Regular suborbits of finite primitive groups

Hong Yi Huang

University of Bristol

Groups, Graphs and Combinatorics, SUSTech

14 November 2021

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.
- G is 2-transitive: $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ are the only suborbits.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.
- G is 2-transitive: $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ are the only suborbits.

Recall: G is called primitive if G_α is maximal in G.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.
- G is 2-transitive: $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ are the only suborbits.

Recall: G is called primitive if G_α is maximal in G.

From now, we assume G is primitive.

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.
- G is 2-transitive: $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ are the only suborbits.

Recall: G is called primitive if G_α is maximal in G.

From now, we assume G is primitive.

- G has a suborbit $\mathcal{O} \neq \{\alpha\}$ with $|\mathcal{O}| \leqslant 5$: classified ✓

Suborbits

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group and $H = G_\alpha$. Then an orbit of H is called a suborbit of G at α.

Examples

- $\{\alpha\}$ is always a suborbit.
- $G = S_n$, $\Omega = \{1, \ldots, n\}$ and $\alpha = 1$: $\{1\}$ and $\{2, \ldots, n\}$ are suborbits.
- G is 2-transitive: $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ are the only suborbits.

Recall: G is called primitive if G_α is maximal in G.

From now, we assume G is primitive.

- G has a suborbit $\mathcal{O} \neq \{\alpha\}$ with $|\mathcal{O}| \leqslant 5$: classified ✓

Question: How large can a suborbit be?

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Question: When do we have a regular suborbit?

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Question: When do we have a regular suborbit?

Example

Consider the action of $G = D_{2n}$ $(n > 2)$ on $\{1, \ldots, n\}$. Then

- $G_\alpha \cong C_2$;

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Question: When do we have a regular suborbit?

Example

Consider the action of $G = D_{2n}$ $(n > 2)$ on $\{1, \dots, n\}$. Then

- $G_\alpha \cong C_2$;
- G is primitive iff n is a prime;

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Question: When do we have a regular suborbit?

Example

Consider the action of $G = D_{2n}$ $(n > 2)$ on $\{1, \ldots, n\}$. Then

- $G_\alpha \cong C_2$;
- G is primitive iff n is a prime;
- if $\alpha = 1$, then $\{2, n\}$ is a regular suborbit.

Regular suborbits

Regular suborbit: A suborbit with length $|H|$ (largest possible length).

Question: When do we have a regular suborbit?

Example

Consider the action of $G = D_{2n}$ $(n > 2)$ on $\{1, \dots, n\}$. Then

- $G_\alpha \cong C_2$;
- G is primitive iff n is a prime;
- if $\alpha = 1$, then $\{2, n\}$ is a regular suborbit.

Note: G has a regular suborbit $\iff$ $H \cap H^g = 1$ for some $g \in G$.

Base-two groups

Base: A subset Δ of Ω with trivial pointwise stabiliser $G_{(\Delta)}$ in G.

Base-two groups

Base: A subset Δ of Ω with trivial pointwise stabiliser $G_{(\Delta)}$ in G.

Examples

- $G = \mathrm{GL}(V)$, $\Omega = V$: Δ contains a basis of V;

Base-two groups

Base: A subset Δ of Ω with trivial pointwise stabiliser $G_{(\Delta)}$ in G.

Examples

- $G = \mathrm{GL}(V)$, $\Omega = V$: Δ contains a basis of V;
- $G = D_{2n}$ $(n > 2)$, $\Omega = \{1, \dots, n\}$: $\Delta = \{1, 2\}$.

Base-two groups

Base: A subset Δ of Ω with trivial pointwise stabiliser $G_{(\Delta)}$ in G.

Examples

- $G = \mathrm{GL}(V)$, $\Omega = V$: Δ contains a basis of V;
- $G = D_{2n}$ $(n > 2)$, $\Omega = \{1, \ldots, n\}$: $\Delta = \{1, 2\}$.

Note: G has a regular suborbit $\iff$ G has a base of size 2 $\iff$ $G_{\alpha\beta} = 1$.

Base-two groups

Base: A subset Δ of Ω with trivial pointwise stabiliser $G_{(\Delta)}$ in G.

Examples

- $G = \mathrm{GL}(V)$, $\Omega = V$: Δ contains a basis of V;
- $G = D_{2n}$ $(n > 2)$, $\Omega = \{1, \ldots, n\}$: $\Delta = \{1, 2\}$.

Note: G has a regular suborbit $\iff$ G has a base of size 2 $\iff$ $G_{\alpha\beta} = 1$.

Problem

Classify the finite primitive groups with a base of size 2.

Affine groups

The **O'Nan-Scott Theorem** divides finite primitive groups into 5 types.

Affine groups

The **O'Nan-Scott Theorem** divides finite primitive groups into 5 types.

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

Affine groups

The **O'Nan-Scott Theorem** divides finite primitive groups into 5 types.

