Irredundant bases for the primitive actions of the symmetric and the alternating groups

Peiran Wu

University of St Andrews

SUSTech Group Theory Seminars
2022-10-24

Irredundant bases for the primitive actions of the symmetric and the alternating groups

Irredundant bases for the primitive actions of the symmetric and the alternating groups

The length

G : finite group

The **length of** G, denoted $\ell(G)$, is the largest $m \in \mathbb{N}$ for which there are $H_0, \ldots, H_m \leqslant G$ with

$$H_0 > H_1 > \cdots > H_m.$$

We can take $H_0 = G$ and $H_m = 1$.

Example

- If $G = 1$, then $\ell(G) = 0$.
- If $G = \mathrm{C}_n$, then $\ell(G) = \Omega(n)$ (# prime factors in n, counted with multiplicity).

In general, $\ell(G) \leqslant \Omega(|G|) \leqslant \log_2 |G|$.

Facts about the length

G : finite group

Lemma

1. *If* $H \leqslant G$, *then* $\ell(H) \leqslant \ell(G)$.
2. *If* $N \trianglelefteq G$, *then* $\ell(G) = \ell(N) + \ell(G/N)$.

Corollary

If G *is soluble, then* $\ell(G) = \Omega(|G|)$.

The length of S_n

We know the length of the symmetric groups exactly:

$$\ell(S_n) = \left\lfloor \frac{3n-1}{2} \right\rfloor - b_n \leqslant \frac{3}{2}n - 2 \ (n \geqslant 2),$$

where b_n is the number of ones in the base-2 expansion of n.

This was conjectured by Babai in 1986 and proved by Cameron, Solomon & Turull in 1989.

On the other hand,

$$\log_2(|\, S_n \,|) = \log_2(n!) \approx n \log_2 n.$$

The stabiliser length

Δ : finite set
G : permutation group on Δ, *i.e.* subgroup of $\mathrm{Sym}(\Delta)$

Given $\Sigma \subseteq \Delta$, let $G_{(\Sigma)}$ be the subgroup of elements in G that fixes Σ pointwise.

The "**stabiliser length**" $\ell_{\mathrm{S}}(G, \Delta)$ **of** G **on** Δ is the largest $m \in \mathbb{N}$ for which there are subsets $\Sigma_0, \ldots, \Sigma_m \subseteq \Delta$ with

$$G_{(\Sigma_0)} > G_{(\Sigma_1)} > \cdots > G_{(\Sigma_m)}.$$

Clearly, $\ell_{\mathrm{S}}(G, \Delta) \leqslant \ell(G)$.

The length and the stabiliser length

Δ : finite set

G : permutation group on Δ, *i.e.* subgroup of $\mathrm{Sym}(\Delta)$

Earlier we saw:

Lemma

1. *If* $H \leqslant G$, *then* $\ell(H) \leqslant \ell(G)$.
2. *If* $N \trianglelefteq G$, *then* $\ell(G) = \ell(N) + \ell(G/N)$.

There are analogous results for the stabiliser length:

Lemma

1. *If* $H \leqslant G$, *then* $\ell_{\mathrm{S}}(H, \Delta) \leqslant \ell_{\mathrm{S}}(G, \Delta)$.
2. *If* $N \trianglelefteq G$, *then* $\ell_{\mathrm{S}}(G, \Delta) \leqslant \ell_{\mathrm{S}}(N, \Delta) + \ell(G/N)$.

Examples of the stabiliser length

Δ : finite set

G : permutation group on Δ, *i.e.* subgroup of $\mathrm{Sym}(\Delta)$

Example

Let $\Delta := \{1, \ldots, n\}$.

- If $G = 1$, then $\ell_{\mathrm{S}}(G, \Delta) = 0$.
- If $G = \langle (1\ 2\ \cdots\ n) \rangle$, then $\ell_{\mathrm{S}}(G, \Delta) = 1$.
- If $G = \mathrm{Sym}(n)$, then $\ell_{\mathrm{S}}(G, \Delta) = n - 1$.
- If $G = \mathrm{Alt}(n)$, then $\ell_{\mathrm{S}}(G, \Delta) = n - 2$.

