Bases for permutation groups

H. Y. Huang (UoB)

@ SUSTech

07 / 09 / 2023

1. Bases

Let $G \leq \mathrm{Sym}(\Omega)$, where $|\Omega| < \infty$ and G is <u>transitive</u>.

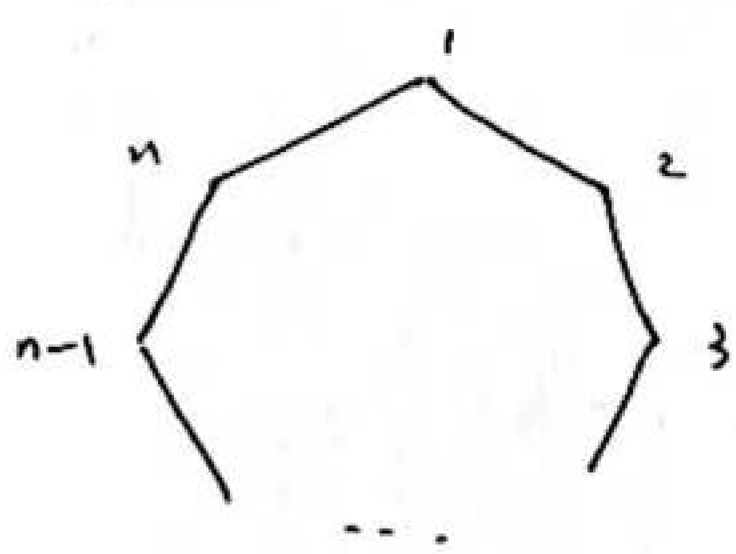
- Point stabiliser: $G_\alpha = \{ g \in G : \alpha^g = \alpha \}$.

<u>Note</u> $\bigcap_{\alpha \in \Omega} G_\alpha = 1$.

<u>Question</u> Any subset $\Delta \subseteq \Omega$ with $\bigcap_{\alpha \in \Delta} G_\alpha = 1$?

<u>Examples</u>

- $G = S_n$, $|\Omega| = n$, $\Delta = \{1, \dots, n-1\}$ $\boxed{b(G) = n-1}$
- $G = D_{2n}$, $|\Omega| = n$, $\Delta = \{1, 2\}$ $\boxed{b(G) = 2}$



- $G = GL(V)$, $\Omega = V \setminus \{0\}$

  Δ contains a basis of V $\boxed{b(G) = \dim V}$

- $G = S_n$, $\Omega = \{ k\text{-subsets of } [n] \}$, $2k \leq n$

  $\Delta = \{ \{1, \dots, k\}, \{2, \dots, k+1\}, \dots, \{n-k+1, \dots, n\} \}$

$b(G) =$ smallest ℓ s.t.

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

by Mecenero & Spiga, 04/08/23

same (?) result by del Valle & Roney-Dougal 08/08/23

Def • $\Delta \subseteq \Omega$ is called a <u>base</u> for G if $\bigcap_{\alpha\in\Delta} G_\alpha = 1$.

• The <u>base size</u> of G, denoted $b(G)$, is the minimal size of a base for G.

Connections

• $b(G)$ = min size of a subset $S \subseteq G$ with $\bigcap_{g\in S} G_\alpha^g = 1$.

• Let Γ be a graph and $G = \mathrm{Aut}(\Gamma)$. Then

$b(G)$ = the <u>fixing number</u> of Γ

= the <u>determining number</u> of Γ

= the <u>rigidity index</u> of Γ.

Q1 Determine $b(G)$?

Q2 Bounds on $b(G)$?

Q3 Classify G with $b(G) = 2$?

Lower bound

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

$$\alpha^x = \alpha^y \ \forall \alpha \in \Delta \iff x^{-1}y \in \bigcap_{\alpha\in\Delta} G_\alpha$$
$$\iff x = y$$

That is,

elements of $G \xleftrightarrow{1-1}$ images of Δ.

We have $|G| \le |\Omega|^{b(G)}$, so $b(G) \ge \log_{|\Omega|}|G|$.

Upper bound

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

$$G \gneq G^{(1)} \gneq G^{(2)} \gneq \dots \gneq G^{(b(G))} = 1$$

Hence, $|G| \geq 2^{b(G)}$, so $b(G) \leq \log_2 |G|$.

2. Primitive groups

- "Primitive" = "transitive" + "$G_\alpha \underset{max}{<} G$".

