Permutation groups, transitive subgroups and bases

Hongyi Huang

Pure Maths Colloquium, University of St Andrews

17 April 2025

University of St Andrews

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Point stabiliser: $G_\alpha = \{g \in G : \alpha^g = \alpha\}$.

Orbit: $\alpha^G = \{\alpha^g : g \in G\}$.

Recall (Orbit-Stabiliser Theorem)**.** $|G| = |G_\alpha| \cdot |\alpha^G|$.

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Point stabiliser: $G_\alpha = \{g \in G : \alpha^g = \alpha\}$.

Orbit: $\alpha^G = \{\alpha^g : g \in G\}$.

Recall (Orbit-Stabiliser Theorem)**.** $|G| = |G_\alpha| \cdot |\alpha^G|$.

G is called **transitive** if $\alpha^G = \Omega$ (so $|G| = |G_\alpha| \cdot |\Omega|$).

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Point stabiliser: $G_\alpha = \{g \in G : \alpha^g = \alpha\}$.

Orbit: $\alpha^G = \{\alpha^g : g \in G\}$.

Recall (Orbit-Stabiliser Theorem)**.** $|G| = |G_\alpha| \cdot |\alpha^G|$.

G is called **transitive** if $\alpha^G = \Omega$ (so $|G| = |G_\alpha| \cdot |\Omega|$).

In this setting, Ω can be identified with the cosets G/H, where $H = G_\alpha$, with $(Hx)^g = Hxg$ for any $x, g \in G$.

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Point stabiliser: $G_\alpha = \{g \in G : \alpha^g = \alpha\}$.

Orbit: $\alpha^G = \{\alpha^g : g \in G\}$.

Recall (Orbit-Stabiliser Theorem)**.** $|G| = |G_\alpha| \cdot |\alpha^G|$.

G is called **transitive** if $\alpha^G = \Omega$ (so $|G| = |G_\alpha| \cdot |\Omega|$).

In this setting, Ω can be identified with the cosets G/H, where $H = G_\alpha$, with $(Hx)^g = Hxg$ for any $x, g \in G$.

Conversely, if $H < G$ is core-free, then $G \leqslant \mathrm{Sym}(G/H)$ is transitive.

Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$, and let $\alpha \in \Omega$.

Point stabiliser: $G_\alpha = \{g \in G : \alpha^g = \alpha\}$.

Orbit: $\alpha^G = \{\alpha^g : g \in G\}$.

Recall (Orbit-Stabiliser Theorem)**.** $|G| = |G_\alpha| \cdot |\alpha^G|$.

G is called **transitive** if $\alpha^G = \Omega$ (so $|G| = |G_\alpha| \cdot |\Omega|$).

In this setting, Ω can be identified with the cosets G/H, where $H = G_\alpha$, with $(Hx)^g = Hxg$ for any $x, g \in G$.

Conversely, if $H < G$ is core-free, then $G \leqslant \mathrm{Sym}(G/H)$ is transitive.

Example

Take $H = 1$. Then $G \leqslant \mathrm{Sym}(G)$ is given by right multiplication.

In particular, every (abstract) group is isomorphic to a transitive permutation group.

Primitive groups

G is called **primitive** if G is transitive and G_α is a maximal subgroup of G.

Remark. These are the basic building blocks of all permutation groups.

Primitive groups

G is called **primitive** if G is transitive and G_α is a maximal subgroup of G.

Remark. These are the basic building blocks of all permutation groups.

Note. NOT every (abstract) group is isomorphic to a primitive permutation group (e.g. a cyclic group of order 4, an abelian group of composite order).

Primitive groups

G is called **primitive** if G is transitive and G_α is a maximal subgroup of G.

Remark. These are the basic building blocks of all permutation groups.

Note. NOT every (abstract) group is isomorphic to a primitive permutation group (e.g. a cyclic group of order 4, an abelian group of composite order).

The **O'Nan-Scott theorem** divides finite primitive groups into 5 types, in terms of their structures and actions.

- Affine
- Almost simple
- Diagonal type
- Product type
- Twisted wreath product

Part I. Transitive subgroups of primitive groups

Part II. Bases for primitive groups

Group factorisations

Let G be a finite group and $H, K \leqslant G$. Write $HK = \{hk : h \in H, k \in K\}$.

Group factorisations

Let G be a finite group and $H, K \leqslant G$. Write $HK = \{hk : h \in H, k \in K\}$.

Fact. $G = HK \iff K$ is transitive on G/H.

The expression $G = HK$ is called a **factorisation** of G.

