

Bases, distinguishing partitions and probabilistic methods

Hong Yi Huang

Discrete Structures and Algorithms Seminar

University of Melbourne

18 August 2022



Automorphisms

Throughout, everything is finite.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\text{Aut}(\Gamma)$: The group of all the automorphisms.

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\text{Aut}(\Gamma)$: The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \text{Aut}(\Gamma) \cong S_n$

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\text{Aut}(\Gamma)$: The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \text{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n \ (n \geq 3) \implies \text{Aut}(\Gamma) \cong D_{2n}$

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\text{Aut}(\Gamma)$: The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \text{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n (n \geq 3) \implies \text{Aut}(\Gamma) \cong D_{2n}$

How can we “break” the symmetries of a graph?

Automorphisms

Throughout, everything is finite.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a simple graph.

Automorphism: $g \in \text{Sym}(V\Gamma)$ such that $v \sim w \iff v^g \sim w^g$.

Automorphism group $\text{Aut}(\Gamma)$: The group of all the automorphisms.

- $\Gamma = \mathbf{K}_n \implies \text{Aut}(\Gamma) \cong S_n$
- $\Gamma = \mathbf{C}_n (n \geq 3) \implies \text{Aut}(\Gamma) \cong D_{2n}$

How can we “break” the symmetries of a graph?

- Colouring vertices (setwise)
- Fixing vertices (pointwise)

Part I

Distinguishing numbers for groups and graphs

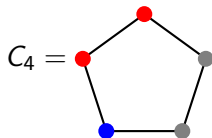
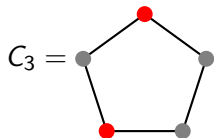
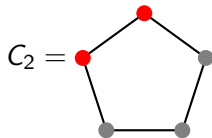
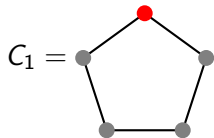
Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

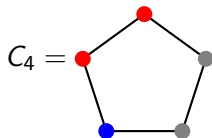
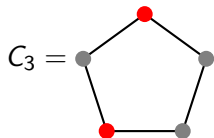
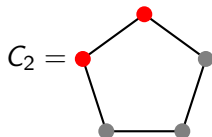
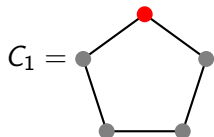
Which automorphisms preserve the following colourings?



Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?

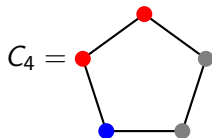
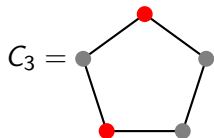
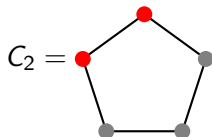
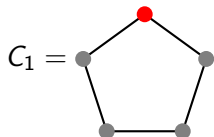


- $\text{Aut}(\Gamma, C_1) \cong \text{Aut}(\Gamma, C_2) \cong \text{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\text{Aut}(\Gamma, C_4) = 1$.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



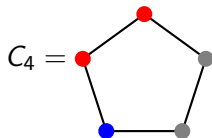
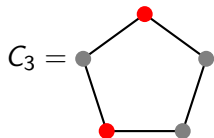
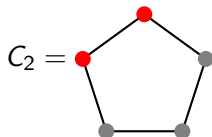
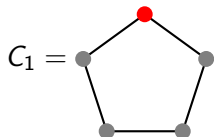
- $\text{Aut}(\Gamma, C_1) \cong \text{Aut}(\Gamma, C_2) \cong \text{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\text{Aut}(\Gamma, C_4) = 1$.

Distinguishing colouring: A colouring C of Γ such that $\text{Aut}(\Gamma, C) = 1$.

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



- $\text{Aut}(\Gamma, C_1) \cong \text{Aut}(\Gamma, C_2) \cong \text{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\text{Aut}(\Gamma, C_4) = 1$.

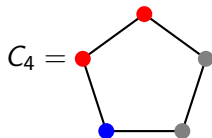
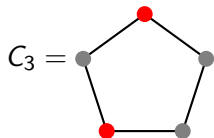
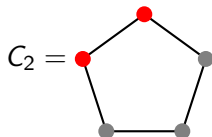
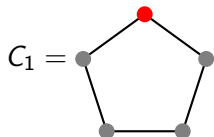
Distinguishing colouring: A colouring C of Γ such that $\text{Aut}(\Gamma, C) = 1$.

Distinguishing number $D(\Gamma)$: The minimal number of colours in a distinguishing colouring of Γ .

Colourings

Consider $\Gamma = \mathbf{C}_5$, where we have $\text{Aut}(\Gamma) \cong D_{10}$.

Which automorphisms preserve the following colourings?



