Symmetry breaking on primitive groups

Hong Yi Huang

Seminars on Groups and Graphs

4 March 2023

University of BRISTOL

Automorphisms

Throughout, everything is finite.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\mathrm{Aut}(\Gamma)$**:** The group of all the automorphisms.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\mathrm{Aut}(\Gamma)$**:** The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \mathrm{Aut}(\Gamma) \cong S_n$

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\mathrm{Aut}(\Gamma)$**:** The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \mathrm{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n \ (n \geqslant 3) \implies \mathrm{Aut}(\Gamma) \cong D_{2n}$

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group Aut(Γ)**:** The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \mathrm{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n \ (n \geqslant 3) \implies \mathrm{Aut}(\Gamma) \cong D_{2n}$

How can we “break” the symmetries of a graph?

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple undirected graph.

Automorphism: $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group Aut(Γ)**:** The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \mathrm{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n \ (n \geqslant 3) \implies \mathrm{Aut}(\Gamma) \cong D_{2n}$

How can we "break" the symmetries of a graph?

- Colouring vertices (setwise)
- Fixing vertices (pointwise)

Part I

Distinguishing numbers for groups and graphs

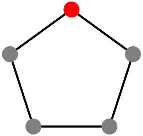
Colourings

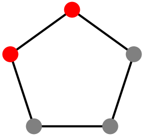
Consider $\Gamma = \mathbf{C}_5$, where we have $\mathrm{Aut}(\Gamma) \cong D_{10}$.

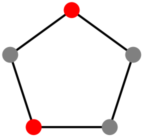
Colourings

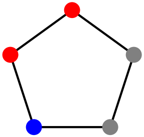
Consider $\Gamma = \mathbf{C}_5$, where we have $\mathrm{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?

$C_1 =$ 

$C_2 =$ 

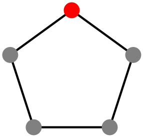
$C_3 =$ 

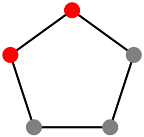
$C_4 =$ 

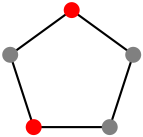
Colourings

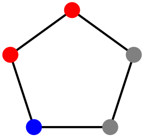
Consider $\Gamma = \mathbf{C}_5$, where we have $\mathrm{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?

$C_1 =$ 

$C_2 =$ 

$C_3 =$ 

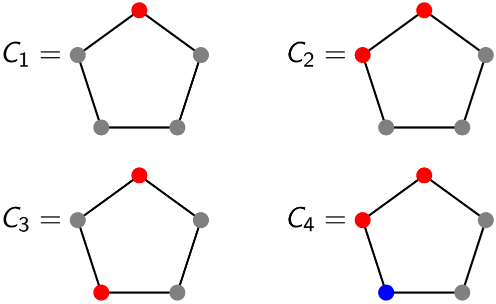
$C_4 =$ 

- $\mathrm{Aut}(\Gamma, C_1) \cong \mathrm{Aut}(\Gamma, C_2) \cong \mathrm{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\mathrm{Aut}(\Gamma, C_4) = 1$.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\mathrm{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



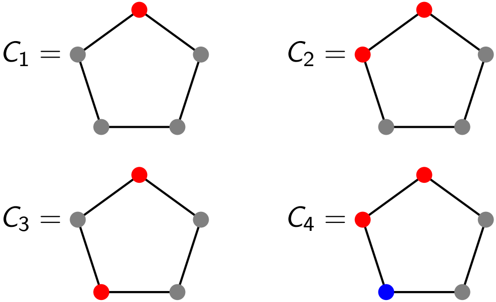
- $\mathrm{Aut}(\Gamma, C_1) \cong \mathrm{Aut}(\Gamma, C_2) \cong \mathrm{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\mathrm{Aut}(\Gamma, C_4) = 1$.

Distinguishing colouring: A colouring C of Γ such that $\mathrm{Aut}(\Gamma, C) = 1$.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\mathrm{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



- $\mathrm{Aut}(\Gamma, C_1) \cong \mathrm{Aut}(\Gamma, C_2) \cong \mathrm{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\mathrm{Aut}(\Gamma, C_4) = 1$.

