Permutations, bases and low rank groups

H. Y. Huang

Bristol

19/03/24.

Consider $G = GL(V) \curvearrowright V \setminus \{0\}$.

(a) $\forall$ basis $\{v_1, \ldots, v_n\}$ of V, $G_{v_1} \cap \cdots \cap G_{v_n} = 1$.

(b) $\forall$ bases $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ of V.

$\exists! \, g \in G$ s.t. $v_i^g = w_i \quad \forall i$.

(c) The G_v-orbits are $\{av\}_{a \in \mathbb{F}}$, $V \setminus \langle v \rangle$.

Throughout, let $G \leqslant \mathrm{Sym}(\Omega)$ be a <u>transitive</u> group

and assume $|\Omega| < \infty$

<u>§1</u>

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

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

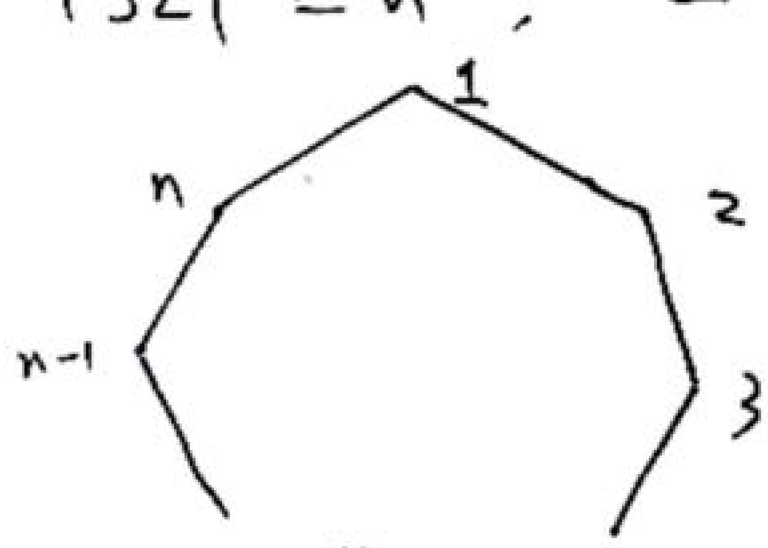
<u>Examples</u>

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

  Δ contains a basis of V. $b(G) = \dim V$.

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

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



P1 Determine $b(G)$.

Blaha, 1992: P1 is NP-hard

Note Let Δ be a base and $x, y \in G$. Then

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

Thus,

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

In particular, $b(G) \geq \log_{|\Omega|} |G|$.

Remark $b(G) \leq \log_2 |G|$.

Probabilistic method I (Liebeck & Shalev, 1999).

$$Q(G) = \frac{|\{(\alpha, \beta) \in \Omega^2 : G_\alpha \cap G_\beta \neq 1\}|}{|\Omega|^2}$$

Note $Q(G) < 1 \iff b(G) \leq 2$.

Suppose $G_\alpha \cap G_\beta \neq 1$. Then $\exists\, x \in G_\alpha \cap G_\beta$ of prime order.

Thus, $\alpha, \beta \in \mathrm{fix}_\Omega(x)$ and

$$Q(G) \leq \sum_{\substack{x \in G \\ |x| \text{ prime}}} \left(\frac{|\mathrm{fix}_\Omega(x)|^2}{|\Omega|^2} \right).$$

$$= \sum_{\substack{x \in G \\ |x| \text{ prime}}} \left(\frac{|x^G \cap G_\alpha|}{|x^G|} \right)^2 =: \hat{Q}(G).$$

Note $\hat{Q}(G) < 1 \Rightarrow b(G) \leq 2$.

Primitive group $G_\alpha \underset{\max}{<} G$

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

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

Let T be a non-abelian finite simple group.

Holomorph $Hol(T) = T : Aut(T)$, which is primitive on T.

$\vdots$ $b(Hol(T)) = 3$

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

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

Note $G := N_{Sym(\Omega)}(T^k) \cong T^k.(Out(T) \times S_k)$ is a "diagonal type" primitive group.

Fawcett, 2013: $b(G) = 2$ only if $3 \leq k \leq |T| - 1$.

Lemma $b(G) = 2 \iff \exists S \subseteq T$, s.t. $|S| = k$ & $Hol(T)_{\{S\}} = 1$.