What about other faithful action of $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$? We will come back to this.

Irredundant bases for the primitive actions of the symmetric and the alternating groups

Bases

Δ : finite set
G : permutation group on Δ, *i.e.* subgroup of $\mathrm{Sym}(\Delta)$

A **base** for G is a subset Σ of Δ such that $G_{(\Sigma)} = 1$.

The minimum size of a base for G (on Δ) is called the **base size of** G and denoted $\mathrm{b}(G, \Delta)$.

Example (Burness, Guralnick & Saxl, 2011)

Let $G \leqslant \mathrm{Sym}(\Delta)$ is isomorphic to S_n to A_n. Suppose G is primitive[1] with point stabiliser H and H is primitive on $\{1, \ldots, n\}$. If $n \geqslant 13$, then $\mathrm{b}(G, \Delta) = 2$.

[1] A transitive permutation group G is primitive if and only if any point stabiliser is a maximal subgroup of G.

Motivation

Lemma

Suppose $\Sigma \subseteq \Delta$ is a base for G and $x, y \in G$. Then $x = y$ if and only if $\delta^x = \delta^y$ for all $\delta \in \Sigma$.

To determine an element, it suffices to know what the element does to a base. This helps optimise memory and storage when doing computations involving permutation groups.

How do we find a base?

1. Find a point δ_1 that G does not fix.
2. Find a point δ_2 that G_{δ_1} does not fix.
3. Iterate until $G_{\delta_1, \ldots, \delta_m} = 1$.
4. Return $\delta_1, \ldots, \delta_m$, which is a base.

Can this process be optimal? How large can m be?

Irredundant bases

An **irredundant base** for G is a base Σ whose elements can be ordered, say as $\delta_1, \ldots, \delta_m$, such that

$$G > G_{\delta_1} > G_{\delta_1,\delta_2} > \cdots > G_{\delta_1,\ldots,\delta_m} = 1.$$

The maximum size of an irredundant base for G (on Δ) is called the **maximum irredundant base size of** G and denoted $\mathrm{I}(G, \Delta)$.

Clearly, $\mathrm{b}(G, \Delta) \leqslant \mathrm{I}(G, \Delta) \leqslant \ell_{\mathrm{S}}(G, \Delta)$.

Connecting the dots

We have $\mathrm{I}(G, \Delta) \leqslant \ell_{\mathrm{S}}(G, \Delta)$.
Let's prove that $\mathrm{I}(G, \Delta) = \ell_{\mathrm{S}}(G, \Delta)$.

Let $m := \ell_{\mathrm{S}}(G, \Delta)$. Then there is a chain:

$$G_{(\Sigma_0)} > G_{(\Sigma_1)} > \cdots > G_{(\Sigma_m)}.$$

- Since m is maximal, $G_{(\Sigma_0)} = G$ and $G_{(\Sigma_m)} = 1$.
- Furthermore, the subset Σ_0 can be replaced with $\emptyset$.
- Since $G_{(\Sigma_i)}$ fixes Σ_{i-1} pointwise, we may replace Σ_i with $\Sigma_{i-1} \cup \{\delta_i\}$ for each $1 \leqslant i \leqslant m$.
- The sequence $\delta_1, \ldots, \delta_m$ is an irredundant base.

Thus, $\mathrm{I}(G, \Delta) \geqslant \ell_{\mathrm{S}}(G, \Delta)$. Therefore $\mathrm{I}(G, \Delta) = \ell_{\mathrm{S}}(G, \Delta)$.

Transitive permutation groups

Suppose G is transitive. Then:

- we can choose a point stabiliser $H < G$;
- for every $\Sigma \subseteq \Delta$, the pointwise stabiliser $G_{(\Sigma)}$ is an intersection of conjugates of H in G;
- write $\mathrm{I}(G, H) := \mathrm{I}(G, \Delta)$.

