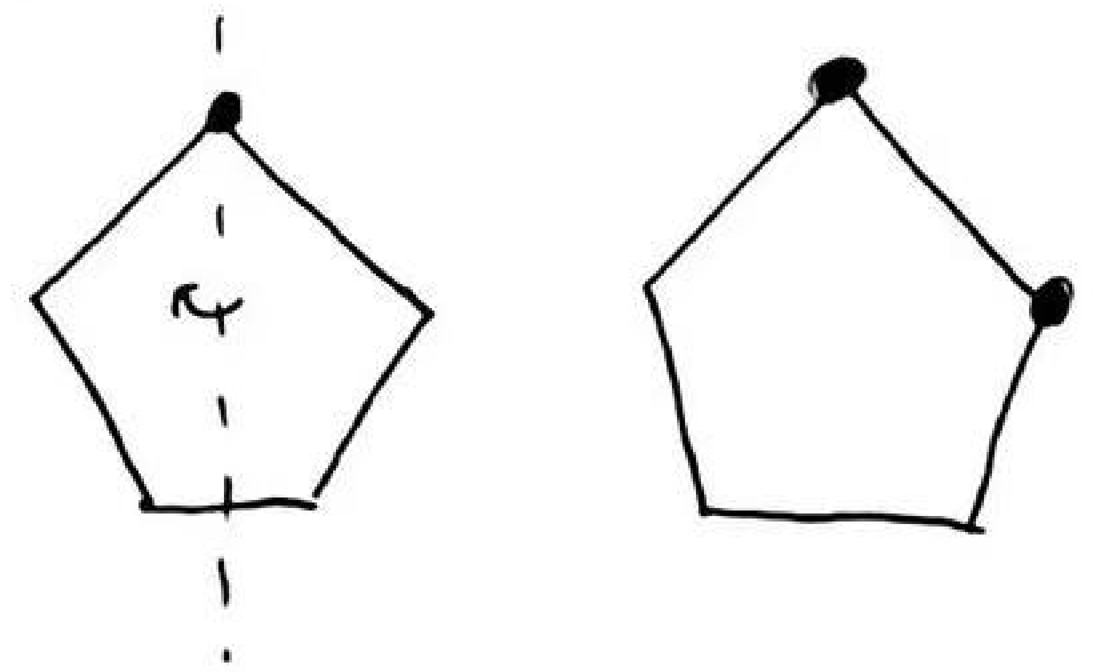
Permutation groups, symmetry breaking & probability.

H. Y. Huang
@ ZJU
24/12/24

§1 Bases.



<u>Fixing set</u>:

$\Delta \subseteq V\Gamma$ s.t. $\bigcap_{\alpha \in \Delta} \mathrm{Aut}(\Gamma)_\alpha = 1$.

<u>Fixing number</u>:

Min size of a fixing set.

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

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

<u>Base size $b(G)$</u> Min size of a base for G.

<u>Examples</u>

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

  Δ contains a basis for V. $b(G) = \dim V$.
- $G = D_{2n}$, $|\Omega| = n$: $b(G) = 2$.
- T non-abelian simple, $\Omega = T$. $G = T : \mathrm{Aut}(T) = \mathrm{Hol}(T)$.

  $G_1 = \mathrm{Aut}(T)$; $G_1 \cap G_x = C_{\mathrm{Aut}(T)}(x) \neq 1 \Rightarrow b(G) \geq 3$.

  <u>Steinberg 1962</u>: $\exists\, x, y \in T$ s.t. $\langle x, y \rangle = T$. ($\Rightarrow b(G) = 3$)

<u>Probabilistic method I</u> (Liebeck & Shalev, 1999)

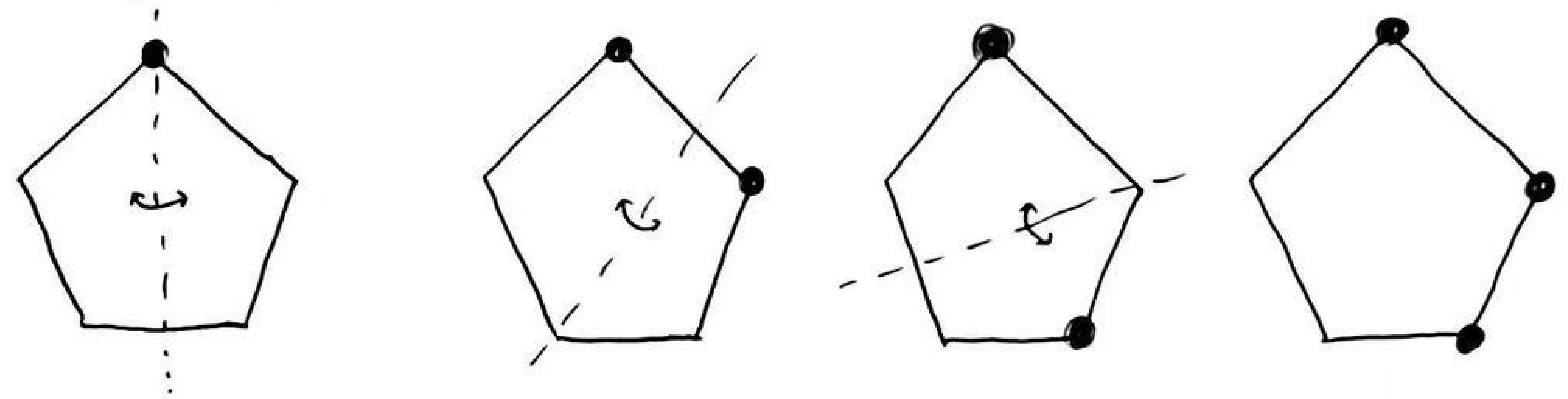
$$Q(G,k) = \frac{|\{(\alpha_1, \dots, \alpha_k) \in \Omega^k : G_{\alpha_1} \cap \dots \cap G_{\alpha_k} \neq 1\}|}{|\Omega|^k}$$