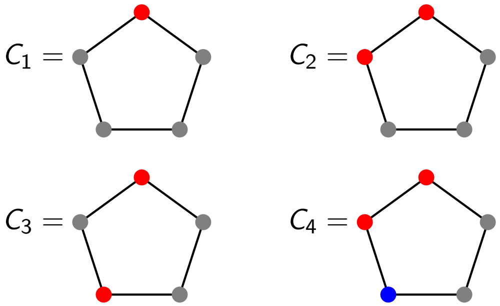
Distinguishing colouring: A colouring C of Γ such that $\mathrm{Aut}(\Gamma, C) = 1$.

Distinguishing number $D(\Gamma)$: The minimal number of colours in a distinguishing colouring of Γ.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



- $\text{Aut}(\Gamma, C_1) \cong \text{Aut}(\Gamma, C_2) \cong \text{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\text{Aut}(\Gamma, C_4) = 1$.

Distinguishing colouring: A colouring C of Γ such that $\text{Aut}(\Gamma, C) = 1$.

Distinguishing number $D(\Gamma)$: The minimal number of colours in a distinguishing colouring of Γ. (e.g. $D(\mathbf{C}_5) = 3$.)

Partitions

Note. A colouring is a partition of vertices.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Remark. $D(\Gamma) = D(\mathrm{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geqslant 6$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Remark. $D(\Gamma) = D(\mathrm{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geqslant 6$.

Examples

- $D(S_n) = n$

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Remark. $D(\Gamma) = D(\mathrm{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geqslant 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Remark. $D(\Gamma) = D(\mathrm{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geqslant 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.
- $D(G) = 1 \iff G = 1$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a **transitive** permutation group of degree n.

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

$$\bigcap_{i=1}^{m} G_{\{\pi_i\}} = 1.$$

Distinguishing number $D(G)$: The minimal size of a dist. partition.

Remark. $D(\Gamma) = D(\mathrm{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geqslant 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.
- $D(G) = 1 \iff G = 1$.
- $G \neq 1$ is regular $\implies D(G) = 2$.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G.

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G.

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$, with 43 exceptions of degree $\leqslant 32$.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G.

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$, with 43 exceptions of degree $\leqslant 32$.

Dolfi, 2000: $D(G) \leqslant 4$ for each exception.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G.

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$, with 43 exceptions of degree $\leqslant 32$.

Dolfi, 2000: $D(G) \leqslant 4$ for each exception.

Theorem (H, 2023+)

Suppose T non-abelian simple, $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T)$, $\Omega = T$ and $3 \leqslant k \leqslant |T| - 3$. Then

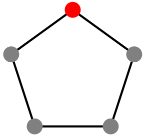
$$\exists\ \Delta \subseteq \Omega \text{ such that } |\Delta| = k \text{ and } G_{\{\Delta\}} = 1.$$

Part II

Bases for permutation groups

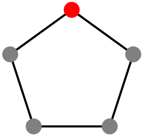
Fixing sets

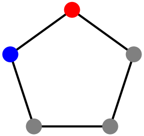
Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



Fixing sets

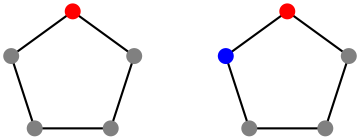
Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?





Fixing sets

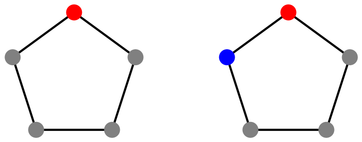
Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?

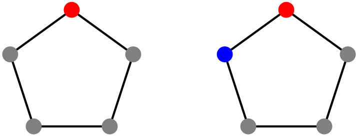


Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number fix(Γ)**:** The minimal size of such a Δ.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



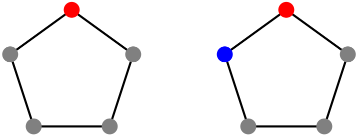
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\mathrm{fix}(\Gamma)$**:** The minimal size of such a Δ.

- $\Gamma = \mathbf{K}_n \implies \mathrm{fix}(\Gamma) = n - 1$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



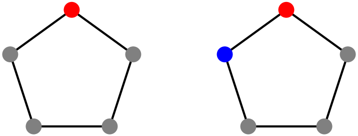
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha\in\Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\mathrm{fix}(\Gamma)$**:** The minimal size of such a Δ.