- $\text{Aut}(\Gamma, C_1) \cong \text{Aut}(\Gamma, C_2) \cong \text{Aut}(\Gamma, C_3) \cong \mathbb{Z}_2$, and $\text{Aut}(\Gamma, C_4) = 1$.

Distinguishing colouring: A colouring C of Γ such that $\text{Aut}(\Gamma, C) = 1$.

Distinguishing number $D(\Gamma)$: The minimal number of colours in a distinguishing colouring of Γ . (e.g. $D(\mathbf{C}_5) = 3$.)

Some results

Klavžar, Wong & Zhu, 2006:

$D(\Gamma) \leq$ the maximal degree of Γ , unless $\Gamma \cong \mathbf{K}_n$, $\mathbf{K}_{n,n}$ or \mathbf{C}_5 .

Some results

Klavžar, Wong & Zhu, 2006:

$D(\Gamma) \leq$ the maximal degree of Γ , unless $\Gamma \cong \mathbf{K}_n$, $\mathbf{K}_{n,n}$ or \mathbf{C}_5 .

Remark. $D(\mathbf{K}_n) = n$; $D(\mathbf{K}_{n,n}) = n + 1$; $D(\mathbf{C}_n) = 2$ if $n \geq 6$.

Some results

Klavžar, Wong & Zhu, 2006:

$D(\Gamma) \leq$ the maximal degree of Γ , unless $\Gamma \cong \mathbf{K}_n$, $\mathbf{K}_{n,n}$ or \mathbf{C}_5 .

Remark. $D(\mathbf{K}_n) = n$; $D(\mathbf{K}_{n,n}) = n + 1$; $D(\mathbf{C}_n) = 2$ if $n \geq 6$.

Praeger, 1993; Devillers, Harper & Morgan, 2019:

If Γ is **2-arc-transitive**, then one of the following holds.

- Γ is complete;
- Γ is bipartite;
- $D(\Gamma) = 2$;
- $\Gamma \cong \mathbf{C}_5$, $\mathbf{K}_3 \square \mathbf{K}_3$, Petersen or its complement.

Partitions

Note. A colouring is a partition of vertices.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Remark. $D(\Gamma) = D(\text{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geq 6$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Remark. $D(\Gamma) = D(\text{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geq 6$.

Examples

- $D(S_n) = n$

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Remark. $D(\Gamma) = D(\text{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geq 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Remark. $D(\Gamma) = D(\text{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geq 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.
- $D(G) = 1 \iff G = 1$.

Partitions

Note. A colouring is a partition of vertices.

Let $G \leq \text{Sym}(\Omega)$ be a **transitive** permutation group of degree n .

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

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

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

Remark. $D(\Gamma) = D(\text{Aut}(\Gamma))$, so $D(D_{10}) = 3$ and $D(D_{2n}) = 2$ for $n \geq 6$.

Examples

- $D(S_n) = n$; $D(A_n) = n - 1$.
- $D(G) = 1 \iff G = 1$.
- $G \neq 1$ is regular $\implies D(G) = 2$.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- G has a regular orbit on the power set $\mathcal{P}(\Omega)$ of Ω ;
- $\exists \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- G has a regular orbit on the power set $\mathcal{P}(\Omega)$ of Ω ;
- $\exists \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G .

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- G has a regular orbit on the power set $\mathcal{P}(\Omega)$ of Ω ;
- $\exists \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G .

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- G has a regular orbit on the power set $\mathcal{P}(\Omega)$ of Ω ;
- $\exists \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G .

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$, with 43 exceptions of degree ≤ 32 .

Primitive groups

Note. The following statements are equivalent.

- $D(G) = 2$;
- G has a regular orbit on the power set $\mathcal{P}(\Omega)$ of Ω ;
- $\exists \Delta \subseteq \Omega$ such that $G_{\{\Delta\}} = 1$.

G is called **primitive** if G_α is maximal in G .

Theorem (Cameron, Neumann & Saxl, 1984; Seress, 1997)

$G \neq A_n, S_n$ primitive $\implies D(G) = 2$, with 43 exceptions of degree ≤ 32 .

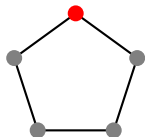
Dolfi, 2000: $D(G) \leq 4$ for each exception.

Part II

Bases for permutation groups

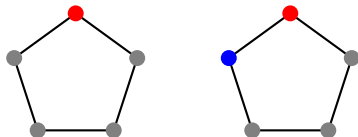
Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



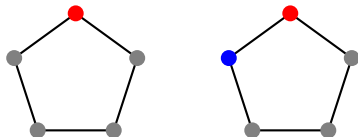
Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



Fixing sets

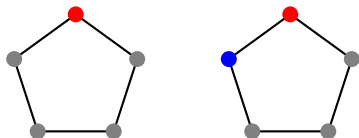
Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?

