(G)| \leqslant f_2(\mathfrak{q}(G), o(\mathrm{Rad}(G))$

Reduction Lemma

Lemma: Let N be a characteristic subgroup of G.

1. $\mathfrak{d}(N) \leqslant \mathfrak{d}(G)$
2. $\mathfrak{m}(N) \leqslant \mathfrak{m}(G)$
3. $\mathfrak{m}(G/N) \leqslant 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$

Reduction Lemma

Lemma: Let N be a characteristic subgroup of G.

1. $\mathfrak{d}(N) \leqslant \mathfrak{d}(G)$
2. $\mathfrak{m}(N) \leqslant \mathfrak{m}(G)$
3. $\mathfrak{m}(G/N) \leqslant 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$

Proof of (1): Aut(N)-orbits are unions of Aut(G)-orbits on N so

$$\mathfrak{d}G = \sum_{o \in Ord(G)} (\omega_o(G) - 1) \geqslant \sum_{o \in Ord(N)} (\omega_o(G) - 1) \geqslant \sum_{o \in Ord(N)} (\omega_o(N) - 1) = \mathfrak{d}N \quad \square$$

Reduction Lemma

Lemma: Let N be a characteristic subgroup of G.

1. $\mathfrak{d}(N) \leqslant \mathfrak{d}(G)$
2. $\mathfrak{m}(N) \leqslant \mathfrak{m}(G)$
3. $\mathfrak{m}(G/N) \leqslant 2^{\mathfrak{d}(G)} + \mathfrak{d}(G)$

Proof of (1): Aut(N)-orbits are unions of Aut(G)-orbits on N so

$$\begin{aligned}\mathfrak{d}G = \sum_{o \in Ord(G)} (\omega_o(G) - 1) &\geqslant \sum_{o \in Ord(N)} (\omega_o(G) - 1) \\ &\geqslant \sum_{o \in Ord(N)} (\omega_o(N) - 1) = \mathfrak{d}N \quad \square\end{aligned}$$

Take $N = \mathrm{Rad}(G)$. Want to bound $|G : N|$ by a function of $\mathfrak{m}(G/N)$.

Reduction to simple case

Note $\mathrm{soc}(G/N) = T_1^{n_1} \times \cdots \times T_k^{n_s}$ where T_i nonabelian simple groups.

Lemma:
$$\mathfrak{m}(G/N) \geqslant \mathfrak{m}(T_1^{n_1} \times \cdots \times T_s^{n_s}) \geqslant \prod_1^s n_i \mathfrak{m}(T_i)$$
$$\geqslant \max\{n_i, \mathfrak{m}(T_i)\} \geqslant \max\{n_i, \mathfrak{q}(T_i)\}$$

Reduction to simple case

Note $\mathrm{soc}(G/N) = T_1^{n_1} \times \cdots \times T_k^{n_s}$ where T_i nonabelian simple groups.

Lemma:
$$\mathfrak{m}(G/N) \geqslant \mathfrak{m}(T_1^{n_1} \times \cdots \times T_s^{n_s}) \geqslant \prod_1^s n_i \mathfrak{m}(T_i)$$
$$\geqslant \max\{n_i, \mathfrak{m}(T_i)\} \geqslant \max\{n_i, \mathfrak{q}(T_i)\}$$

So n_i and $\mathfrak{q}(T_i)$ are bounded above by $\mathfrak{m}(G/N)$.

We are trying to bound $|G/N|$ by a function of $\mathfrak{m}(G/N)$.

Reduction to simple case

Note $\mathrm{soc}(G/N) = T_1^{n_1} \times \cdots \times T_k^{n_s}$ where T_i nonabelian simple groups.

Lemma: $$\mathfrak{m}(G/N) \geqslant \mathfrak{m}(T_1^{n_1} \times \cdots \times T_s^{n_s}) \geqslant \prod_1^s n_i \mathfrak{m}(T_i)$$
$$\geqslant \max\{n_i, \mathfrak{m}(T_i)\} \geqslant \max\{n_i, \mathfrak{q}(T_i)\}$$

So n_i and $\mathfrak{q}(T_i)$ are bounded above by $\mathfrak{m}(G/N)$.