- $\Gamma = \mathbf{K}_n \implies \mathrm{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \mathrm{fix}(\Gamma) = 2$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



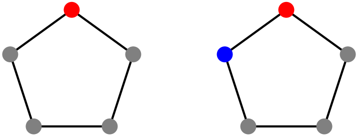
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\mathrm{fix}(\Gamma)$**:** The minimal size of such a Δ.

- $\Gamma = \mathbf{K}_n \implies \mathrm{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \mathrm{fix}(\Gamma) = 2$.
- $\mathrm{Aut}(\Gamma) = 1 \iff \mathrm{fix}(\Gamma) = 0$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we "pin" each coloured vertex?



Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\mathrm{fix}(\Gamma)$**:** The minimal size of such a Δ.

- $\Gamma = \mathbf{K}_n \implies \mathrm{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \mathrm{fix}(\Gamma) = 2$.
- $\mathrm{Aut}(\Gamma) = 1 \iff \mathrm{fix}(\Gamma) = 0$.
- $D(\Gamma) \leqslant \mathrm{fix}(\Gamma) + 1$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.
- $G = D_{2n}$ $(n \geqslant 3)$, $\Omega = \{1, \ldots, n\} \implies b(G) = 2$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.
- $G = D_{2n}$ $(n \geqslant 3)$, $\Omega = \{1, \ldots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.
- $G = D_{2n}$ $(n \geqslant 3)$, $\Omega = \{1, \ldots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leqslant b(G) + 1$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.
- $G = D_{2n}$ $(n \geqslant 3)$, $\Omega = \{1, \ldots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leqslant b(G) + 1$.
- $G = \mathrm{GL}_d(q)$, $\Omega = \mathbb{F}_q^d \setminus \{0\} \implies b(G) = d$.

Bases

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

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G.

Remark. $\mathrm{fix}(\Gamma) = b(\mathrm{Aut}(\Gamma))$.

- $G = S_n$, $\Omega = \{1, \ldots, n\} \implies b(G) = n - 1$.
- $G = D_{2n}$ $(n \geqslant 3)$, $\Omega = \{1, \ldots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leqslant b(G) + 1$.
- $G = \mathrm{GL}_d(q)$, $\Omega = \mathbb{F}_q^d \setminus \{0\} \implies b(G) = d$.

  Klavžar, Wong & Zhu, 2006: $D(G) = 2$ if $\mathbb{F}_q^d \neq \mathbb{F}_2^2, \mathbb{F}_2^3, \mathbb{F}_4^2$ or $\mathbb{F}_3^2$.

Base sizes

Observation: If Δ is a base and $x, y \in G$,

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)}$$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ.

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ.

- $|G| \leqslant |\Omega|^{b(G)}$, so $\log_{|\Omega|} |G| \leqslant b(G)$.

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ.

- $|G| \leqslant |\Omega|^{b(G)}$, so $\log_{|\Omega|} |G| \leqslant b(G)$.
- A small base Δ provides an efficient way to store the elements of G, using $|\Delta|$-tuples rather than $|\Omega|$-tuples.

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ.

- $|G| \leqslant |\Omega|^{b(G)}$, so $\log_{|\Omega|} |G| \leqslant b(G)$.
- A small base Δ provides an efficient way to store the elements of G, using $|\Delta|$-tuples rather than $|\Omega|$-tuples.

Observation: If $\Delta = \{\alpha_1, \ldots, \alpha_{b(G)}\}$ is a base and $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$ then

$$G > G^{(1)} > G^{(2)} > \cdots > G^{(b(G)-1)} > G^{(b(G))} = 1.$$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ.

- $|G| \leqslant |\Omega|^{b(G)}$, so $\log_{|\Omega|} |G| \leqslant b(G)$.
- A small base Δ provides an efficient way to store the elements of G, using $|\Delta|$-tuples rather than $|\Omega|$-tuples.

Observation: If $\Delta = \{\alpha_1, \ldots, \alpha_{b(G)}\}$ is a base and $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$ then

$$G > G^{(1)} > G^{(2)} > \cdots > G^{(b(G)-1)} > G^{(b(G))} = 1.$$

Thus, $2^{b(G)} \leqslant |G|$ and so $\log_{|\Omega|} |G| \leqslant b(G) \leqslant \log_2 |G|$.