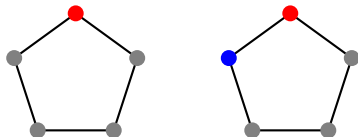


Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\text{fix}(\Gamma)$: The minimal size of such a Δ .

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



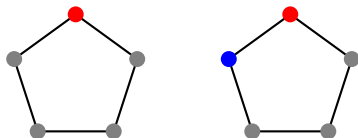
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\text{fix}(\Gamma)$: The minimal size of such a Δ .

- $\Gamma = \mathbf{K}_n \implies \text{fix}(\Gamma) = n - 1$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



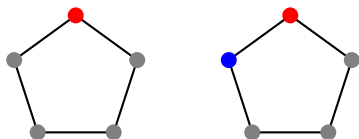
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\text{fix}(\Gamma)$: The minimal size of such a Δ .

- $\Gamma = \mathbf{K}_n \implies \text{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \text{fix}(\Gamma) = 2$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



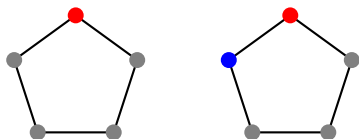
Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\text{fix}(\Gamma)$: The minimal size of such a Δ .

- $\Gamma = \mathbf{K}_n \implies \text{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \text{fix}(\Gamma) = 2$.
- $\text{Aut}(\Gamma) = 1 \iff \text{fix}(\Gamma) = 0$.

Fixing sets

Which automorphisms of $\Gamma = \mathbf{C}_5$ survive if we “pin” each coloured vertex?



Fixing (determining) set: A subset $\Delta \subseteq V\Gamma$ such that $\bigcap_{\alpha \in \Delta} \text{Aut}(\Gamma)_\alpha = 1$.

Fixing (determining) number $\text{fix}(\Gamma)$: The minimal size of such a Δ .

- $\Gamma = \mathbf{K}_n \implies \text{fix}(\Gamma) = n - 1$.
- $\Gamma = \mathbf{C}_n \implies \text{fix}(\Gamma) = 2$.
- $\text{Aut}(\Gamma) = 1 \iff \text{fix}(\Gamma) = 0$.
- $D(\Gamma) \leq \text{fix}(\Gamma) + 1$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.
- $G = D_{2n} (n \geq 3), \Omega = \{1, \dots, n\} \implies b(G) = 2$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.
- $G = D_{2n} (n \geq 3), \Omega = \{1, \dots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.
- $G = D_{2n} (n \geq 3), \Omega = \{1, \dots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leq b(G) + 1$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.
- $G = D_{2n} (n \geq 3), \Omega = \{1, \dots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leq b(G) + 1$.
- $G = \text{GL}_d(q), \Omega = \mathbb{F}_q^d \setminus \{0\} \implies b(G) = d$.

Bases

Let $G \leq \text{Sym}(\Omega)$ be a transitive permutation group.

Base: A subset $\Delta \subseteq \Omega$ such that $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha = 1$.

Base size $b(G)$: The minimal size of a base for G .

Remark. $\text{fix}(\Gamma) = b(\text{Aut}(\Gamma))$.

- $G = S_n, \Omega = \{1, \dots, n\} \implies b(G) = n - 1$.
- $G = D_{2n} (n \geq 3), \Omega = \{1, \dots, n\} \implies b(G) = 2$.
- $b(G) = 0 \iff G = 1$.
- $D(G) \leq b(G) + 1$.
- $G = \text{GL}_d(q), \Omega = \mathbb{F}_q^d \setminus \{0\} \implies b(G) = d$.

Klavžar, Wong & Zhu, 2006: $D(G) = 2$ if $\mathbb{F}_q^d \neq \mathbb{F}_2^2, \mathbb{F}_2^3, \mathbb{F}_4^2$ or \mathbb{F}_3^2 .

Base sizes

Observation: If Δ is a base and $x, y \in G$,

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)}$$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ .

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ .

- $|G| \leq n^{b(G)}$

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ .

- $|G| \leq n^{b(G)}$
- A small base Δ provides an efficient way to store the elements of G , using $|\Delta|$ -tuples rather than $|\Omega|$ -tuples.

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ .

- $|G| \leq n^{b(G)}$
- A small base Δ provides an efficient way to store the elements of G , using $|\Delta|$ -tuples rather than $|\Omega|$ -tuples.

Question: How small is $b(G)$?

Base sizes

Observation: If Δ is a base and $x, y \in G$, then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in \Delta \iff xy^{-1} \in \bigcap_{\alpha \in \Delta} G_\alpha = G_{(\Delta)} \iff x = y.$$

That is, each group element is uniquely determined by its action on Δ .