We are trying to bound $|G/N|$ by a function of $\mathfrak{m}(G/N)$.

Now
$G/N \leqslant \mathrm{Aut}(\mathrm{soc}(G/N)) = (\mathrm{Aut}(T_1) \wr S_{n_1}) \times \cdots \times (\mathrm{Aut}(T_s) \wr S_{n_s})$.

- $|\mathrm{Out}(T_i)|$ bounded above by $|T_i|$.
- Want to bound $|T_i|$ in terms of $\mathfrak{q}(T_i)$.

Some new parameters

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_\mathfrak{q}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Some new parameters

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_{\mathfrak{q}}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

1. $\frac{\log o(T)}{\log\omega(T)} \to 0$ as $|T| \to \infty$.

Some new parameters

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_\mathfrak{q}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

1. $\frac{\log o(T)}{\log\omega(T)} \to 0$ as $|T| \to \infty$.
2. $\epsilon_\omega(A_n) \to \frac{1}{2}$ and $\epsilon_\mathfrak{q}(A_n) \to \frac{1}{2}$ as $n \to \infty$
3. $\liminf_{|T|\to\infty} \epsilon_\omega(T) = \frac{1}{2} = \liminf_{|T|\to\infty} \epsilon_\mathfrak{q}(T)$.

Some new parameters

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_\mathfrak{q}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

1. $\frac{\log o(T)}{\log\omega(T)} \to 0$ as $|T| \to \infty$.
2. $\epsilon_\omega(A_n) \to \frac{1}{2}$ and $\epsilon_\mathfrak{q}(A_n) \to \frac{1}{2}$ as $n \to \infty$
3. $\liminf_{|T|\to\infty} \epsilon_\omega(T) = \frac{1}{2} = \liminf_{|T|\to\infty} \epsilon_\mathfrak{q}(T)$.
4. $\mathfrak{q}(T) \to \infty$ as $|T| \to \infty$

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_\mathfrak{q}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

5. $\epsilon_\omega(T) \geqslant \frac{\log\log 4}{\log\log 60} \approx 0.231720$, with equality if and only if $T \cong A_5$.

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_\mathfrak{q}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

5. $\epsilon_\omega(T) \geqslant \frac{\log\log 4}{\log\log 60} \approx 0.231720$, with equality if and only if $T \cong A_5$.
6. $\epsilon_\mathfrak{q}(T) \geqslant \epsilon_\mathfrak{q}(M) = \frac{\log\log(413/73)}{\log\log|M|} \approx 0.114045$, with equality if and only if $T \cong M$,

Define

$$\epsilon_\omega(T) = \frac{\log\log \omega(T)}{\log\log |T|}$$

$$\epsilon_{\mathfrak{q}}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log |T|}$$

Main Theorem II (Bors-Giudici-Praeger):

5. $\epsilon_\omega(T) \geqslant \frac{\log\log 4}{\log\log 60} \approx 0.231720$, with equality if and only if $T \cong A_5$.
6. $\epsilon_{\mathfrak{q}}(T) \geqslant \epsilon_{\mathfrak{q}}(M) = \frac{\log\log(413/73)}{\log\log|M|} \approx 0.114045$, with equality if and only if $T \cong M$, where M is the monster simple group.

This gives our bound for $|T|$ in terms of $\mathfrak{q}(T)$.

Define

$$\epsilon_\omega(T) = \frac{\log\log\omega(T)}{\log\log|T|}$$

$$\epsilon_{\mathfrak{q}}(T) = \frac{\log\log(\mathfrak{q}(T)+3)}{\log\log|T|}$$

Main Theorem II (Bors-Giudici-Praeger):

5. $\epsilon_\omega(T) \geqslant \frac{\log\log 4}{\log\log 60} \approx 0.231720$, with equality if and only if $T \cong A_5$.
6. $\epsilon_{\mathfrak{q}}(T) \geqslant \epsilon_{\mathfrak{q}}(M) = \frac{\log\log(413/73)}{\log\log|M|} \approx 0.114045$, with equality if and only if $T \cong M$, where M is the monster simple group.