<u>Example</u> $G = D_{2n}$, $|\Omega| = n$. Then G primitive $\iff$ n prime.

<u>Bounds</u>

- Bochert, 1889: $|\Omega| = n$, $G \neq A_n, S_n$ $\Rightarrow$ $b(G) \leq \frac{n}{2}$.
- Liebeck, 1984: $b(G) < c\sqrt{|\Omega|}$ for some absolute constant c.
- Duyan, Halasi, & Maróti, 2018:
$$b(G) \leq c \log_{|\Omega|} |G|$$
for some absolute constant c. (Pyber's conjecture, 1993).
- Halasi, Liebeck & Maróti, 2019: $b(G) \leq 2 \log_{|\Omega|} |G| + 24$

Special cases:

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

Probabilistic method (Liebeck & Shalev, 1999).

$$Q(G,c) = \frac{|\{(\alpha_1,\dots,\alpha_c)\in\Omega^c : \bigcap G_{\alpha_i} \neq 1\}|}{|\Omega|^c}$$

is the probability that a random c-tuple is NOT a base.

Note $b(G) \leq c \iff Q(G,c) < 1$.

We have

$$Q(G,c) \leq \sum_{\substack{x\in G \\ |x| \text{ prime}}} \left(\frac{|x^G \cap G_\alpha|}{|G_\alpha|}\right)^c =: \widehat{Q}(G,c)$$

Note $\widehat{Q}(G,c) < 1 \Rightarrow b(G) \leq c$.

O'Nan - Scott

Finite primitive groups are divided into 5 types:

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

3. Diagonal type

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

$$X = \{(x, \dots, x) : x \in T\} \leq T^k$$

Then $T^k \leq \mathrm{Sym}(\Omega)$, where $\Omega = [T^k : X]$.

A group G is said to be <u>diagonal type</u> if

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

<u>Note</u> G induces $P_G \leq S_k$.

<u>Lemma</u> G is primitive $\iff$ P_G is primitive, or $\boxed{k=2 \text{ and } P_G = 1}$

$$T : \mathrm{Inn}(T) \trianglelefteq G \leq T : \mathrm{Aut}(T) = \mathrm{Hol}(T).$$

<u>Theorem</u> (Fawcett, 2013) $P_G \notin \{A_k, S_k\} \Rightarrow b(G) = 2$.

<u>Key observation</u>

$b(G) = 2$ if $\exists\, S \subseteq T$ s.t. $|S| = k$ and $\mathrm{Hol}(T)_{\{S\}} = 1$.

<u>Examples</u>.

- Suppose $T = \langle x, y \rangle$ with $|x| = 2$ and $|y| = 3$.

  Then $\mathrm{Hol}(T)_{\{S\}} = 1$, where $S = \{1, x, y\}$.

  <u>proof</u>. $g^{-1}S = S^{\alpha^{-1}}$ if $g\alpha \in \mathrm{Hol}(T)_{\{S\}}$, whence $g \in S$.

  If $g \neq 1$, then $x^{-1}y \in S^{\alpha^{-1}}$ or $y^{-1}x \in S^{\alpha^{-1}}$, but $|x^{-1}y| \neq 2$ or 3.

  If $g = 1$, then $\alpha \in C_{\mathrm{Aut}(T)}(x) \cap C_{\mathrm{Aut}(T)}(y) = 1$.

- Suppose $|x| = |y| = 2$ and $x^{\mathrm{Aut}(T)} \neq y^{\mathrm{Aut}(T)}$.

  <u>Note</u> $\exists\, z \in T$ s.t. $\langle x, z \rangle = \langle y, z \rangle = T$.

  Then $\mathrm{Hol}(T)_{\{S\}} = 1$, where $S = \{1, x, y, z\}$.

Theorem (H, 2023+) If $3 \leq k \leq |T|-3$, then $\exists\, S \subseteq T$ s.t.

$|S| = k$ and $\mathrm{Hol}(T)_{\{S\}} = 1$.

Theorem (H, 2023+) $b(G) = 2 \iff$ one of the following:

(i) $P_G \notin \{A_k, S_k\}$

(ii) $3 \leq k \leq |T|-3$

(iii) $k \in \{|T|-2, |T|-1\}$ and $S_k \nleq G$.

Theorem (H, 2023+) Base sizes of diagonal type primitive groups are determined.