- $|G| \leq n^{b(G)}$
- A small base Δ provides an efficient way to store the elements of G , using $|\Delta|$ -tuples rather than $|\Omega|$ -tuples.

Question: How small is $b(G)$?

Note. $b(G) = 1 \iff G \neq 1$ is regular.

Part III

The base-two project

Base-two groups

Let $G \leq \text{Sym}(\Omega)$ be transitive of degree n with point stabiliser $H = G_\alpha$.

Base-two groups

Let $G \leq \text{Sym}(\Omega)$ be transitive of degree n with point stabiliser $H = G_\alpha$.

$$\begin{aligned} b(G) = 2 &\iff H \neq 1 \text{ has a regular orbit on } \Omega \\ &\iff H \neq 1 \text{ \& } H \cap H^g = 1 \text{ for some } g \in G \end{aligned}$$

Base-two groups

Let $G \leq \text{Sym}(\Omega)$ be transitive of degree n with point stabiliser $H = G_\alpha$.

$$\begin{aligned} b(G) = 2 &\iff H \neq 1 \text{ has a regular orbit on } \Omega \\ &\iff H \neq 1 \text{ \& } H \cap H^g = 1 \text{ for some } g \in G \end{aligned}$$

Recall. G is called **primitive** if H is maximal in G .

Base-two groups

Let $G \leq \text{Sym}(\Omega)$ be transitive of degree n with point stabiliser $H = G_\alpha$.

$$\begin{aligned} b(G) = 2 &\iff H \neq 1 \text{ has a regular orbit on } \Omega \\ &\iff H \neq 1 \text{ \& } H \cap H^g = 1 \text{ for some } g \in G \end{aligned}$$

Recall. G is called **primitive** if H is maximal in G .

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Base-two groups

Let $G \leq \text{Sym}(\Omega)$ be transitive of degree n with point stabiliser $H = G_\alpha$.

$$\begin{aligned} b(G) = 2 &\iff H \neq 1 \text{ has a regular orbit on } \Omega \\ &\iff H \neq 1 \text{ \& } H \cap H^g = 1 \text{ for some } g \in G \end{aligned}$$

Recall. G is called **primitive** if H is maximal in G .

Problem. Classify the finite primitive groups G with $b(G) = 2$.

Example

p prime, $G = D_{2p}$ and $\Omega = \{1, \dots, p\} \implies G$ primitive and $b(G) = 2$.

Probabilistic methods

Let

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

be the probability that a random pair in Ω is **not** a base for G .

Probabilistic methods

Let

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

be the probability that a random pair in Ω is **not** a base for G .

Note. $\{\alpha, \beta\}$ is not a base iff there exists $x \in G_\alpha \cap G_\beta$ of prime order.

Probabilistic methods

Let

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

be the probability that a random pair in Ω is **not** a base for G .

Note. $\{\alpha, \beta\}$ is not a base iff there exists $x \in G_\alpha \cap G_\beta$ of prime order.

The probability that a random pair is fixed by $x \in G$ is $\text{fpr}(x)^2$, where

$$\text{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap H|}{|x^G|}$$

is the fixed point ratio of x .

Probabilistic methods

Let

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

be the probability that a random pair in Ω is **not** a base for G .

Note. $\{\alpha, \beta\}$ is not a base iff there exists $x \in G_\alpha \cap G_\beta$ of prime order.

The probability that a random pair is fixed by $x \in G$ is $\text{fpr}(x)^2$, where

$$\text{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap H|}{|x^G|}$$

is the fixed point ratio of x . Therefore,

$$Q(G) \leq \sum_{x \in \mathcal{P}} \text{fpr}(x)^2 = \sum_i |x_i^G| \text{fpr}(x)^2 =: \hat{Q}(G),$$

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

Probabilistic methods

Let

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

be the probability that a random pair in Ω is **not** a base for G .

Note. $\{\alpha, \beta\}$ is not a base iff there exists $x \in G_\alpha \cap G_\beta$ of prime order.

The probability that a random pair is fixed by $x \in G$ is $\text{fpr}(x)^2$, where

$$\text{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap H|}{|x^G|}$$

is the fixed point ratio of x . Therefore,

$$Q(G) \leq \sum_{x \in \mathcal{P}} \text{fpr}(x)^2 = \sum_i |x_i^G| \text{fpr}(x)^2 =: \hat{Q}(G),$$

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

Probabilistic method: $\hat{Q}(G) < 1 \implies b(G) \leq 2$.

An example

We have $b(G) \leq 2$ if

$$\widehat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

An example

We have $b(G) \leq 2$ if

$$\hat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\hat{Q}(G) \leq A^2/B$.

