Minimal degree and base size of permutation groups

Fabio Mastrogiacomo

Università degli Studi di Milano-Bicocca
Università degli Studi di Pavia

June 26, 2025

Bases of permutation groups

In this talk, $G \leq \mathrm{Sym}(\Omega)$ is a finite permutation group acting on a finite set Ω.

Bases of permutation groups

In this talk, $G \leq \mathrm{Sym}(\Omega)$ is a finite permutation group acting on a finite set Ω.

We are interested in two invariant of a permutation group. The *base size* and the *minimal degree*.

Bases of permutation groups

In this talk, $G \leq \mathrm{Sym}(\Omega)$ is a finite permutation group acting on a finite set Ω.

We are interested in two invariant of a permutation group. The *base size* and the *minimal degree*.

Definition

A base for G is a sequence of points $(\omega_1, \ldots, \omega_\ell)$ of Ω such that the pointwise stabilizer of the sequence is trivial, i.e.

$$G_{\omega_1,\ldots,\omega_\ell} = \bigcap_{i=1}^{\ell} G_{\omega_i} = 1.$$

Bases of permutation groups

In this talk, $G \leq \mathrm{Sym}(\Omega)$ is a finite permutation group acting on a finite set Ω.

We are interested in two invariant of a permutation group. The *base size* and the *minimal degree*.

Definition

A base for G is a sequence of points $(\omega_1, \ldots, \omega_\ell)$ of Ω such that the pointwise stabilizer of the sequence is trivial, i.e.

$$G_{\omega_1,\ldots,\omega_\ell} = \bigcap_{i=1}^{\ell} G_{\omega_i} = 1.$$

The base size of G, $b(G)$, is the minimal cardinality of a base.

Bases of permutation groups

Bases are interesting because each element of G is uniquely determined by its action on a base.

Bases of permutation groups

Bases are interesting because each element of G is uniquely determined by its action on a base.

Indeed, if $(\omega_1, \ldots, \omega_\ell)$ is a base for G and $g, h \in G$, then

$$\omega_i^g = \omega_i^h \ \forall i \in \{1, \ldots, \ell\} \iff gh^{-1} \in \bigcap_{i=1}^{\ell} G_{\omega_i} \iff g = h.$$

Bases are interesting because each element of G is uniquely determined by its action on a base.

Indeed, if $(\omega_1, \ldots, \omega_\ell)$ is a base for G and $g, h \in G$, then

$$\omega_i^g = \omega_i^h \ \forall i \in \{1, \ldots, \ell\} \iff gh^{-1} \in \bigcap_{i=1}^{\ell} G_{\omega_i} \iff g = h.$$

If you want to "store" a permutation group into a computer system (GAP, Magma), it is sufficient to know a base for it, and the action on such a base.

Bases are interesting because each element of G is uniquely determined by its action on a base.

Indeed, if $(\omega_1, \ldots, \omega_\ell)$ is a base for G and $g, h \in G$, then

$$\omega_i^g = \omega_i^h \; \forall i \in \{1, \ldots, \ell\} \iff gh^{-1} \in \bigcap_{i=1}^{\ell} G_{\omega_i} \iff g = h.$$

If you want to "store" a permutation group into a computer system (GAP, Magma), it is sufficient to know a base for it, and the action on such a base.

This is good, because usually a base is very small compared with the degree of the group.

Example

- $b(S_n) = n - 1$.
- $b(A_n) = n - 2$
- $b(D_{2n}) = 2$.
- Let $V = \mathbb{F}_q^d$ and let $G = GL(V)$ acting on V. Then, $(v_1, \ldots, v_k)$ is a base for G if and only if it contains a basis of the vector space V. Thus, $b(G) = d$.

Minimal degree

Definition

The minimal degree of a permutation group G, denoted with $\mu(G)$, is the cardinality of the minimum support of a non-identity element:

$$\mu(G) = \min_{g \in G \setminus \{1\}} |\mathrm{supp}(g)|.$$

Minimal degree

Example

- $\mu(S_n) = 2$
- $\mu(A_n) = 3$
- $\mu(D_{2n}) = \begin{cases} n-1 \text{ if } n \text{ odd}, \\ n-2 \text{ if } n \text{ even}. \end{cases}$
- $\mu(\mathrm{GL}(d,q)) = q^{d-1}(q-1)$.

The product of base size and minimal degree

These two invariants have been always studied separately.

The product of base size and minimal degree

These two invariants have been always studied separately.

There are few results in the literature that treat these two together.

The product of base size and minimal degree

These two invariants have been always studied separately.

There are few results in the literature that treat these two together.

We now consider the product of these two invariants.

The product of base size and minimal degree

These two invariants have been always studied separately.

There are few results in the literature that treat these two together.

We now consider the product of these two invariants.

Lemma

Let G be a transitive permutation group of degree n. Then,

$$\mu(G)b(G) \geq n.$$

The product of base size and minimal degree

These two invariants have been always studied separately.

There are few results in the literature that treat these two together.

We now consider the product of these two invariants.

Lemma

Let G be a transitive permutation group of degree n. Then,

$$\mu(G)b(G) \geq n.$$

What about an upper bound?

The product of base size and minimal degree

These two invariants have been always studied separately.

There are few results in the literature that treat these two together.

We now consider the product of these two invariants.

Lemma

Let G be a transitive permutation group of degree n. Then,

$$\mu(G)b(G) \geq n.$$

What about an upper bound?

Of course both the minimal degree and the base size are at most n, and so

$$\mu(G)b(G) \leq n^2.$$

Primitive groups

Can we say something better then $\mu(G)b(G) \leq n^2$?

Primitive groups

Can we say something better then $\mu(G)b(G) \leq n^2$?

Yes, for primitive groups!

Primitive groups

Can we say something better then $\mu(G)b(G) \leq n^2$?

Yes, for primitive groups!

Definition

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group. A nonempty subset $\Delta \subseteq \Omega$ is called a block if, for every $g \in G$, $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$.
The block Δ is called trivial if $\Delta = \Omega$ or Δ is a singleton.
The group G is called primitive if it does not admit non-trivial blocks.

The product of base size and minimal degree

Theorem (M., 2024)

Let G be a primitive permutation group of degree n, with $(G, n) \neq (\mathrm{M}_{24}, 24)$. Then,

$$\mu(G)b(G) \leq n \log n.$$

The bound is asymptotically best possible, up to a multiplicative constant.

The product of base size and minimal degree

We have a result about primitive groups.

The product of base size and minimal degree

We have a result about primitive groups.

This is really common in the literature.

The product of base size and minimal degree

We have a result about primitive groups.

This is really common in the literature.

Can we say something similar for transitive (non-primitive) groups?

The product of base size and minimal degree

We have a result about primitive groups.

This is really common in the literature.

Can we say something similar for transitive (non-primitive) groups?

Surprising, we can not!

The product of base size and minimal degree

We have a result about primitive groups.

This is really common in the literature.

Can we say something similar for transitive (non-primitive) groups?

Surprising, we can not!

Actually, the opposite situation holds.

The product of base size and minimal degree

Recall that if G is a permutation group of degree n, then

$$\mu(G)b(G) \leq n^2.$$

The product of base size and minimal degree

Recall that if G is a permutation group of degree n, then

$$\mu(G)b(G) \leq n^2.$$

Theorem (Guerra, Maróti, M., Spiga; 2025+)

For every $\varepsilon > 0$, there exists a transitive permutation group G of degree n with

$$\mu(G)b(G) \geq n^{2-\varepsilon}.$$

THANK YOU!