Probabilistic method II (H, 2024).

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

Then $b(G) = 2$ if

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

Theorem (H, 2024)

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

Theorem (Fawcett 2013; H, 2024)

P1 is done if G is "diagonal type" primitive.

§ 2

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

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

<u>Examples</u>

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

<u>P2</u> Classify G with $r(G) = 1$.

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

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

<u>Results</u>

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: G "diagonal type" primitive & $b(G) = 2$ ✓

<u>Theorem</u> (Freedman, H, Lee & Rekvényi, 2024+)

G "diagonal type" primitive & $b(G) > 2 \Rightarrow r(G) > 1$.

§ 3

Rank # G_α-orbits on Ω. (# G-orbits on Ω^2).

Example $G = GL_n(q)$, $\Omega = \mathbb{F}_q^n \setminus \{0\}$ $\Rightarrow$ rank $(G) = q$.

Note rank $(G) = 2$ $\iff$ G is 2-transitive
(classified via CFSG)

affine

almost simple

Burnside ($\sim$1900s)

P3 Classify rank 3 permutation groups.

Examples · $G = GL_n(3)$ on $\mathbb{F}_3^n \setminus \{0\}$. - imprimitive

· $G = S_n$, $\Omega = \{$2-subsets of $[n]\}$. - primitive

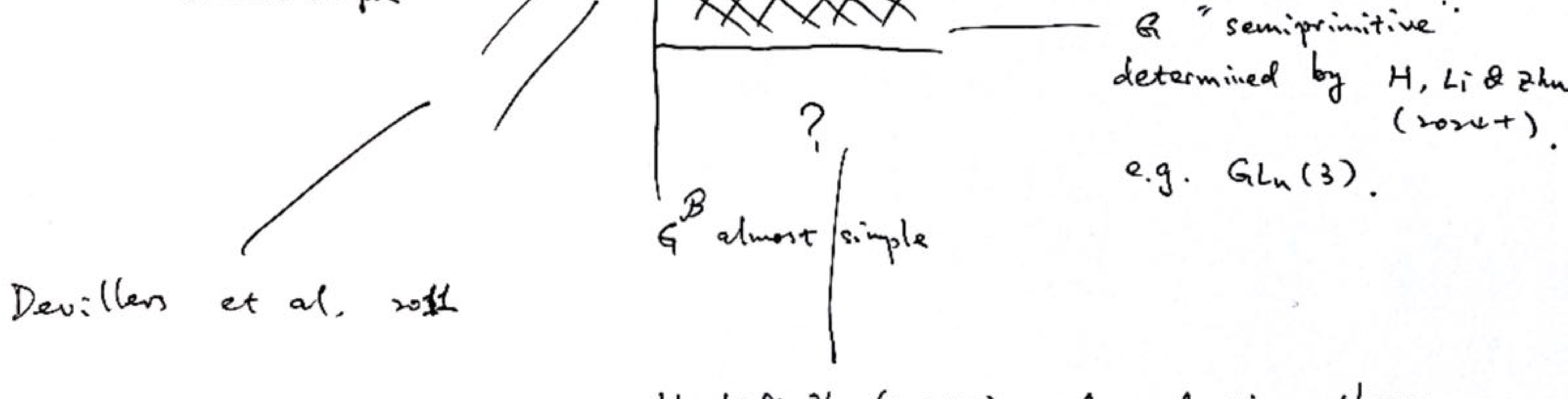
Primitive rank 3 groups: Classified 40yrs ago

(Liebeck, Saxl, ...).

Lemma Let G be an imprimitive rank 3 group. Then

- $\exists!$ non-trivial G-invariant partition $\mathcal{B} = B^G$ of Ω.
- $G^{\mathcal{B}}$ and G_B^B are 2-transitive.

e.g. $G = GL_n(3)$, $\Omega = \mathbb{F}_3^n \setminus \{0\}$ $\Rightarrow$ $\mathcal{B} = \{$1-spaces$\}$, $G^{\mathcal{B}} = PGL_n(3)$, $G_B^B = S_2$



H, Li & Zhu (2024+): A reduction theorem.

e.g. $(G_{(\mathcal{B})})^{(B)}$ is transitive on $B' \in \mathcal{B} \setminus \{B\}$.