An example

We have $b(G) \leq 2$ if

$$\widehat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\widehat{Q}(G) \leq A^2/B$.

Example

Let $p \geq 11$ be a prime, $G = S_p$ and $H = \text{AGL}_1(p)$.

An example

We have $b(G) \leq 2$ if

$$\hat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\hat{Q}(G) \leq A^2/B$.

Example

Let $p \geq 11$ be a prime, $G = S_p$ and $H = \text{AGL}_1(p)$. Note that we have $\sum_i |x_i^G \cap H| \leq |H| = p(p-1) =: A$.

An example

We have $b(G) \leq 2$ if

$$\widehat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\widehat{Q}(G) \leq A^2/B$.

Example

Let $p \geq 11$ be a prime, $G = S_p$ and $H = \text{AGL}_1(p)$. Note that we have $\sum_i |x_i^G \cap H| \leq |H| = p(p-1) =: A$.

If $|x_i| = p$ then $|x_i^G| = (p-1)!$,

An example

We have $b(G) \leq 2$ if

$$\widehat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\widehat{Q}(G) \leq A^2/B$.

Example

Let $p \geq 11$ be a prime, $G = S_p$ and $H = \text{AGL}_1(p)$. Note that we have $\sum_i |x_i^G \cap H| \leq |H| = p(p-1) =: A$.

If $|x_i| = p$ then $|x_i^G| = (p-1)!$, and if x_i has cycle shape $[1, r^{(p-1)/r}]$ then

$$|x_i^G| = \frac{p!}{r^{(p-1)/r} \left(\frac{p-1}{r}\right)!} \geq \frac{p!}{2^{(p-1)/2} \left(\frac{p-1}{2}\right)!} =: B.$$

An example

We have $b(G) \leq 2$ if

$$\widehat{Q}(G) = \sum_i |x_i^G| \text{fpr}(x)^2 = \sum_i \frac{|x_i^G \cap H|^2}{|x_i^G|} < 1,$$

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

Note. If $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for all i , then $\widehat{Q}(G) \leq A^2/B$.

Example

Let $p \geq 11$ be a prime, $G = S_p$ and $H = \text{AGL}_1(p)$. Note that we have $\sum_i |x_i^G \cap H| \leq |H| = p(p-1) =: A$.

If $|x_i| = p$ then $|x_i^G| = (p-1)!$, and if x_i has cycle shape $[1, r^{(p-1)/r}]$ then

$$|x_i^G| = \frac{p!}{r^{(p-1)/r} \left(\frac{p-1}{r}\right)!} \geq \frac{p!}{2^{(p-1)/2} \left(\frac{p-1}{2}\right)!} =: B.$$

It is easy to see that $A^2/B \rightarrow 0$, so $\widehat{Q}(G) \rightarrow 0$ and $b(G) \leq 2$.

Some results

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

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

- **Burness et al., 2010/11:** T alternating or sporadic ✓

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

- **Burness et al., 2010/11:** T alternating or sporadic ✓
- G Lie type: Partial answers

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

- **Burness et al., 2010/11:** T alternating or sporadic ✓
- G Lie type: Partial answers

Product type: $G \leq L \wr P$ with its product action on Σ^k , where $L \leq \text{Sym}(\Sigma)$.

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

- **Burness et al., 2010/11:** T alternating or sporadic ✓
- G Lie type: Partial answers

Product type: $G \leq L \wr P$ with its product action on Σ^k , where $L \leq \text{Sym}(\Sigma)$.

Bailey & Cameron, 2011:

$$b(L \wr P) = 2 \iff L_\sigma \text{ has at least } D(P) \text{ regular orbits on } \Sigma.$$

Some results

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

Affine: Partial classification in the setting $H/Z(H)$ is simple.

Twisted wreath type: Partial results (**Fawcett, 2022**)

Almost simple: $T \triangleleft G \leq \text{Aut}(T)$ for non-abelian simple T .

- **Burness et al., 2010/11:** T alternating or sporadic ✓
- G Lie type: Partial answers

Product type: $G \leq L \wr P$ with its product action on Σ^k , where $L \leq \text{Sym}(\Sigma)$.

Bailey & Cameron, 2011:

$$b(L \wr P) = 2 \iff L_\sigma \text{ has at least } D(P) \text{ regular orbits on } \Sigma.$$

Burness & H, 2022+: Progress where $G < L \wr P$

Diagonal type

Diagonal type: $T^k \trianglelefteq G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\text{Aut}(T)}(x) \cap C_{\text{Aut}(T)}(y) = 1$ and so $g = 1$.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\text{Aut}(T)}(x) \cap C_{\text{Aut}(T)}(y) = 1$ and so $g = 1$.

