Bases for permutation groups

H. Y. Huang (Bristol)

@ Milano - Bicocca

06/09/24

Throughout, let $G \leq \mathrm{Sym}(\Omega)$ be a <u>transitive</u> group and assume $|\Omega| < \infty$.

§1 Bases

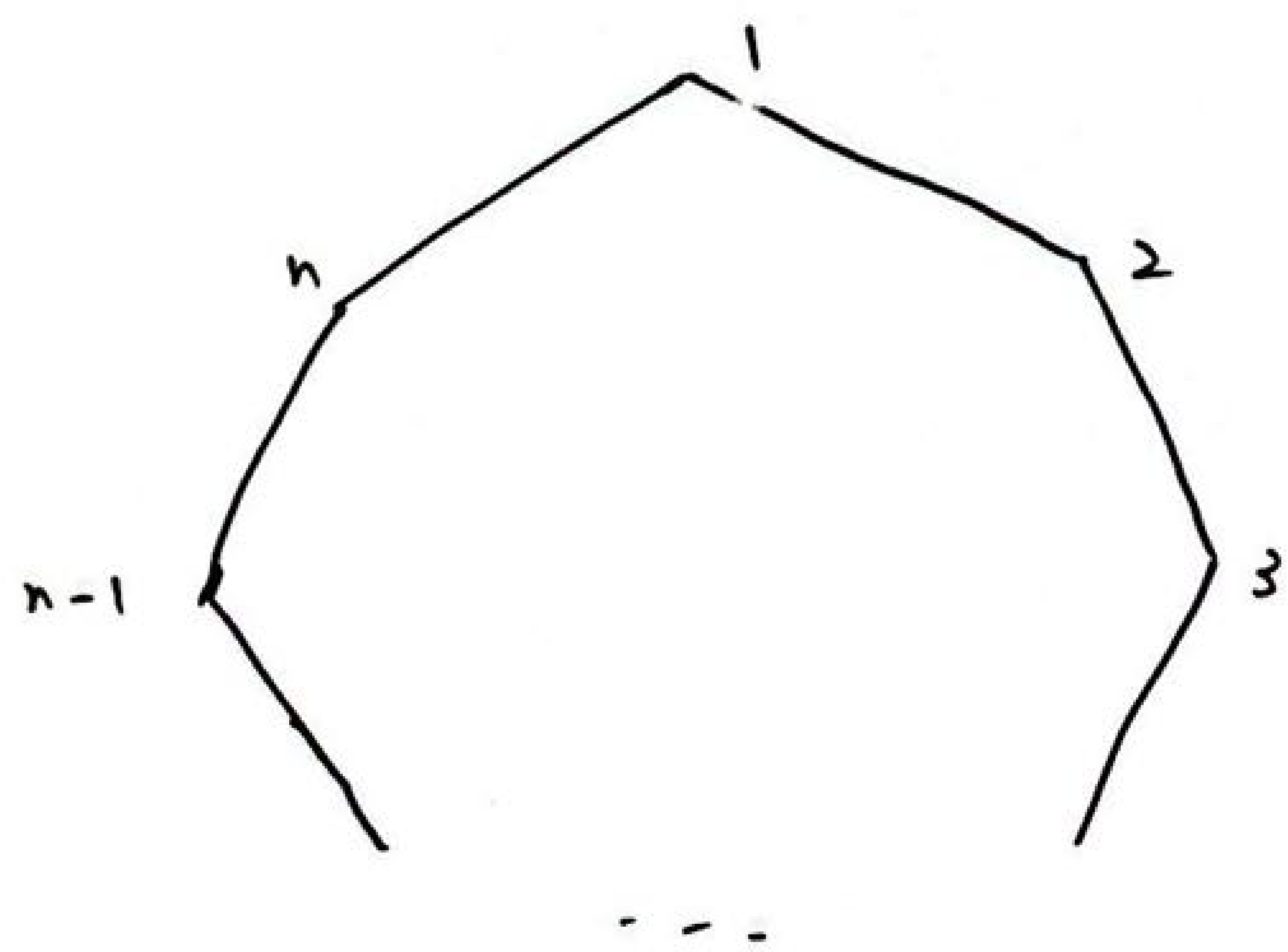
Base $\Delta \subseteq \Omega$ s.t. $\bigcap_{\alpha \in \Delta} G_\alpha = 1$

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

Examples

- $G = S_n$, $|\Omega| = n$, $\Delta = \{1, \dots, n-1\}$; $b(G) = n-1$.
- $G = GL(V)$, $\Omega = V \setminus \{0\}$:

  Δ contains a basis of V, $b(G) = \dim V$
- $G = D_{2n}$, $|\Omega| = n$, $\Delta = \{1, 2\}$; $b(G) = 2$



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

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

  $b(G)$? Ask Pablo.