Group factorisations

Let G be a finite group and $H, K \leqslant G$. Write $HK = \{hk : h \in H, k \in K\}$.

Fact. $G = HK \iff K$ is transitive on G/H.

The expression $G = HK$ is called a **factorisation** of G.

Example

$G = S_n$, $H = S_{n-1}$ and K is a transitive group on $[n]$.

Group factorisations

Let G be a finite group and $H, K \leqslant G$. Write $HK = \{hk : h \in H, k \in K\}$.

Fact. $G = HK \iff K$ is transitive on G/H.

The expression $G = HK$ is called a **factorisation** of G.

Example

$G = S_n$, $H = S_{n-1}$ and K is a transitive group on $[n]$.

Example

$q = p^f$, $G = \mathrm{PGL}_2(q)$, $H = C_p^f{:}C_{q-1}$ is the stabiliser of a 1-space of $\mathbb{F}_q^2$.
The group $K = C_{q+1}$ is transitive on 1-spaces, so we have $G = HK$.

Group factorisations

Let G be a finite group and $H, K \leqslant G$. Write $HK = \{hk : h \in H, k \in K\}$.

Fact. $G = HK \iff K$ is transitive on G/H.

The expression $G = HK$ is called a **factorisation** of G.

Example

$G = S_n$, $H = S_{n-1}$ and K is a transitive group on $[n]$.

Example

$q = p^f$, $G = \mathrm{PGL}_2(q)$, $H = C_p^f{:}C_{q-1}$ is the stabiliser of a 1-space of $\mathbb{F}_q^2$.
The group $K = C_{q+1}$ is transitive on 1-spaces, so we have $G = HK$.

Example

The group $\mathrm{PGL}_2(q)$ is transitive on the triples of distinct 1-spaces of $\mathbb{F}_q^2$, so we have the factorisation $S_{q+1} = S_{q-2}\,\mathrm{PGL}_2(q)$.

Almost simple groups

G is called **almost simple** if $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T, and $T = \mathrm{soc}(G)$ is the **socle** of G.

Almost simple groups

G is called **almost simple** if $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T, and $T = \mathrm{soc}(G)$ is the **socle** of G.

Examples. A_n, S_n, $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$, $\mathbb{M}$....

Almost simple groups

G is called **almost simple** if $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T, and $T = \mathrm{soc}(G)$ is the **socle** of G.

Examples. A_n, S_n, $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$, $\mathbb{M}$....

Contributed by Li, Liebeck, Praeger, Saxl, Wang, Xia...

Theorem. The factorisations of almost simple groups are classified.

Final step: **Feng, Li, Li, Wang, Xia & Zou, 2024**.

Almost simple groups

G is called **almost simple** if $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T, and $T = \mathrm{soc}(G)$ is the **socle** of G.

Examples. A_n, S_n, $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$, $\mathbb{M}$....

Contributed by Li, Liebeck, Praeger, Saxl, Wang, Xia...

Theorem. The factorisations of almost simple groups are classified.

Final step: **Feng, Li, Li, Wang, Xia & Zou, 2024**.

Corollary. The transitive subgroups of almost simple primitive groups are determined, up to conjugacy.

Primitive groups

Main theme. Determine the transitive subgroups of primitive groups.

Recall the O'Nan-Scott theorem:

- Affine
- Almost simple
- Diagonal type
- Product type
- Twisted wreath products

Primitive groups

Main theme. Determine the transitive subgroups of primitive groups.

Recall the O'Nan-Scott theorem:

- Affine
- Almost simple ✓
- Diagonal type
- Product type
- Twisted wreath products

Problem. Classify the **regular** subgroups and the **soluble** transitive subgroups of primitive groups of **diagonal type**, up to conjugacy.

Remark. A transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is called **regular** if $|G| = |\Omega|$.

The holomorphs of simple groups

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

$$G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$$

be the **holomorph** of T. Then $G \leqslant \mathrm{Sym}(T)$ is primitive of diagonal type.

The holomorphs of simple groups

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

$$G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$$

be the **holomorph** of T. Then $G \leqslant \mathrm{Sym}(T)$ is primitive of diagonal type.

Notes.

- $G_1 = \mathrm{Aut}(T)$.

The holomorphs of simple groups

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

$$G = \mathrm{Hol}(T) = T{:}\,\mathrm{Aut}(T) = T^2.\,\mathrm{Out}(T)$$

be the **holomorph** of T. Then $G \leqslant \mathrm{Sym}(T)$ is primitive of diagonal type.