$\mathrm{I}(G, H)$ is equal to the largest $m \in \mathbb{N}$ for which there are $K_0, \ldots, K_m \leqslant G$ that are intersections of G-conjugates of H satisfying

$$K_0 > K_1 > \cdots > K_m.$$

We can take $K_0 = G$, $K_1 = H$ and $K_m = 1$.

Clearly, $\mathrm{I}(G, H) \leqslant \ell(H) + 1$.

Recap

We have seen the following so far:

- $\ell(G)$, the length of a group G.
- $\mathrm{b}(G, \Delta)$, the base size of a permutation group G on Δ.
- $\mathrm{I}(G, \Delta)$, the maximum irredundant base size of a permutation group G on Δ.
- $\mathrm{b}(G, \Delta) \leqslant \mathrm{I}(G, \Delta) \leqslant \ell(G)$.
- If G is transitive with point stabiliser H, then $\mathrm{I}(G, H) \leqslant \ell(H) + 1$.
- If $N \trianglelefteq G$, then $\mathrm{I}(G, \Delta) \leqslant \mathrm{I}(N, \Delta) + \ell(G/N)$.

We now focus on the symmetric and the alternating groups.

Irredundant bases for the primitive actions of the symmetric and the alternating groups

The symmetri/alternating groups

From now on, let G be S_n and A_n $(n \geqslant 5)$ acting primitively on a set Δ.

The following are known:

- $\ell(\mathrm{S}_n) = \left\lfloor \frac{3n-1}{2} \right\rfloor - b_n \leqslant \frac{3}{2}n - 2$.
- $\ell(\mathrm{A}_n) = \left\lfloor \frac{3n-3}{2} \right\rfloor - b_n \leqslant \frac{3}{2}n - 3$.
- $\mathrm{b}(G, \Delta) = 2$ if $n \geqslant 13$ and G is primitive on Δ with the point stabiliser primitive on $\{1, \ldots, n\}$.

What can we say about $\mathrm{I}(G, \Delta)$?

How different is $\mathrm{I}(G, \Delta)$ from $\mathrm{b}(G, \Delta)$, $\ell(H) + 1$, and $\ell(G)$?

Primitive actions of the symmetric/alternating groups

Theorem (Scott, 1980; Aschbacher & Scott, 1985; Liebeck, Praeger & Saxl, 1987)

Let G be S_n or A_n ($n \geqslant 5$). Every maximal subgroup (other than A_n) of G is one of the following (up to conjugacy):

- *(intransitive case)* $(S_m \times S_k) \cap G$ ($n = m + k$ and $m \neq k$),
- *(imprimitive case)* $(S_m \wr S_k) \cap G$ ($n = mk$, $m \geqslant 2$, $k \geqslant 2$),
- *(affine case)* $\mathrm{AGL}_d(p) \cap G$ ($n = p^d$, p prime),
- *(diagonal case)* $(T^k \cdot (\mathrm{Out}(T) \times S_k)) \cap G$ ($n = |T|^{k-1}$, T non-abelian simple),
- *(wreath case)* $(S_m \wr S_k) \cap G$ ($n = m^k$, $m \geqslant 5$, $k \geqslant 2$),
- *(almost simple case) an almost simple group acting primitively with socle $T < A_n$.*

In each of the last 4 cases, the maximal subgroup is primitive on $\{1, \ldots, n\}$.

Primitive actions of the alternating groups

Suppose $G = \mathrm{A}_n$. The point stabiliser H is a maximal subgroup of G. We make the following distinction of cases:

1. $H = \mathrm{A}_n \cap M$, where M is a maximal subgroup of S_n. Then the action of A_n with point stabiliser H is the restriction of the action of S_n with point stabiliser M. By previous lemmas,

$$\mathrm{I}(\mathrm{S}_n, M) - 1 \leqslant \mathrm{I}(\mathrm{A}_n, H) \leqslant \mathrm{I}(\mathrm{S}_n, M).$$

2. all other cases, *e.g.* $n = 2^d$ and $H = \mathrm{AGL}_d(2) < \mathrm{A}_n$.