Some general bounds

Let G be primitive with degree n.

Questions: Better bounds on $b(G)$? Or even determine $b(G)$?

Some general bounds

Let G be primitive with degree n.

Questions: Better bounds on $b(G)$? Or even determine $b(G)$?

Conjecture (Pyber, 1993)

There is an absolute constant c such that $\log_n |G| \leqslant b(G) \leqslant c \log_n |G|$.

Some general bounds

Let G be primitive with degree n.

Questions: Better bounds on $b(G)$? Or even determine $b(G)$?

Conjecture (Pyber, 1993)

There is an absolute constant c such that $\log_n |G| \leqslant b(G) \leqslant c \log_n |G|$.

Duyan, Halasi & Maróti, 2018: Pyber's conjecture is true.

Some general bounds

Let G be primitive with degree n.

Questions: Better bounds on $b(G)$? Or even determine $b(G)$?

Conjecture (Pyber, 1993)

There is an absolute constant c such that $\log_n |G| \leqslant b(G) \leqslant c \log_n |G|$.

Duyan, Halasi & Maróti, 2018: Pyber's conjecture is true.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2 \log_n |G| + 24$.

Some general bounds

Let G be primitive with degree n.

Questions: Better bounds on $b(G)$? Or even determine $b(G)$?

Conjecture (Pyber, 1993)

There is an absolute constant c such that $\log_n |G| \leqslant b(G) \leqslant c \log_n |G|$.

Duyan, Halasi & Maróti, 2018: Pyber's conjecture is true.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2 \log_n |G| + 24$.

Soluble groups:

- **Seress, 1996:** G soluble $\implies b(G) \leqslant 4$
- **Burness, 2021:** G_α soluble $\implies b(G) \leqslant 5$

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

- **Fawcett, 2022:** $b(G) = 2$ if P is quasiprimitive.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

- **Fawcett, 2022:** $b(G) = 2$ if P is quasiprimitive.

Product type: $G \leqslant L \wr P$ in its product action, $L \leqslant \mathrm{Sym}(\Gamma)$ primitive.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

- **Fawcett, 2022:** $b(G) = 2$ if P is quasiprimitive.

Product type: $G \leqslant L \wr P$ in its product action, $L \leqslant \mathrm{Sym}(\Gamma)$ primitive.

- **Bailey & Cameron, 2011:** The case where $G = L \wr P$.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

- **Fawcett, 2022:** $b(G) = 2$ if P is quasiprimitive.

Product type: $G \leqslant L \wr P$ in its product action, $L \leqslant \mathrm{Sym}(\Gamma)$ primitive.

- **Bailey & Cameron, 2011:** The case where $G = L \wr P$.

  e.g. $b(L \wr P) = 2 \iff L_\gamma$ has at least $D(P)$ regular orbits on Γ.

O'Nan-Scott families

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

- **Halasi & Podoski, 2016:** $b(G) \leqslant 3$ if $(|V|, |H|) = 1$.
- $H/Z(H)$ quasisimple: partial results.

Twisted wreath: $G = T^k{:}P$, $P \leqslant S_k$ transitive.

- **Fawcett, 2022:** $b(G) = 2$ if P is quasiprimitive.

Product type: $G \leqslant L \wr P$ in its product action, $L \leqslant \mathrm{Sym}(\Gamma)$ primitive.

- **Bailey & Cameron, 2011:** The case where $G = L \wr P$.

  e.g. $b(L \wr P) = 2 \iff L_\gamma$ has at least $D(P)$ regular orbits on Γ.
- **Burness & H, 2023:** partial results on $G < L \wr P$.