Notes.

- $G_1 = \mathrm{Aut}(T)$.
- G has 2 regular normal subgroups isomorphic to T.

The holomorphs of simple groups

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

$$G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$$

be the **holomorph** of T. Then $G \leqslant \mathrm{Sym}(T)$ is primitive of diagonal type.

Notes.

- $G_1 = \mathrm{Aut}(T)$.
- G has 2 regular normal subgroups isomorphic to T.

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteqslant HK = HT = KT \leqslant \mathrm{Aut}(T).$$

The holomorphs of simple groups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

The holomorphs of simple groups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Example

$B \cong T$ is regular normal: $H = T$ and $K = 1$.

The holomorphs of simple groups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Example

$B \cong T$ is regular normal: $H = T$ and $K = 1$.

Example

q odd, $T = A_{q+1}$, $B \cong (A_{q-2} \times \mathrm{PSL}_2(q)).2$:

$H = S_{q-2}$, $K = \mathrm{PGL}_2(q)$, w.r.t. the factorisation $S_{q+1} = S_{q-2}\,\mathrm{PGL}_2(q)$.

The holomorphs of simple groups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Example

$B \cong T$ is regular normal: $H = T$ and $K = 1$.

Example

q odd, $T = A_{q+1}$, $B \cong (A_{q-2} \times \mathrm{PSL}_2(q)).2$:

$H = S_{q-2}$, $K = \mathrm{PGL}_2(q)$, w.r.t. the factorisation $S_{q+1} = S_{q-2}\,\mathrm{PGL}_2(q)$.

If $T = HK$, then $\exists$ a transitive subgroup of G isomorphic to $H \times K$.

Soluble transitive subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Soluble transitive subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Note. If B is soluble, then both H and K are soluble.

Soluble transitive subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteqslant HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Note. If B is soluble, then both H and K are soluble.

Li & Xia, 2022: Apart from finitely many cases, we have $T = \mathrm{PSL}_2(q)$.

Soluble transitive subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Note. If B is soluble, then both H and K are soluble.

Li & Xia, 2022: Apart from finitely many cases, we have $T = \mathrm{PSL}_2(q)$.

e.g. $q = p^f$, $T = \mathrm{PSL}_2(q)$, $H = C_p^f{:}C_{q-1}$, $K = C_{q+1}$, $HK = \mathrm{PGL}_2(q)$.

Soluble transitive subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteqslant HK = HT = KT \leqslant \mathrm{Aut}(T).$$

Note. If B is soluble, then both H and K are soluble.

Li & Xia, 2022: Apart from finitely many cases, we have $T = \mathrm{PSL}_2(q)$.

e.g. $q = p^f$, $T = \mathrm{PSL}_2(q)$, $H = C_p^f{:}C_{q-1}$, $K = C_{q+1}$, $HK = \mathrm{PGL}_2(q)$.

With more technical treatment...

Theorem (H & Wang, 2025+)

For every finite simple group T, the **soluble transitive** subgroups of $\mathrm{Hol}(T)$ are determined, up to conjugacy.

Regular subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T). \qquad (\star)$$

Regular subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T). \qquad (\star)$$

If B is regular, then there exists $N \trianglelefteq H$ and $M \trianglelefteq K$ such that

$$H/N \cong K/M \text{ and } |H:N| = |HK:T||H \cap K|. \qquad (\star\star)$$

Regular subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T). \qquad (\star)$$

If B is regular, then there exists $N \trianglelefteq H$ and $M \trianglelefteq K$ such that

$$H/N \cong K/M \text{ and } |H : N| = |HK : T||H \cap K|. \qquad (\star\star)$$

Much effort is needed to determine the factorisations satisfying $(\star)$ and $(\star\star)$.

Regular subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T). \qquad (\star)$$

If B is regular, then there exists $N \trianglelefteq H$ and $M \trianglelefteq K$ such that

$$H/N \cong K/M \text{ and } |H : N| = |HK : T||H \cap K|. \qquad (\star\star)$$

Much effort is needed to determine the factorisations satisfying $(\star)$ and $(\star\star)$.

Example

Assume $HK = S_n$ with $H = S_{n-1}$ (so K is transitive on $[n]$).

Regular subgroups

Key observation (Liebeck, Praeger & Saxl, 2000).