This gives our bound for $|T|$ in terms of $\mathfrak{q}(T)$.

$$\mathfrak{q}(M) = 194/73 \qquad \mathfrak{q}(A_{43}) \cong 56 \qquad \mathfrak{q}(\mathrm{PSL}_7(13)) \geqslant 6180$$

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\mathrm{Out}(T)|}$

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\operatorname{Out}(T)|}$

$T = A_n$: use asymptotics on partitions and Erdős-Turan on element orders in S_n

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\mathrm{Out}(T)|}$

$T = A_n$: use asymptotics on partitions and Erdős-Turan on element orders in S_n

T a group of Lie type:

- Fulman-Guralnick: $k(\mathrm{InnDiag}(T)) \geqslant q^d$
- $o(T) \leqslant (\#\text{unipotent orders})(\#\text{semisimple orders})$

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\mathrm{Out}(T)|}$

$T = A_n$: use asymptotics on partitions and Erdős-Turan on element orders in S_n

T a group of Lie type:

- Fulman-Guralnick: $k(\mathrm{InnDiag}(T)) \geqslant q^d$
- $o(T) \leqslant (\#\text{unipotent orders})(\#\text{semisimple orders})$
- $$\begin{aligned}\#\text{ss orders} \leqslant & (\#\text{ conjugacy classes of maximal tori}) \times \\ & (\text{maximal }\#\text{ element orders in a maximal torus})\end{aligned}$$

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\text{Out}(T)|}$

$T = A_n$: use asymptotics on partitions and Erdős-Turan on element orders in S_n

T a group of Lie type:

- Fulman-Guralnick: $k(\text{InnDiag}(T)) \geqslant q^d$
- $o(T) \leqslant (\#\text{unipotent orders})(\#\text{semisimple orders})$
- $$\begin{aligned}\#\text{ss orders} \leqslant &(\#\text{ conjugacy classes of maximal tori})\times \\ &(\text{maximal }\#\text{ element orders in a maximal torus})\end{aligned}$$
- order of torus $\leqslant (q+1)^d$ so $\#$ element orders $\leqslant 2(q+1)^{d/2}$

Some tools

Note $\omega(G) \geqslant \frac{k(T)}{|\operatorname{Out}(T)|}$

$T = A_n$: use asymptotics on partitions and Erdős-Turan on element orders in S_n

T a group of Lie type:

- Fulman-Guralnick: $k(\mathrm{InnDiag}(T)) \geqslant q^d$
- $o(T) \leqslant (\#\text{unipotent orders})(\#\text{semisimple orders})$
-

$$\begin{aligned}\#\text{ss orders} \leqslant &(\#\text{ conjugacy classes of maximal tori})\times\\ &(\text{maximal }\#\text{ element orders in a maximal torus})\end{aligned}$$

- order of torus $\leqslant (q+1)^d$ so $\#$ element orders $\leqslant 2(q+1)^{d/2}$
- yields $o(T) \leqslant q^{(\frac{1}{2}+\frac{\epsilon}{2})d}$ if $\max\{d, q\} \geqslant N_2(\epsilon)$

Finishing up

Enough for asymptotics. Gives bounds for $\epsilon_{\omega}(T)$, $\epsilon_{\mathfrak{q}}(T)$ for large d and q.

For lower values of d and q use better bounds on number of conjugacy classes or exact structure of tori.

Finishing up

Enough for asymptotics. Gives bounds for $\epsilon_\omega(T)$, $\epsilon_\mathfrak{q}(T)$ for large d and q.

For lower values of d and q use better bounds on number of conjugacy classes or exact structure of tori.

Get down to 68 groups. Either calculate $\epsilon_\mathfrak{q}(T)$ exactly or get better bounds for $o(T)$.