Fawcett, 2013: $P \neq A_k, S_k \implies b(G) = 2$.

Diagonal type

Diagonal type: $T^k \triangleleft G \leq T^k \cdot (\text{Out}(T) \times P)$, P is primitive or $P = A_2$.

Write $\Omega = T^k/D$, where $D = \{(t, \dots, t) : t \in T\}$ and set $\alpha = D$, so

$$G_\alpha = G \cap \{(a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in P\}.$$

Note. If $k > 32$ and $P \neq A_k, S_k$ then $D(P) = 2$, so there exists a distinguishing partition $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$ of **distinct sizes**.

Write $T = \langle x, y \rangle$ and $\beta = D(t_1, \dots, t_k) \in \Omega$, where

$$t_i = 1 \text{ if } i \in \Delta_1, \quad t_i = x \text{ if } i \in \Delta_2, \quad t_i = y \text{ if } i \in \Delta_3.$$

Suppose $g = (a, \dots, a)\pi \in G_\alpha \cap G_\beta$. Then $\pi = 1$ since π preserves $[k] = \Delta_1 \cup \Delta_2 \cup \Delta_3$. Thus, $a \in C_{\text{Aut}(T)}(x) \cap C_{\text{Aut}(T)}(y) = 1$ and so $g = 1$.

Fawcett, 2013: $P \neq A_k, S_k \implies b(G) = 2$.

H, 2022+: If $P = A_k$, then $b(G) = 2 \iff 2 < k < |T|$.

Part IV

The Saxl graph of a base-two group

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.

e.g. $G = D_{2p}$ and $n = p$ prime.

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.
e.g. $G = D_{2p}$ and $n = p$ prime.
- $G = \mathbb{Z}_m \wr \mathbb{Z}_2$ and $n = 2m \implies \Sigma(G) \cong \mathbf{K}_{m,m}$.

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.
e.g. $G = D_{2p}$ and $n = p$ prime.
- $G = \mathbb{Z}_m \wr \mathbb{Z}_2$ and $n = 2m \implies \Sigma(G) \cong \mathbf{K}_{m,m}$.
- $G = \text{GL}_2(q)$ and $\Omega = \mathbb{F}_q^2 \setminus \{0\}$.

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.

e.g. $G = D_{2p}$ and $n = p$ prime.

- $G = \mathbb{Z}_m \wr \mathbb{Z}_2$ and $n = 2m \implies \Sigma(G) \cong \mathbf{K}_{m,m}$.

- $G = \text{GL}_2(q)$ and $\Omega = \mathbb{F}_q^2 \setminus \{0\}$.

Note. $\{\alpha, \beta\}$ is a base $\iff \{\alpha, \beta\}$ is a basis for \mathbb{F}_q^2 .

Saxl graphs

Assume $G \leq \text{Sym}(\Omega)$ is transitive of degree n and $b(G) = 2$.

Burness & Giudici, 2020: Saxl graph $\Sigma(G)$:

vertices Ω , with $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example

- G is **Frobenius** $\iff \Sigma(G) \cong \mathbf{K}_n$.

e.g. $G = D_{2p}$ and $n = p$ prime.

- $G = \mathbb{Z}_m \wr \mathbb{Z}_2$ and $n = 2m \implies \Sigma(G) \cong \mathbf{K}_{m,m}$.

- $G = \text{GL}_2(q)$ and $\Omega = \mathbb{F}_q^2 \setminus \{0\}$.

Note. $\{\alpha, \beta\}$ is a base $\iff \{\alpha, \beta\}$ is a basis for \mathbb{F}_q^2 .

Hence, $\Sigma(G) \cong \mathbf{K}_{q^2-1} - (q+1)\mathbf{K}_{q-1}$ is **complete multipartite**.

Further example

- $G = \text{PGL}_2(q)$ and $\Omega = \{2\text{-subsets of } \{1\text{-spaces in } \mathbb{F}_q^2\}\}$.

Further example

- $G = \text{PGL}_2(q)$ and $\Omega = \{2\text{-subsets of } \{1\text{-spaces in } \mathbb{F}_q^2\}\}$.

Note. $G_\alpha \cong D_{2(q-1)}$ and $\{\alpha, \beta\}$ is a base $\iff |\alpha \cap \beta| = 1$.

Further example

- $G = \text{PGL}_2(q)$ and $\Omega = \{2\text{-subsets of } \{1\text{-spaces in } \mathbb{F}_q^2\}\}$.

Note. $G_\alpha \cong D_{2(q-1)}$ and $\{\alpha, \beta\}$ is a base $\iff |\alpha \cap \beta| = 1$.

Hence, $\Sigma(G) \cong J(q+1, 2)$ is a **Johnson graph**.