Building a chain with intersections of conjugates of H

Let $G = S_n$ $(n \geqslant 5)$ and $H \neq A_n$ a maximal subgroup of S_n. Let J be an intersection of S_n-conjugates of H.

Which proper subgroups of J can be written as $J \cap J^x$ for some $x \in S_n$?

Once we have an answer, we can continue to find $J \cap J^x \cap J^{x'}$ or replace J with $J \cap J^x$ and ask the above question again.

The affine case

- Let $G = \mathrm{S}_n$ where $n = p^d$ with $d \geqslant 2$ and $p \geqslant 3$.
- Let $V = \mathbb{F}_p^d$ and identify $G \cong \mathrm{Sym}(V)$. Let $H = \mathrm{AGL}_d(p) = V \cdot \mathrm{GL}(V)$.
- Let K be the subgroup of $\mathrm{GL}(V)$ that stabilises setwise some proper,non-trivial subspace $W \subseteq V$.
- Let $\alpha \in \mathbb{F}_p^\times \setminus \{1\}$ be a primitive element and define a function $x : V \to V$ with

$$\mathbf{v}^x := \begin{cases} \alpha\mathbf{v}, & \text{if } \mathbf{v} \in W, \\ \mathbf{v}, & \text{otherwise} \end{cases}$$

- Then $K = H \cap H^x$.

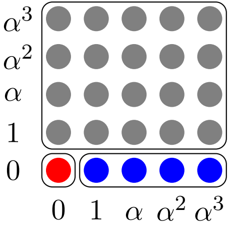

Figure: The three orbits of a subspace stabiliser in $\mathrm{GL}_2(\mathbb{F}_5)$

Primitive actions of the symmetric groups (affine case)

G	S_n	
H	$AGL_d(p)$ $(n = p^d,\ p$ prime $> 2)$	
	$d = 1$	$d \geqslant 2$
$b(G,H)$	2 †1	
$I(G,H)$	$\Omega(p-1) - \epsilon + 2$ †2	$\geqslant \frac{d(d-1)}{2} + (\Omega(p-1) - \epsilon)d$ †2
$\ell(H) + 1$	$\Omega(p-1) + 2$	$\geqslant \frac{d(d-1)}{2} + \Omega(p-1)d$
$\ell(G)$	$\approx \frac{3}{2}p^d$	

If $p = 5$, then $\epsilon = 1$; otherwise, $\epsilon = 0$.

†1 except when $n = 5$ or 9; Burness, Guralnick & Saxl, 2011
†2 W.

Primitive actions of the symmetric groups (intransitive and imprimitive cases)

G	S_n	
H	$S_m \times S_k$ $(n = m + k,$ $m \neq k)$	$S_m \wr S_k$ $(n = mk,$ $m \geqslant 2,\ k \geqslant 2)$
$b(G, H)$	$\geqslant \log n$ †1	$\leqslant \max\{5, \lceil \log_k(m+3) \rceil\}$ †3
$I(G, H)$	$n - 1$ if $m \mid n$; $n - 2$ otherwise †2	$\geqslant (m-1)k$ (exact?)
$\ell(H) + 1$	$\leqslant \frac{3}{2}n - 4$	$\leqslant \frac{3}{2}(m-1)k + k - 1$
$\ell(G)$	$\approx \frac{3}{2}n$	

†1 Burness, Guralnick & Saxl, 2011

†2 Gill & Lodà, 2021 (arXiv)

†3 Morris & Spiga, 2021

To-dos

- $\mathrm{I}(\mathrm{S}_n, H)$ for the remaining maximal groups H.
- $\mathrm{I}(\mathrm{A}_n, H)$ where H is not induced from a maximal subgroup of S_n.
- Bounds on $\mathrm{I}(\mathrm{S}_n, H)$ and $\mathrm{I}(\mathrm{A}_n, H)$ in terms of n.
- Bounds on $\mathrm{I}(\mathrm{S}_n, H)$ and $\mathrm{I}(\mathrm{A}_n, H)$ in terms of $|\Delta| =$ the index of H.