If B is a transitive subgroup of G, then there exist $H, K \leqslant \mathrm{Aut}(T)$ isomorphic to some quotient groups of B such that

$$T \trianglelefteq HK = HT = KT \leqslant \mathrm{Aut}(T). \qquad (\star)$$

If B is regular, then there exists $N \trianglelefteq H$ and $M \trianglelefteq K$ such that

$$H/N \cong K/M \text{ and } |H : N| = |HK : T||H \cap K|. \qquad (\star\star)$$

Much effort is needed to determine the factorisations satisfying $(\star)$ and $(\star\star)$.

Example

Assume $HK = S_n$ with $H = S_{n-1}$ (so K is transitive on $[n]$). Then $(\star) + (\star\star) \iff |K| = n$ and the Sylow 2-subgroups of K are cyclic.

Regular subgroups of holomorphs and applications

Theorem (H & Wang, 2025+)

For every finite simple group T, the **regular** subgroups of $\mathrm{Hol}(T)$ are determined, up to conjugacy.

Regular subgroups of holomorphs and applications

Theorem (H & Wang, 2025+)

For every finite simple group T, the **regular** subgroups of $\mathrm{Hol}(T)$ are determined, up to conjugacy.

For a finite group Y, TFAE:

- B is isomorphic to a regular subgroup of $\mathrm{Hol}(Y)$;
- $\exists$ a **Hopf-Galois structure** of type B on any Galois extension with Galois group Y.
- $\exists$ a **skew brace** $(X, +, \circ)$ with $Y \cong (X, +)$ and $B \cong (X, \circ)$.

Regular subgroups of holomorphs and applications

Theorem (H & Wang, 2025+)

For every finite simple group T, the **regular** subgroups of $\mathrm{Hol}(T)$ are determined, up to conjugacy.

For a finite group Y, TFAE:

- B is isomorphic to a regular subgroup of $\mathrm{Hol}(Y)$;
- $\exists$ a **Hopf-Galois structure** of type B on any Galois extension with Galois group Y.
- $\exists$ a **skew brace** $(X, +, \circ)$ with $Y \cong (X, +)$ and $B \cong (X, \circ)$.

Theorem (H & Wang, 2025+)

- The types of Hopf-Galois structures are determined on any Galois extension whose Galois group is finite simple.
- The skew braces with finite simple additive groups are classified.

Main result

Theorem (H & Wang, 2025+). The regular and the soluble transitive subgroups of **diagonal type** groups are determined, up to conjugacy.

Main result

Theorem (H & Wang, 2025+). The regular and the soluble transitive subgroups of **diagonal type** groups are determined, up to conjugacy.

This is mainly built on

- **Liebeck, Praeger & Saxl, 2000**
- **Morris & Spiga, 2021:** Describes the regular subgroups of general diagonal type groups based on those of the holomorphs
- The results for holomorphs

Part I. Transitive subgroups of primitive groups

Part II. Bases for primitive groups

Bases

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

Base: $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$.

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

Bases

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

Base: $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$.

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

Other base-related invariants: Irredundant base size; Greedy base size... (Ask some of the audience)

Bases

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

Base: $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$.

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

Other base-related invariants: Irredundant base size; Greedy base size... (Ask some of the audience)

Examples

- $G = S_n$, $|\Omega| = n$: $b(G) = n - 1$.

Bases

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

Base: $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$.

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

Other base-related invariants: Irredundant base size; Greedy base size... (Ask some of the audience)

Examples

- $G = S_n$, $|\Omega| = n$: $b(G) = n - 1$.
- $G = \mathrm{GL}(V)$, $\Omega = V$: $b(G) = \dim V$.

Bases

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

Base: $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$.

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

Other base-related invariants: Irredundant base size; Greedy base size... (Ask some of the audience)

Examples

- $G = S_n$, $|\Omega| = n$: $b(G) = n - 1$.
- $G = \mathrm{GL}(V)$, $\Omega = V$: $b(G) = \dim V$.
- $G = D_{2n}$, $|\Omega| = n$: $b(G) = 2$.

Connections

Abstract group theory. Write $H = G_\alpha$ and view $\Omega = G/H$. Then

$$b(G) = \text{minimal cardinality of a subset } S \subseteq G \text{ with } \bigcap_{g \in S} H^g = 1.$$

Connections

Abstract group theory. Write $H = G_\alpha$ and view $\Omega = G/H$. Then

$$b(G) = \text{minimal cardinality of a subset } S \subseteq G \text{ with } \bigcap_{g \in S} H^g = 1.$$

Computational group theory. The **Schreier-Sims algorithm** to find $|G|$, to determine whether $g \in G$, or others (in polynomial time)...