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓
- G_α is intransitive: partial results **(Halasi, 2012)**

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓
- G_α is intransitive: partial results **(Halasi, 2012)**

Sporadic socle: Done ✓ **(Burness, O'Brien & Wilson, 2010)**

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓
- G_α is intransitive: partial results **(Halasi, 2012)**

Sporadic socle: Done ✓ **(Burness, O'Brien & Wilson, 2010)**

$\mathrm{soc}(G)$ **is Lie type:**

- **Burness, Guralnick & Saxl, 2014:** G classical and $G_\alpha \in \mathcal{S}$ ✓

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓
- G_α is intransitive: partial results **(Halasi, 2012)**

Sporadic socle: Done ✓ **(Burness, O'Brien & Wilson, 2010)**

$\mathrm{soc}(G)$ **is Lie type:**

- **Burness, Guralnick & Saxl, 2014:** G classical and $G_\alpha \in \mathcal{S}$ ✓
- **Burness, Liebeck & Shalev, 2007:** $b(G) \leqslant 6$ if G is exceptional

Almost simple groups

Alternating socle A_m:

- **Burness, Guralnick & Saxl, 2011:** G_α is primitive on $[m]$ ✓
- **Morris & Spiga, 2021:** G_α is imprimitive on $[m]$ ✓
- G_α is intransitive: partial results **(Halasi, 2012)**

Sporadic socle: Done ✓ **(Burness, O'Brien & Wilson, 2010)**

$\mathrm{soc}(G)$ **is Lie type:**

- **Burness, Guralnick & Saxl, 2014:** G classical and $G_\alpha \in \mathcal{S}$ ✓
- **Burness, Liebeck & Shalev, 2007:** $b(G) \leqslant 6$ if G is exceptional
- **Burness & Thomas, 2023:** $b(G) = 2$ if G is exceptional and G_α is the normaliser of a maximal torus ✓

Part III

Base sizes of diagonal type primitive groups

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \ldots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \dots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type group: G with $T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k)$.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \dots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type group: G with $T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k)$.

Note. $N_{\mathrm{Sym}(\Omega)}(T^k) = T^k.(\mathrm{Out}(T) \times S_k)$ is a maximal subgroup of $\mathrm{Sym}(\Omega)$.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \ldots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type group: G with $T^k \trianglelefteq G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k)$.

Note. $N_{\mathrm{Sym}(\Omega)}(T^k) = T^k.(\mathrm{Out}(T) \times S_k)$ is a maximal subgroup of $\mathrm{Sym}(\Omega)$.

- G induces a subgroup P of S_k on the k components.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \ldots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type group: G with $T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k)$.

Note. $N_{\mathrm{Sym}(\Omega)}(T^k) = T^k.(\mathrm{Out}(T) \times S_k)$ is a maximal subgroup of $\mathrm{Sym}(\Omega)$.

- G induces a subgroup P of S_k on the k components.
- G is primitive $\iff$ P is primitive, or $k = 2$ and $P = 1$.

Diagonal type primitive groups

Let T be a non-abelian finite simple group.

Write $\Omega = [T^k : D]$, where $D = \{(t, \ldots, t) : t \in T\}$, so $T^k \leqslant \mathrm{Sym}(\Omega)$.

Diagonal type group: G with $T^k \trianglelefteq G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k)$.

Note. $N_{\mathrm{Sym}(\Omega)}(T^k) = T^k.(\mathrm{Out}(T) \times S_k)$ is a maximal subgroup of $\mathrm{Sym}(\Omega)$.

- G induces a subgroup P of S_k on the k components.
- G is primitive $\iff$ P is primitive, or $k = 2$ and $P = 1$.

Thus, $T^k \trianglelefteq G \leqslant T^k.(\mathrm{Out}(T) \times P)$.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \dots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \dots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \;\; t_i = x \text{ if } i \in \Delta_2, \;\; t_i = y \text{ if } i \in \Delta_3.$$

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \ldots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \;\; t_i = x \text{ if } i \in \Delta_2, \;\; t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \ldots, a)\pi \in G_\alpha \cap G_\beta$.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \ldots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \;\; t_i = x \text{ if } i \in \Delta_2, \;\; t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \ldots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \dots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \;\; t_i = x \text{ if } i \in \Delta_2, \;\; t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$ and so $g = 1$.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \ldots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1,\ \ t_i = x \text{ if } i \in \Delta_2,\ \ t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \ldots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$ and so $g = 1$.

Fawcett, 2013: $P \neq A_k, S_k \implies b(G) = 2$.

A construction

Set $\alpha = D$ and suppose $G = T^k.(\mathrm{Out}(T) \times P)$. Then

$$G_\alpha = \{(a, \dots, a)\pi : a \in \mathrm{Aut}(T), \pi \in P\} \cong \mathrm{Aut}(T) \times P.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1,\ \ t_i = x \text{ if } i \in \Delta_2,\ \ t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$ and so $g = 1$.