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

Problem

Determine the pairs (H, V), where H is a finite group, V is a faithful irreducible $\mathbb{F}_p H$-module and H has a regular orbit on V.

Affine groups

The **O'Nan-Scott Theorem** divides finite primitive groups into 5 types.

Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^d$ and $H \leqslant \mathrm{GL}(V)$ irreducible.

Problem

Determine the pairs (H, V), where H is a finite group, V is a faithful irreducible $\mathbb{F}_pH$-module and H has a regular orbit on V.

Partial results when H quasisimple:

- $(|H|, p) = 1$: **Goodwin 2000; Köhler & Pahlings 2001** ✓
- $(|H|, p) \neq 1$: **Fawcett et al. 2016/19; Lee 2020/21**

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓
- G_0 Lie type: Partial results (e.g. G_0 classical and $H \in \mathcal{S}$)

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓
- G_0 Lie type: Partial results (e.g. G_0 classical and $H \in \mathcal{S}$)

Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, where T is non-abelian simple, P is primitive or $k = 2$ and $P = 1$.

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓
- G_0 Lie type: Partial results (e.g. G_0 classical and $H \in \mathcal{S}$)

Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, where T is non-abelian simple, P is primitive or $k = 2$ and $P = 1$.

Theorem (Fawcett 2013)

If $P \neq A_k$ or S_k, then G has a regular suborbit.

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓
- G_0 Lie type: Partial results (e.g. G_0 classical and $H \in \mathcal{S}$)

Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, where T is non-abelian simple, P is primitive or $k = 2$ and $P = 1$.

Theorem (Fawcett 2013)

If $P \neq A_k$ or S_k, then G has a regular suborbit.

Twisted wreath: $G = T^k{:}P$, where P is transitive.

Other results

Almost simple: $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

- H soluble: **Burness 2021** ✓
- G_0 alternating or sporadic: **James 2006; Burness et al. 2010/11** ✓
- G_0 Lie type: Partial results (e.g. G_0 classical and $H \in \mathcal{S}$)

Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, where T is non-abelian simple, P is primitive or $k = 2$ and $P = 1$.

Theorem (Fawcett 2013)

If $P \neq A_k$ or S_k, then G has a regular suborbit.

Twisted wreath: $G = T^k{:}P$, where P is transitive.

Theorem (Fawcett 2021+)

P quasiprimitive $\implies$ G has a regular suborbit.

Product-type groups

Product type: $T^k \leqslant G \leqslant L \wr P$, where $T = \mathrm{soc}(L)$ and $P \leqslant S_k$.

Note: G induces L and P in its product action.

Product-type groups

Product type: $T^k \leqslant G \leqslant L \wr P$, where $T = \mathrm{soc}(L)$ and $P \leqslant S_k$.

Note: G induces L and P in its product action.

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff

$$\#\ \text{regular suborbits of } L \geqslant \text{the } \textit{distinguishing number} \text{ of } P.$$

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

- **Chen & H 2021+:** a general method using inclusion-exclusion

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

- **Chen & H 2021+:** a general method using inclusion-exclusion
- Probabilistic method: lower bounds for $r(G)$

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

- **Chen & H 2021+:** a general method using inclusion-exclusion
- Probabilistic method: lower bounds for $r(G)$

Problem

Classify the finite primitive groups G with $r(G) = 1$.

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

- **Chen & H 2021+:** a general method using inclusion-exclusion
- Probabilistic method: lower bounds for $r(G)$

Problem

Classify the finite primitive groups G with $r(G) = 1$.

Burness & H 2021+: G almost simple, H soluble and $r(G) = 1$ ✓

Number of regular suborbits

Let $r(G)$ be the number of regular suborbits of G (at α).

Question: Can we determine $r(G)$?

- **Chen & H 2021+:** a general method using inclusion-exclusion
- Probabilistic method: lower bounds for $r(G)$

Problem

Classify the finite primitive groups G with $r(G) = 1$.

Burness & H 2021+: G almost simple, H soluble and $r(G) = 1$ ✓

e.g. $G = \mathrm{PGL}_2(q)$ and $H = D_{2(q-1)}$.

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing number $D(G)$: The minimal size of a distinguishing partition.

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing number $D(G)$: The minimal size of a distinguishing partition.

Examples

- G is any group and $|\Pi| = |\Omega|$;

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing number $D(G)$: The minimal size of a distinguishing partition.

Examples

- G is any group and $|\Pi| = |\Omega|$;
- $D(G) = 1 \iff G = 1$;

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing number $D(G)$: The minimal size of a distinguishing partition.