Connections

Abstract group theory. Write $H = G_\alpha$ and view $\Omega = G/H$. Then

$$b(G) = \text{minimal cardinality of a subset } S \subseteq G \text{ with } \bigcap_{g \in S} H^g = 1.$$

Computational group theory. The **Schreier-Sims algorithm** to find $|G|$, to determine whether $g \in G$, or others (in polynomial time)...

Graph theory. For a graph Γ with vertex set V, let $G = \mathrm{Aut}(\Gamma) \leqslant \mathrm{Sym}(V)$. Then

$$\begin{aligned} b(G) &= \text{the } \textbf{fixing number} \text{ of } \Gamma \\ &= \text{the } \textbf{determining number} \text{ of } \Gamma \\ &= \text{the } \textbf{rigidity index} \text{ of } \Gamma. \end{aligned}$$

Connections

Abstract group theory. Write $H = G_\alpha$ and view $\Omega = G/H$. Then

$$b(G) = \text{minimal cardinality of a subset } S \subseteq G \text{ with } \bigcap_{g\in S} H^g = 1.$$

Computational group theory. The **Schreier-Sims algorithm** to find $|G|$, to determine whether $g \in G$, or others (in polynomial time)...

Graph theory. For a graph Γ with vertex set V, let $G = \mathrm{Aut}(\Gamma) \leqslant \mathrm{Sym}(V)$. Then

$$\begin{aligned} b(G) &= \text{the \textbf{fixing number} of } \Gamma \\ &= \text{the \textbf{determining number} of } \Gamma \\ &= \text{the \textbf{rigidity index} of } \Gamma. \end{aligned}$$

Representation theory. For $H \leqslant G$ core-free, the **depth** $d_G(H)$ is the minimal depth of the inclusion of complex group algebras $\mathbb{C}H \subseteq \mathbb{C}G$. Then

$$d_G(H) \leqslant 2b(G) - 1$$

with respect to the permutation representation of G on G/H.

Bounds

Let Δ be a base of size $b(G)$ and let $x, y \in G$. Then

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

Bounds

Let Δ be a base of size $b(G)$ and let $x, y \in G$. Then

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

Thus, we have $|G| \leqslant |\Omega|^{b(G)}$, so $b(G) \geqslant \log_{|\Omega|} |G|$.

Bounds

Let Δ be a base of size $b(G)$ and let $x, y \in G$. Then

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

Thus, we have $|G| \leqslant |\Omega|^{b(G)}$, so $b(G) \geqslant \log_{|\Omega|} |G|$.

Write $\Delta = \{\alpha_1, \ldots, \alpha_{b(G)}\}$ and $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$.

Bounds

Let Δ be a base of size $b(G)$ and let $x, y \in G$. Then

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

Thus, we have $|G| \leqslant |\Omega|^{b(G)}$, so $b(G) \geqslant \log_{|\Omega|} |G|$.

Write $\Delta = \{\alpha_1, \ldots, \alpha_{b(G)}\}$ and $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$. Then

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

Bounds

Let Δ be a base of size $b(G)$ and let $x, y \in G$. Then

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

Thus, we have $|G| \leqslant |\Omega|^{b(G)}$, so $b(G) \geqslant \log_{|\Omega|} |G|$.

Write $\Delta = \{\alpha_1, \ldots, \alpha_{b(G)}\}$ and $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$. Then

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

Hence, $|G| \geqslant 2^{b(G)}$ and so $b(G) \leqslant \log_2 |G|$.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Notes.

- $Q(G,c) < 1 \iff b(G) \leqslant c$.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Notes.

- $Q(G,c) < 1 \iff b(G) \leqslant c$.
- $(\alpha_1,\ldots,\alpha_c)$ is not a base $\iff \exists\, x \in G_{\alpha_1} \cap \cdots \cap G_{\alpha_c}$ of prime order.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Notes.

- $Q(G,c) < 1 \iff b(G) \leqslant c$.
- $(\alpha_1,\ldots,\alpha_c)$ is not a base $\iff \exists\, x \in G_{\alpha_1} \cap \cdots \cap G_{\alpha_c}$ of prime order.
- For $x \in G$, the probability that a random c-tuple of Ω is fixed by x is $\mathrm{fpr}(x)^c$, where $\mathrm{fpr}(x)$ is the **fixed point ratio** of x on Ω.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Notes.