Fawcett, 2013: $P \neq A_k, S_k \implies b(G) = 2$.

Remark. This method is not useful for $P \in \{A_k, S_k\}$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\,\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Let $\Delta = \{t_1, \ldots, t_k\}$ be such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Let $\Delta = \{t_1, \ldots, t_k\}$ be such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Let $\alpha = D$ and $\beta = D(t_1, \ldots, t_k)$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Let $\Delta = \{t_1, \dots, t_k\}$ be such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Let $\alpha = D$ and $\beta = D(t_1, \dots, t_k)$.

Note. If $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$, then $t_{i^\pi} = xt_i^a$ for some $x \in T$, so $x^{-1}a \in X_{\{\Delta\}}$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\ \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Let $\Delta = \{t_1, \dots, t_k\}$ be such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Let $\alpha = D$ and $\beta = D(t_1, \dots, t_k)$.

Note. If $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$, then $t_{i^\pi} = x t_i^a$ for some $x \in T$, so $x^{-1}a \in X_{\{\Delta\}}$. Thus, $a = 1$ and $x = 1$, which implies $\pi = 1$ as $t_1, \dots, t_k$ are distinct. Hence $g = 1$.

Holomorph

Let $X = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) \leqslant \mathrm{Sym}(T)$. Recall that

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$, then $\exists\, \Delta \subseteq T$ such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Assume $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$.

Let $\Delta = \{t_1, \ldots, t_k\}$ be such that $|\Delta| = k$ and $X_{\{\Delta\}} = 1$.

Let $\alpha = D$ and $\beta = D(t_1, \ldots, t_k)$.

Note. If $g = (a, \ldots, a)\pi \in G_\alpha \cap G_\beta$, then $t_{i^\pi} = x t_i^a$ for some $x \in T$, so $x^{-1}a \in X_{\{\Delta\}}$. Thus, $a = 1$ and $x = 1$, which implies $\pi = 1$ as $t_1, \ldots, t_k$ are distinct. Hence $g = 1$.

Theorem (H, 2023+)

If $3 \leqslant k \leqslant |T| - 3$ and $G = T^k.(\mathrm{Out}(T) \times S_k)$, then $b(G) = 2$.

Base sizes

Theorem (H, 2023+)

Suppose $G \leqslant T^k.(\mathrm{Out}(T) \times P)$ is a diagonal type primitive group of top group P. Then $b(G) = 2$ iff one of the following holds:

- $P \notin \{A_k, S_k\}$;
- $3 \leqslant k \leqslant |T| - 3$;
- $k \in \{|T| - 2, |T| - 1\}$ and $S_k \nleqslant G$.

Base sizes

Theorem (H, 2023+)

Suppose $G \leqslant T^k.(\mathrm{Out}(T) \times P)$ is a diagonal type primitive group of top group P. Then $b(G) = 2$ iff one of the following holds:

- $P \notin \{A_k, S_k\}$;
- $3 \leqslant k \leqslant |T| - 3$;
- $k \in \{|T| - 2, |T| - 1\}$ and $S_k \nleqslant G$.

Theorem (H, 2023+)

Suppose G is a diagonal type primitive group. Then $b(G)$ is known. ✓

Part IV

Connections and related problems

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Recall. Apart from 43 exceptions, $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Recall. Apart from 43 exceptions, $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Note. If $k < b(G)$ and $|\Delta| = k$, then $G_{\{\Delta\}} \geqslant G_{(\Delta)} > 1$.

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Recall. Apart from 43 exceptions, $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Note. If $k < b(G)$ and $|\Delta| = k$, then $G_{\{\Delta\}} \geqslant G_{(\Delta)} > 1$.

Define the following property:

$$\forall\ b(G) \leqslant k \leqslant |\Omega| - b(G),\ \exists\ \Delta \subseteq \Omega \text{ s.t. } |\Delta| = k \text{ and } G_{\{\Delta\}} = 1. \qquad (\star)$$

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Recall. Apart from 43 exceptions, $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Note. If $k < b(G)$ and $|\Delta| = k$, then $G_{\{\Delta\}} \geqslant G_{(\Delta)} > 1$.