<u>Note</u> If $G_{\alpha_1} \cap \dots \cap G_{\alpha_k} \neq 1$ then $\exists\, x \in G$ of prime order s.t. $x \in G_{\alpha_1} \cap \dots \cap G_{\alpha_k}$. So

$$Q(G,k) \leq \sum_{x \in \mathcal{P}} \left(\frac{|\mathrm{fix}_\Omega(x)|}{|\Omega|} \right)^k = \sum_{x \in \mathcal{P}} \left(\frac{|x^G \cap G_\alpha|}{|x^G|} \right)^k =: \widehat{Q}(G,k),$$

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

§2 Distinguishing numbers.



Distinguishing partition: A partition $\Pi = \{\pi_1, \dots, \pi_m\}$ of Ω s.t.

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

Distinguishing number $D(G)$. Min size of a distinguishing partition

Examples

- $D(S_n) = n$
- $G = GL_d(q)$, $\Omega = \mathbb{F}_q^d \setminus \{0\}$.
  Klavžar, Wong & Zhu, 2006: $D(G) = 2$ if $\mathbb{F}_q^d \neq \mathbb{F}_2^2, \mathbb{F}_2^3, \mathbb{F}_4^2, \mathbb{F}_3^2$.
- $D(D_{2n}) = 2$ for $n \geq 6$; $D(D_{10}) = 3$.

Note $D(G) \leq 2 \iff \exists \Delta \subseteq \Omega$ s.t. $G_{\{\Delta\}} = 1$.

Probabilistic method II (Cameron, Neumann & Saxl, 1984).

$$Q(G) = \frac{|\{\Delta \subseteq \Omega : G_{\{\Delta\}} \neq 1\}|}{2^{|\Omega|}}$$

Note $G_{\{\Delta\}} \neq 1 \Rightarrow \exists x \in G_{\{\Delta\}}$ of prime order. So

$$Q(G) = \frac{1}{2^{|\Omega|}} \left| \bigcup_{x \in \mathcal{P}} \mathrm{fix}_{2^\Omega}(x) \right| \leq \frac{1}{2^{|\Omega|}} \sum_{x \in \mathcal{P}} |\mathrm{fix}_{2^\Omega}(x)|.$$

For $x \in G$ of cycle shape $[r^m, 1^{|\Omega|-mr}]$, we have $|\mathrm{fix}_{2^\Omega}(x)| = 2^{|\Omega|-m(r-1)}$

Let $\mu(G)$ be the minimal degree of G. Then $\mu(G) \leq mr$ and

$$|\mathrm{fix}_{2^\Omega}(x)| = 2^{|\Omega|-m(r-1)} \leq 2^{|\Omega|-(r-1)\mu(G)/r} \leq 2^{|\Omega|-\mu(G)/2}.$$

Thus, $Q(G) \leq \dfrac{|G|}{2^{\mu(G)/2}}$.

<u>Theorem</u> (Cameron, Neumann & Saxl, 1984; Seress, 1997).

$G \notin \{A_n, S_n\}$ primitive $\Rightarrow D(G) = 2$, with 43 exceptions of degree ≤ 32.

<u>Probabilistic method III</u> (H, 2024).

$$Q_k(G) = \frac{|\{\Delta \subseteq \Omega : |\Delta| = k \ \& \ G_{\{\Delta\}} = 1\}|}{\binom{|\Omega|}{k}}.$$

Then $Q_k(G) \leq \frac{1}{\binom{|\Omega|}{k}} \sum_{x \in \mathcal{P}} |fix_{\{k\text{-sets}\}}(x)|$.

For $x \in G$ of cycle shape $[r^m, 1^{|\Omega| - mr}]$, x fixes

$$\sum_{u=0}^{\lfloor k/r \rfloor} \binom{m}{u} \binom{|\Omega| - mr}{k - ru}$$

k-subsets of Ω.

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

If $3 \leq k \leq |T| - 3$, then $\exists \, \Delta \subseteq T$ s.t. $Hol(T)_{\{\Delta\}} = 1$ & $|\Delta| = k$.

§3 Connections.

<u>Trivial bound</u> $D(G) \leq b(G) + 1$

<u>Product type groups</u>. $L \leq Sym(\Gamma)$, $P \leq S_k$, $\Omega = \Gamma^k$, $G = L \wr P$.

<u>Theorem</u> (Bailey & Cameron, 2011)

$b(G) \leq m \iff G$ has at least $D(P)$ regular orbits on Ω^m.

<u>Diagonal type groups</u>.

Let T be a non-abelian simple group and let

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

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

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

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

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

Lemma G is primitive $\iff$ P_G is primitive, or $\boxed{k=2 \ \& \ P_G = 1}$

$\downarrow$

$G \leq \mathrm{Hol}(T)$.

Theorem (Fawcett, 2013)

$P_G \notin \{A_k, S_k\} \Rightarrow b(G) = 2$.

proof Steinberg + Cameron-Neumann-Saxl + constructions.

Proposition (H, 2024)

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

Hence, $3 \leq k \leq |T| - 3 \Rightarrow b(G) = 2$.

Theorem (H, 2024)

$b(G)$ is computed in all cases.