- $Q(G,c) < 1 \iff b(G) \leqslant c$.
- $(\alpha_1,\ldots,\alpha_c)$ is not a base $\iff \exists\, x \in G_{\alpha_1} \cap \cdots \cap G_{\alpha_c}$ of prime order.
- For $x \in G$, the probability that a random c-tuple of Ω is fixed by x is $\mathrm{fpr}(x)^c$, where $\mathrm{fpr}(x)$ is the **fixed point ratio** of x on Ω.
- $\mathrm{fpr}(x) = \frac{|x^G \cap G_\alpha|}{|x^G|}$ if G is transitive.

Probabilistic method (Liebeck & Shalev, 1999)

Let $c \geqslant 2$ be an integer and let

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : G_{\alpha_1} \cap \cdots \cap G_{\alpha_c} \neq 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of Ω is NOT a base for G.

Notes.

- $Q(G,c) < 1 \iff b(G) \leqslant c$.
- $(\alpha_1,\ldots,\alpha_c)$ is not a base $\iff \exists\, x \in G_{\alpha_1} \cap \cdots \cap G_{\alpha_c}$ of prime order.
- For $x \in G$, the probability that a random c-tuple of Ω is fixed by x is $\mathrm{fpr}(x)^c$, where $\mathrm{fpr}(x)$ is the **fixed point ratio** of x on Ω.
- $\mathrm{fpr}(x) = \frac{|x^G \cap G_\alpha|}{|x^G|}$ if G is transitive.

Therefore, if G is transitive, then

$$Q(G,c) \leqslant \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c = \sum_{x \in \mathcal{P}} \frac{|x^G \cap G_\alpha|^c}{|x^G|^c},$$

where $\mathcal{P}$ is the set of prime order elements in G.

Primitive groups

Assume G is primitive.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2\log_{|\Omega|}|G| + 24$.

This establishes a strong form of **Pyber's conjecture (1993)**.

Primitive groups

Assume G is primitive.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2\log_{|\Omega|}|G| + 24$.

This establishes a strong form of **Pyber's conjecture (1993)**.

Some other bounds:

- **Seress, 1996:** $b(G) \leqslant 4$ if G is soluble.

Primitive groups

Assume G is primitive.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2\log_{|\Omega|}|G| + 24$.

This establishes a strong form of **Pyber's conjecture (1993)**.

Some other bounds:

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

Primitive groups

Assume G is primitive.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2\log_{|\Omega|}|G| + 24$.

This establishes a strong form of **Pyber's conjecture (1993)**.

Some other bounds:

- **Seress, 1996:** $b(G) \leqslant 4$ if G is soluble.
- **Burness, 2021:** $b(G) \leqslant 5$ if G_α is soluble.
- **Burness et al., 2007-11:** $b(G) \leqslant 7$ if G is almost simple in a **non-standard** action **(Cameron's conjecture)**.

Primitive groups

Assume G is primitive.

Halasi, Liebeck & Maróti, 2019: $b(G) \leqslant 2\log_{|\Omega|}|G| + 24$.

This establishes a strong form of **Pyber's conjecture (1993)**.

Some other bounds:

- **Seress, 1996:** $b(G) \leqslant 4$ if G is soluble.
- **Burness, 2021:** $b(G) \leqslant 5$ if G_α is soluble.
- **Burness et al., 2007-11:** $b(G) \leqslant 7$ if G is almost simple in a **non-standard** action **(Cameron's conjecture)**.

Problem. Determine $b(G)$ for all primitive groups $G \leqslant \mathrm{Sym}(\Omega)$.

Example: Symmetric groups on subsets

Let $G = S_n$ and $\Omega = \{k\text{-subsets of } [n]\}$, where $2k < n$ (so G is primitive).

Example: Symmetric groups on subsets

Let $G = S_n$ and $\Omega = \{k\text{-subsets of } [n]\}$, where $2k < n$ (so G is primitive).

Mecenero & Spiga, 2024:

$b(G)$ = smallest integer ℓ such that

$$\sum_{\substack{\pi \vdash n \\ \pi=(1^{c_1},\ldots,n^{c_n})}} (-1)^{n-\sum_{i=1}^n c_i} \frac{n!}{\prod_{i=1}^n i^{c_i} c_i!} \left(\sum_{\substack{\eta \vdash k \\ \eta=(1^{b_1},\ldots,k^{b_k})}} \prod_{j=1}^k \binom{c_j}{b_j} \right)^\ell \neq 0.$$

del Valle & Roney-Dougal, 2024:

$b(G)$ = smallest integer ℓ such that $\exists\, r \leqslant \ell + 1$ satisfying

$$0 \leqslant \frac{1}{r}\left(\ell k - \sum_{i=1}^{r-1} i \binom{\ell}{i}\right) \leqslant \binom{\ell}{r}$$

and

$$\sum_{i=0}^{r-1} \binom{\ell}{i} + \frac{1}{r}\left(\ell k - \sum_{i=1}^{r-1} i \binom{\ell}{i}\right) \geqslant n.$$

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

Steinberg, 1962 (+ CFSG): $\exists\, x, y \in T$ such that $T = \langle x, y \rangle$.