Define the following property:

$$\forall\ b(G) \leqslant k \leqslant |\Omega| - b(G),\ \exists\ \Delta \subseteq \Omega \text{ s.t. } |\Delta| = k \text{ and } G_{\{\Delta\}} = 1. \qquad (\star)$$

Problem. Classify the finite primitive groups with property $(\star)$.

Subsets with trivial stabiliser

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group. Assume $G \notin \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$.

Recall. Apart from 43 exceptions, $\exists\ \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Note. If $k < b(G)$ and $|\Delta| = k$, then $G_{\{\Delta\}} \geqslant G_{(\Delta)} > 1$.

Define the following property:

$$\forall\ b(G) \leqslant k \leqslant |\Omega| - b(G),\ \exists\ \Delta \subseteq \Omega \text{ s.t. } |\Delta| = k \text{ and } G_{\{\Delta\}} = 1. \qquad (\star)$$

Problem. Classify the finite primitive groups with property $(\star)$.

Theorem (H, 2023+)

If G is **holomorph simple**, then G has the property $(\star)$.

Automorphisms

Let G be a non-abelian finite group. For $S \subseteq G \setminus \{1\}$, let

$$\mathrm{Aut}(G,S) = \{g \in \mathrm{Aut}(G) : S^g = S\}$$

Automorphisms

Let G be a non-abelian finite group. For $S \subseteq G \setminus \{1\}$, let

$$\mathrm{Aut}(G,S) = \{g \in \mathrm{Aut}(G) : S^g = S\}$$

and define the property

$$\forall\ 2 \leqslant k \leqslant |G| - 3,\ \exists\ S \subseteq G \setminus \{1\} \text{ s.t. } |S| = k \text{ and } \mathrm{Aut}(G,S) = 1. \quad (\star\star)$$

Automorphisms

Let G be a non-abelian finite group. For $S \subseteq G \setminus \{1\}$, let

$$\mathrm{Aut}(G,S) = \{g \in \mathrm{Aut}(G) : S^g = S\}$$

and define the property

$$\forall\ 2 \leqslant k \leqslant |G| - 3,\ \exists\ S \subseteq G \setminus \{1\} \text{ s.t. } |S| = k \text{ and } \mathrm{Aut}(G,S) = 1. \quad (\star\star)$$

Note. If $|S| = 1$ or $|G| - 2$, then $\mathrm{Aut}(G,S) \neq 1$.

Automorphisms

Let G be a non-abelian finite group. For $S \subseteq G \setminus \{1\}$, let

$$\mathrm{Aut}(G,S) = \{g \in \mathrm{Aut}(G) : S^g = S\}$$

and define the property

$$\forall\ 2 \leqslant k \leqslant |G|-3,\ \exists\ S \subseteq G \setminus \{1\} \text{ s.t. } |S| = k \text{ and } \mathrm{Aut}(G,S) = 1. \quad (\star\star)$$

Note. If $|S| = 1$ or $|G|-2$, then $\mathrm{Aut}(G,S) \neq 1$.

Problem. Classify the non-abelian finite groups G with the property $(\star\star)$.

Automorphisms

Let G be a non-abelian finite group. For $S \subseteq G \setminus \{1\}$, let

$$\mathrm{Aut}(G, S) = \{g \in \mathrm{Aut}(G) : S^g = S\}$$

and define the property

$$\forall\ 2 \leqslant k \leqslant |G| - 3,\ \exists\ S \subseteq G \setminus \{1\} \text{ s.t. } |S| = k \text{ and } \mathrm{Aut}(G, S) = 1. \quad (\star\star)$$

Note. If $|S| = 1$ or $|G| - 2$, then $\mathrm{Aut}(G, S) \neq 1$.

Problem. Classify the non-abelian finite groups G with the property $(\star\star)$.

Theorem (H, 2023+)

If G is simple, then G has the property $(\star\star)$.

Asymptotic results

Let T be a non-abelian finite simple group and define

$$\mathbb{P}_k(T) := \frac{|\{S \subseteq T \setminus \{1\} : |S| = k,\ \mathrm{Aut}(T,S) \neq 1\}|}{\binom{|T|-1}{k}}$$

be the probability that a random k-subset of $T \setminus \{1\}$ has non-trivial setwise stabiliser in $\mathrm{Aut}(T)$.