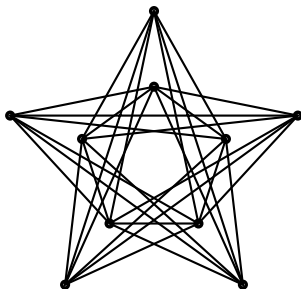
Further example

- $G = \text{PGL}_2(q)$ and $\Omega = \{2\text{-subsets of } \{1\text{-spaces in } \mathbb{F}_q^2\}\}$.

Note. $G_\alpha \cong D_{2(q-1)}$ and $\{\alpha, \beta\}$ is a base $\iff |\alpha \cap \beta| = 1$.

Hence, $\Sigma(G) \cong J(q+1, 2)$ is a **Johnson graph**.

For example, when $q = 4$ we have the complement of the Petersen.



Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.
- $|\Sigma(\alpha)| = r(G)|G_\alpha|$, where $r(G)$ is the number of regular G_α -orbits.

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.
- $|\Sigma(\alpha)| = r(G)|G_\alpha|$, where $r(G)$ is the number of regular G_α -orbits.

Burness & Giudici, 2020: $|\Sigma(\alpha)| = p$ is a prime iff the following holds:

- $G = \mathbb{Z}_p \wr \mathbb{Z}_2$, $n = 2p$ and $\Sigma(G) \cong \mathbf{K}_{p,p}$;
- $G = S_3$, $n = p + 1 = 3$ and $\Sigma(G) \cong \mathbf{K}_3$;
- $G = \text{AGL}_1(2^f)$, $n = p + 1 = 2^f$ and $\Sigma(G) \cong \mathbf{K}_{p+1}$.

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.
- $|\Sigma(\alpha)| = r(G)|G_\alpha|$, where $r(G)$ is the number of regular G_α -orbits.

Burness & Giudici, 2020: $|\Sigma(\alpha)| = p$ is a prime iff the following holds:

- $G = \mathbb{Z}_p \wr \mathbb{Z}_2$, $n = 2p$ and $\Sigma(G) \cong \mathbf{K}_{p,p}$;
- $G = S_3$, $n = p + 1 = 3$ and $\Sigma(G) \cong \mathbf{K}_3$;
- $G = \text{AGL}_1(2^f)$, $n = p + 1 = 2^f$ and $\Sigma(G) \cong \mathbf{K}_{p+1}$.

In particular, the Petersen graph is not a Saxl graph.

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.
- $|\Sigma(\alpha)| = r(G)|G_\alpha|$, where $r(G)$ is the number of regular G_α -orbits.

Burness & Giudici, 2020: $|\Sigma(\alpha)| = p$ is a prime iff the following holds:

- $G = \mathbb{Z}_p \wr \mathbb{Z}_2$, $n = 2p$ and $\Sigma(G) \cong \mathbf{K}_{p,p}$;
- $G = S_3$, $n = p + 1 = 3$ and $\Sigma(G) \cong \mathbf{K}_3$;
- $G = \text{AGL}_1(2^f)$, $n = p + 1 = 2^f$ and $\Sigma(G) \cong \mathbf{K}_{p+1}$.

In particular, the Petersen graph is not a Saxl graph.

Chen & H, 2022: G almost simple primitive and $|\Sigma(\alpha)|$ prime-power ✓

Valency

Let $\Sigma(\alpha)$ be the set of neighbours of α in $\Sigma(G)$.

Notes.

- $\Sigma(\alpha)$ is the union of regular G_α -orbits.
- $|\Sigma(\alpha)| = r(G)|G_\alpha|$, where $r(G)$ is the number of regular G_α -orbits.

Burness & Giudici, 2020: $|\Sigma(\alpha)| = p$ is a prime iff the following holds:

- $G = \mathbb{Z}_p \wr \mathbb{Z}_2$, $n = 2p$ and $\Sigma(G) \cong \mathbf{K}_{p,p}$;
- $G = S_3$, $n = p + 1 = 3$ and $\Sigma(G) \cong \mathbf{K}_3$;
- $G = \text{AGL}_1(2^f)$, $n = p + 1 = 2^f$ and $\Sigma(G) \cong \mathbf{K}_{p+1}$.

In particular, the Petersen graph is not a Saxl graph.

Chen & H, 2022: G almost simple primitive and $|\Sigma(\alpha)|$ prime-power ✓

e.g. $q = 2^f + 1$, $G = \text{PGL}_2(q)$, $G_\alpha = D_{2(q-1)}$ and $|\Sigma(\alpha)| = 2^{f+1}$.

Orbital graphs

Note. $\Sigma(G)$ is the union of the $r(G)$ regular **orbital graphs** of G .