P1 Determine $b(G)$.

Trivial bounds $\log_{|\Omega|}|G| \le b(G) \le \log_2 |G|$.

Probabilistic method I (Liebeck & Shalev, 1999)

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

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

Suppose $G_{\alpha_1}\cap\cdots\cap G_{\alpha_c}\neq 1$. Then $\exists\, x\in G_{\alpha_1}\cap\cdots\cap G_{\alpha_c}$ of prime order. Thus, $\alpha_1,\ldots,\alpha_c\in \mathrm{fix}_\Omega(x)$ and

$$Q(G,c) \le \sum_{\substack{x\in G\\ |x| \text{ prime}}}\left(\frac{|\mathrm{fix}_\Omega(x)|}{|\Omega|}\right)^c$$

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

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

Primitive group $G_\alpha \le_{\max} G$

e.g. $G = D_{2n}$, $|\Omega| = n$: G is primitive $\iff$ n is prime.

- Bochert, 1889: $|\Omega| = n$, $G\neq A_n, S_n$ primitive $\Rightarrow b(G)\le \frac{n}{2}$.

...

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

O'Nan - Scott Finite primitive groups are divided into 5 types

- affine
- almost simple (ask Pablo)
- diagonal type
- Product type
- twisted wreath products.

§2 Diagonal type groups

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

$$D = \{(t, \dots, t) : t \in T\} \leq T^k$$

Then $T^k \leq \mathrm{Sym}(\Omega)$ with $\Omega = [T^k : D]$.

A group $G \leq \mathrm{Sym}(\Omega)$ is said to be of <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 $P_G \leq S_k$, so $T^k \trianglelefteq G \leq T^k.(\mathrm{Out}(T) \times P_G)$.

<u>Lemma</u> G is primitive $\iff$ P_G is primitive, or $k = 2$ & $P_G = 1$

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

<u>Key observation</u> $b(G) = 2$ if

$$\exists\, S \subseteq T \text{ s.t. } |S| = k \ \& \ \mathrm{Hol}(T)_{\{S\}} = 1 \qquad (*)$$

<u>Probabilistic method II</u> (H, 2024)

Let $\mathrm{fix}(\sigma, k) = \{S \subseteq T : |S| = k \ \& \ \sigma \in \mathrm{Hol}(T)_{\{S\}}\}$

Then $b(G) = 2$ if

$$\sum_{\substack{\sigma \in \mathrm{Hol}(T) \\ |\sigma| \text{ prime}}} |\mathrm{fix}(\sigma, k)| < \binom{|T|}{k}$$

<u>Theorem</u> (H, 2024)

If $3 \leq k \leq |T| - 3$, then $(*)$ holds.

<u>Theorem</u> (Fawcett 2013; H, 2024)

P1 is done if G is a diagonal type primitive group.

§3 Regular orbits

Note $b(G) = \min\{k \mid G \text{ has a regular orbit on } \Omega^k\}$

$\mathrm{reg}(G) :=$ # regular G-orbits on $\Omega^{b(G)}$

Examples

- $G = S_n$, $|\Omega| = n$: $\mathrm{reg}(G) = 1$
- $G = GL(V)$, $\Omega = V \setminus \{0\}$: $\mathrm{reg}(G) = 1$
- $G = D_{2n}$, $|\Omega| = n$: $\mathrm{reg}(G) = \lceil \frac{n}{2} \rceil - 1$

P2 Classify G with $\mathrm{reg}(G) = 1$.

Example $G = PGL_2(q)$, $\Omega = \{2\text{-subsets of } \{1\text{-spaces of } \mathbb{F}_q^2\}\}$.

Then $\{\alpha, \beta\}$ is a base $\Leftrightarrow |\alpha \cap \beta| = 1$. So $\mathrm{reg}(G) = 1$.

Recall Probabilistic method I

$$Q(G, b(G)) = 1 - \frac{\mathrm{reg}(G) \cdot |G|}{|\Omega|^{b(G)}}$$

Results

Burness & H, 2022/23 : G almost simple, $G_\alpha \underset{\max}{<} G$ soluble ✓

(e.g. $(G, G_\alpha) = (PGL_2(q), D_{2(q-1)})$).

H, 2024 ; Freedman, H, Lee & Rekvényi, 2024+ :

If G is a diagonal type primitive group, then

$\mathrm{reg}(G) = 1 \Leftrightarrow G = T^k.(\mathrm{Out}(T) \times S_k)$ with $T = A_5$ & $k \in \{3,5,$