This shows that $b(G) = 3$.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

Steinberg, 1962 (+ CFSG): $\exists\, x, y \in T$ such that $T = \langle x, y \rangle$.

This shows that $b(G) = 3$.

A (slight) generalisation. Now let $G = N_{\mathrm{Sym}(T)}(\mathrm{Hol}(T)) = \mathrm{Hol}(T).2$.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

Steinberg, 1962 (+ CFSG): $\exists\, x, y \in T$ such that $T = \langle x, y \rangle$.

This shows that $b(G) = 3$.

A (slight) generalisation. Now let $G = N_{\mathrm{Sym}(T)}(\mathrm{Hol}(T)) = \mathrm{Hol}(T).2$.

Here $\{1, x, y\}$ is a base if $T = \langle x, y \rangle$ and $\nexists\, \alpha \in \mathrm{Aut}(T)$ such that

$$(x, y)^\alpha = (x^{-1}, y^{-1}).$$

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

Steinberg, 1962 (+ CFSG): $\exists\, x, y \in T$ such that $T = \langle x, y \rangle$.

This shows that $b(G) = 3$.

A (slight) generalisation. Now let $G = N_{\mathrm{Sym}(T)}(\mathrm{Hol}(T)) = \mathrm{Hol}(T).2$.

Here $\{1, x, y\}$ is a base if $T = \langle x, y \rangle$ and $\nexists\, \alpha \in \mathrm{Aut}(T)$ such that

$$(x, y)^{\alpha} = (x^{-1}, y^{-1}).$$

Lucchini & Spiga, 2023: Such a pair exists if and only if $T \neq \mathrm{PSL}_2(q)$.

The holomorphs of simple groups

Let $G = \mathrm{Hol}(T) = T{:}\mathrm{Aut}(T) = T^2.\mathrm{Out}(T)$ be the **holomorph** of a non-abelian simple group T. Recall that $G \leqslant \mathrm{Sym}(T)$ is primitive.

- 1-point stabiliser: $G_1 = \mathrm{Aut}(T)$.
- 2-point stabiliser: $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \implies b(G) \geqslant 3$.

Steinberg, 1962 (+ CFSG): $\exists\, x, y \in T$ such that $T = \langle x, y \rangle$.

This shows that $b(G) = 3$.

A (slight) generalisation. Now let $G = N_{\mathrm{Sym}(T)}(\mathrm{Hol}(T)) = \mathrm{Hol}(T).2$.

Here $\{1, x, y\}$ is a base if $T = \langle x, y \rangle$ and $\nexists\, \alpha \in \mathrm{Aut}(T)$ such that

$$(x, y)^\alpha = (x^{-1}, y^{-1}).$$

Lucchini & Spiga, 2023: Such a pair exists if and only if $T \neq \mathrm{PSL}_2(q)$.

H, 2024: $b(G) \in \{3, 4\}$, with $b(G) = 4$ if and only if $T \in \{A_5, A_6\}$.

General diagonal type groups

Write $D = \{(t, \ldots, t) : t \in T\} \leqslant T^k$,

General diagonal type groups

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

General diagonal type groups

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

Diagonal type group: A group $G \leqslant \mathrm{Sym}(\Omega)$ with

$$T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k) \cong T^k.(\mathrm{Out}(T) \times S_k).$$

General diagonal type groups

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

Diagonal type group: A group $G \leqslant \mathrm{Sym}(\Omega)$ with

$$T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k) \cong T^k.(\mathrm{Out}(T) \times S_k).$$

Notes.

- G induces a subgroup $P \leqslant S_k$ on $[k]$.

General diagonal type groups

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

Diagonal type group: A group $G \leqslant \mathrm{Sym}(\Omega)$ with

$$T^k \trianglelefteq G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k) \cong T^k.(\mathrm{Out}(T) \times S_k).$$

Notes.

- G induces a subgroup $P \leqslant S_k$ on $[k]$.
- G is primitive $\iff$ P is primitive, or $k = 2$ and $P = 1$ (holomorph).