Examples

- G is any group and $|\Pi| = |\Omega|$;
- $D(G) = 1 \iff G = 1$;
- G is regular, $\Pi = \{\{\alpha\}, \Omega \setminus \{\alpha\}\}$ and so $D(G) = 2$;

Distinguishing numbers

Distinguishing partition: A partition $\Pi = \{\pi_1, \ldots, \pi_m\}$ of Ω such that

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

Distinguishing number $D(G)$: The minimal size of a distinguishing partition.

Examples

- G is any group and $|\Pi| = |\Omega|$;
- $D(G) = 1 \iff G = 1$;
- G is regular, $\Pi = \{\{\alpha\}, \Omega \setminus \{\alpha\}\}$ and so $D(G) = 2$;
- $D(S_n) = n$ and $D(A_n) = n - 1$.

Product-type groups

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff $r(L) \geqslant D(P)$.

Product-type groups

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff $r(L) \geqslant D(P)$.

Observations:

- $L \wr S_k$ has a regular suborbit iff $r(L) \geqslant k$;

Product-type groups

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff $r(L) \geqslant D(P)$.

Observations:

- $L \wr S_k$ has a regular suborbit iff $r(L) \geqslant k$;
- If $r(L) = 1$ and $P \neq 1$, then $L \wr P$ has no regular suborbit.

Product-type groups

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff $r(L) \geqslant D(P)$.

Observations:

- $L \wr S_k$ has a regular suborbit iff $r(L) \geqslant k$;
- If $r(L) = 1$ and $P \neq 1$, then $L \wr P$ has no regular suborbit.

Theorem (Burness & H, in progress)

Let $r = r(L)$, $P \leqslant S_k$ with $D = D(P)$. Then

$$r(L \wr P) = \frac{1}{|P|} \sum_{m=D}^{k} m! \binom{r}{m} D(P, m),$$

where $D(P, m)$ is the number of distinguishing partitions into m parts.

Product-type groups

Theorem (Bailey & Cameron 2013)

$L \wr P$ has a regular suborbit iff $r(L) \geqslant D(P)$.

Observations:

- $L \wr S_k$ has a regular suborbit iff $r(L) \geqslant k$;
- If $r(L) = 1$ and $P \neq 1$, then $L \wr P$ has no regular suborbit.

Theorem (Burness & H, in progress)

Let $r = r(L)$, $P \leqslant S_k$ with $D = D(P)$. Then

$$r(L \wr P) = \frac{1}{|P|} \sum_{m=D}^{k} m! \binom{r}{m} D(P, m),$$

where $D(P, m)$ is the number of distinguishing partitions into m parts.

In particular, we have $r(L \wr S_k) = \binom{r}{k}$.

An Example

Suppose $P = C_p$ for some prime p and $r = r(L)$.

An Example

Suppose $P = C_p$ for some prime p and $r = r(L)$.

Note:

- $D(P) = 2$;

An Example

Suppose $P = C_p$ for some prime p and $r = r(L)$.

Note:

- $D(P) = 2$;
- Any partition other than Ω is a distinguishing partition for P.

An Example

Suppose $P = C_p$ for some prime p and $r = r(L)$.

Note:

- $D(P) = 2$;
- Any partition other than Ω is a distinguishing partition for P.

This implies

$$D(P, m) = S(p, m)$$

is the *Stirling number of the second kind*.

An Example

Suppose $P = C_p$ for some prime p and $r = r(L)$.

Note:

- $D(P) = 2$;
- Any partition other than Ω is a distinguishing partition for P.

This implies

$$D(P, m) = S(p, m)$$

is the *Stirling number of the second kind*. Thus,

$$|P| r(L \wr P) = \sum_{m=2}^{p} m! \binom{m}{r} S(p, m) = r^p - r$$

and therefore $r(L \wr P) = (r^p - r)/p$.

Future work

Existence of regular suborbit:

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;
- Diagonal groups $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$ with $P = A_k$ or S_k.

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;
- Diagonal groups $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$ with $P = A_k$ or S_k.

Theorem (Fawcett 2013)

If $P = A_k$ or S_k, then G has a regular suborbit only if $2 < k < |T|$.

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;
- Diagonal groups $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$ with $P = A_k$ or S_k.

Theorem (Fawcett 2013)

If $P = A_k$ or S_k, then G has a regular suborbit only if $2 < k < |T|$.

Number of regular suborbits:

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;
- Diagonal groups $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$ with $P = A_k$ or S_k.

Theorem (Fawcett 2013)

If $P = A_k$ or S_k, then G has a regular suborbit only if $2 < k < |T|$.

Number of regular suborbits:

- Unique regular suborbit;

Future work

Existence of regular suborbit:

- Almost simple primitive groups of Lie type;
- General product-type groups;
- Diagonal groups $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$ with $P = A_k$ or S_k.

Theorem (Fawcett 2013)

If $P = A_k$ or S_k, then G has a regular suborbit only if $2 < k < |T|$.

Number of regular suborbits:

- Unique regular suborbit;
- Asymptotic results.

Thank you!