Asymptotic results

Let T be a non-abelian finite simple group and define

$$\mathbb{P}_k(T) := \frac{|\{S \subseteq T \setminus \{1\} : |S| = k,\ \mathrm{Aut}(T,S) \neq 1\}|}{\binom{|T|-1}{k}}$$

be the probability that a random k-subset of $T \setminus \{1\}$ has non-trivial setwise stabiliser in $\mathrm{Aut}(T)$.

Recall. $\mathbb{P}_k(T) < 1$ if $2 \leqslant k \leqslant |T| - 3$.

Asymptotic results

Let T be a non-abelian finite simple group and define

$$\mathbb{P}_k(T) := \frac{|\{S \subseteq T \setminus \{1\} : |S| = k,\ \mathrm{Aut}(T,S) \neq 1\}|}{\binom{|T|-1}{k}}$$

be the probability that a random k-subset of $T \setminus \{1\}$ has non-trivial setwise stabiliser in $\mathrm{Aut}(T)$.

Recall. $\mathbb{P}_k(T) < 1$ if $2 \leqslant k \leqslant |T| - 3$.

Theorem (H, 2023+)

If $k \geqslant 4$, then $\mathbb{P}_k(T) \to 0$ as $|T| \to \infty$.

Asymptotic results

Let T be a non-abelian finite simple group and define

$$\mathbb{P}_k(T) := \frac{|\{S \subseteq T \setminus \{1\} : |S| = k,\ \mathrm{Aut}(T,S) \neq 1\}|}{\binom{|T|-1}{k}}$$

be the probability that a random k-subset of $T \setminus \{1\}$ has non-trivial setwise stabiliser in $\mathrm{Aut}(T)$.

Recall. $\mathbb{P}_k(T) < 1$ if $2 \leqslant k \leqslant |T| - 3$.

Theorem (H, 2023+)

If $k \geqslant 4$, then $\mathbb{P}_k(T) \to 0$ as $|T| \to \infty$.

Theorem (H, 2023+)

If $5 \log |T| < k < |T| - 5 \log |T|$, then $\mathbb{P}_k(T) < 1/|T|$.

Asymptotic results

Let T be a non-abelian finite simple group and define

$$\mathbb{P}_k(T) := \frac{|\{S \subseteq T \setminus \{1\} : |S| = k,\ \mathrm{Aut}(T,S) \neq 1\}|}{\binom{|T|-1}{k}}$$

be the probability that a random k-subset of $T \setminus \{1\}$ has non-trivial setwise stabiliser in $\mathrm{Aut}(T)$.

Recall. $\mathbb{P}_k(T) < 1$ if $2 \leqslant k \leqslant |T| - 3$.

Theorem (H, 2023+)

If $k \geqslant 4$, then $\mathbb{P}_k(T) \to 0$ as $|T| \to \infty$.

Theorem (H, 2023+)

If $5 \log |T| < k < |T| - 5 \log |T|$, then $\mathbb{P}_k(T) < 1/|T|$.

An application: existence of DRR with prescribed valency. (Pablo Spiga)

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Chen & H, 2022: General method in computing $r(G)$.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Chen & H, 2022: General method in computing $r(G)$.

Problem. Classify the finite primitive groups G with $r(G) = 1$.

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Chen & H, 2022: General method in computing $r(G)$.

Problem. Classify the finite primitive groups G with $r(G) = 1$.

- **H, 2023+:** G diagonal type ✓

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Chen & H, 2022: General method in computing $r(G)$.

Problem. Classify the finite primitive groups G with $r(G) = 1$.

- **H, 2023+:** G diagonal type ✓
- **Burness & H, 2022:** G almost simple, G_α soluble ✓

Bases and regular suborbits

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Remark. Other than diagonal type groups, this still remains very open.

Note. $b(G) \leqslant 2 \iff G_\alpha$ has a regular orbit on Ω.

Let $r(G)$ be the number of regular G_α-orbits on Ω.

Chen & H, 2022: General method in computing $r(G)$.

Problem. Classify the finite primitive groups G with $r(G) = 1$.

- **H, 2023+:** G diagonal type ✓
- **Burness & H, 2022:** G almost simple, G_α soluble ✓
- **Burness & H, 2023:** Some product type groups.

Thank you!