General diagonal type groups

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

Diagonal type group: A group $G \leqslant \mathrm{Sym}(\Omega)$ with

$$T^k \trianglelefteqslant G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k) \cong T^k.(\mathrm{Out}(T) \times S_k).$$

Notes.

- G induces a subgroup $P \leqslant S_k$ on $[k]$.
- G is primitive $\iff$ P is primitive, or $k = 2$ and $P = 1$ (holomorph).

Fawcett, 2013: $b(G) = 2$ if $P \notin \{A_k, S_k\}$.

General diagonal type groups

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

Diagonal type group: A group $G \leqslant \mathrm{Sym}(\Omega)$ with

$$T^k \trianglelefteq G \leqslant N_{\mathrm{Sym}(\Omega)}(T^k) \cong T^k.(\mathrm{Out}(T) \times S_k).$$

Notes.

- G induces a subgroup $P \leqslant S_k$ on $[k]$.
- G is primitive $\iff$ P is primitive, or $k = 2$ and $P = 1$ (holomorph).

Fawcett, 2013: $b(G) = 2$ if $P \notin \{A_k, S_k\}$.

This is (basically) based on Steinberg and

Cameron, Neumann & Saxl, 1984; Seress, 1997: With 43 exceptions, if $P \notin \{A_k, S_k\}$ then $\exists\ \Delta \subseteq [k]$ with setwise stabiliser $P_{\{\Delta\}} = 1$.

Back to the holomorph

Let $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group.

For $S \subseteq T$, write $\mathrm{Hol}(T,S)$ for its setwise stabiliser in $\mathrm{Hol}(T)$.

Back to the holomorph

Let $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group.

For $S \subseteq T$, write $\mathrm{Hol}(T, S)$ for its setwise stabiliser in $\mathrm{Hol}(T)$.

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1.$$

Back to the holomorph

Let $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group.

For $S \subseteq T$, write $\mathrm{Hol}(T, S)$ for its setwise stabiliser in $\mathrm{Hol}(T)$.

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1.$$

Remark. For $G = T^k.(\mathrm{Out}(T) \times S_k)$, this is an "if and only if".

Back to the holomorph

Let $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group.

For $S \subseteq T$, write $\mathrm{Hol}(T, S)$ for its setwise stabiliser in $\mathrm{Hol}(T)$.

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1.$$

Remark. For $G = T^k.(\mathrm{Out}(T) \times S_k)$, this is an "if and only if".

Example

For "most" T, there exist $x, y \in T$ such that $|x| = 2$, $|y| = 3$ and $T = \langle x, y \rangle$. Then take $S = \{1, x, y\}$.

Back to the holomorph

Let $G \leqslant T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal type primitive group.

For $S \subseteq T$, write $\mathrm{Hol}(T, S)$ for its setwise stabiliser in $\mathrm{Hol}(T)$.

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1.$$

Remark. For $G = T^k.(\mathrm{Out}(T) \times S_k)$, this is an "if and only if".

Example

For "most" T, there exist $x, y \in T$ such that $|x| = 2$, $|y| = 3$ and $T = \langle x, y \rangle$. Then take $S = \{1, x, y\}$.

General case: Give a "nice" upper bound on the probability that a random k-subset S satisfies $\mathrm{Hol}(T, S) \neq 1$ (if the bound is < 1 then we are happy).

Main results

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1. \qquad (\diamond)$$

Main results

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1. \qquad (\diamond)$$

Note. $(\diamond)$ holds only if $3 \leqslant k \leqslant |T| - 3$ since $b(\mathrm{Hol}(T)) = 3$.

Main results

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1. \qquad (\diamond)$$

Note. $(\diamond)$ holds only if $3 \leqslant k \leqslant |T| - 3$ since $b(\mathrm{Hol}(T)) = 3$.

Theorem (H, 2024)

For $3 \leqslant k \leqslant |T| - 3$, property $(\diamond)$ holds.

Main results

Key observation (H, 2024). $b(G) = 2$ if

$$\exists\ S \subseteq T \text{ with } |S| = k \text{ and } \mathrm{Hol}(T, S) = 1. \qquad (\diamond)$$

Note. $(\diamond)$ holds only if $3 \leqslant k \leqslant |T| - 3$ since $b(\mathrm{Hol}(T)) = 3$.

Theorem (H, 2024)

For $3 \leqslant k \leqslant |T| - 3$, property $(\diamond)$ holds.

Heavily based on this, and built on Fawcett...

Theorem (H, 2024). The exact base size for every **diagonal type** primitive group is determined.

Thank you!