Orbital graphs

Note. $\Sigma(G)$ is the union of the $r(G)$ regular **orbital graphs** of G .

Thus, $\Sigma(G)$ is a **G -orbital graph** $\iff r(G) = 1$.

Orbital graphs

Note. $\Sigma(G)$ is the union of the $r(G)$ regular **orbital graphs** of G .

Thus, $\Sigma(G)$ is a **G -orbital graph** $\iff r(G) = 1$.

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

Orbital graphs

Note. $\Sigma(G)$ is the union of the $r(G)$ regular **orbital graphs** of G .

Thus, $\Sigma(G)$ is a **G -orbital graph** $\iff r(G) = 1$.

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

Burness & H, 2021+: G almost simple and G_α soluble ✓

Orbital graphs

Note. $\Sigma(G)$ is the union of the $r(G)$ regular **orbital graphs** of G .

Thus, $\Sigma(G)$ is a **G -orbital graph** $\iff r(G) = 1$.

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

Burness & H, 2021+: G almost simple and G_α soluble ✓

e.g. $G = \text{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$.

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Recall that

$$Q(G) = 1 - \frac{r(G)|G_\alpha|}{|\Omega|} = 1 - \frac{|\Sigma(\alpha)|}{|\Omega|}$$

is the probability that a random pair in Ω is not a base for G .

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Recall that

$$Q(G) = 1 - \frac{r(G)|G_\alpha|}{|\Omega|} = 1 - \frac{|\Sigma(\alpha)|}{|\Omega|}$$

is the probability that a random pair in Ω is not a base for G .

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

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Recall that

$$Q(G) = 1 - \frac{r(G)|G_\alpha|}{|\Omega|} = 1 - \frac{|\Sigma(\alpha)|}{|\Omega|}$$

is the probability that a random pair in Ω is not a base for G .

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

Note. $Q(G) < 1/2 \iff |\Sigma(\alpha)| > \frac{1}{2}|\Omega|$

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Recall that

$$Q(G) = 1 - \frac{r(G)|G_\alpha|}{|\Omega|} = 1 - \frac{|\Sigma(\alpha)|}{|\Omega|}$$

is the probability that a random pair in Ω is not a base for G .

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

Note. $Q(G) < 1/2 \iff |\Sigma(\alpha)| > \frac{1}{2}|\Omega| \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Connectedness

Note. G is primitive $\implies \Sigma(G)$ is connected.

Question: What is the diameter of $\Sigma(G)$ if G is primitive?

Conjecture (Burness & Giudici, 2020)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

Recall that

$$Q(G) = 1 - \frac{r(G)|G_\alpha|}{|\Omega|} = 1 - \frac{|\Sigma(\alpha)|}{|\Omega|}$$

is the probability that a random pair in Ω is not a base for G .

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

Note. $Q(G) < 1/2 \iff |\Sigma(\alpha)| > \frac{1}{2}|\Omega| \implies \Sigma(\alpha) \cap \Sigma(\beta) \neq \emptyset$.

e.g. $p \geq 11$ prime, $(G, H) = (S_p, \text{AGL}_1(p)) \implies Q(G) < 1/2$.

Burness-Giudici conjecture

Example

If $G = \mathrm{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Burness-Giudici conjecture

Example

If $G = \text{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Some other evidence:

- **Chen & Du 2020+; Burness & H, 2021+:** $\text{soc}(G) = L_2(q)$ ✓

Burness-Giudici conjecture

Example

If $G = \mathrm{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Some other evidence:

- **Chen & Du 2020+; Burness & H, 2021+:** $\mathrm{soc}(G) = L_2(q)$ ✓
- **Burness & H, 2021+:** G almost simple with G_α soluble ✓

Burness-Giudici conjecture

Example

If $G = \mathrm{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Some other evidence:

- **Chen & Du 2020+; Burness & H, 2021+:** $\mathrm{soc}(G) = L_2(q)$ ✓
- **Burness & H, 2021+:** G almost simple with G_α soluble ✓

Recall. $\Sigma(\alpha)$ is the union of regular G_α -orbits.

Burness-Giudici conjecture

Example

If $G = \mathrm{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Some other evidence:

- **Chen & Du 2020+; Burness & H, 2021+:** $\mathrm{soc}(G) = L_2(q)$ ✓
- **Burness & H, 2021+:** G almost simple with G_α soluble ✓

Recall. $\Sigma(\alpha)$ is the union of regular G_α -orbits.

BG conjecture: $\Sigma(\alpha)$ meets the union of regular G_β -orbits.

Burness-Giudici conjecture

Example

If $G = \mathrm{PGL}_2(q)$ and $G_\alpha = D_{2(q-1)}$, then $\Sigma(G) = J(q+1, 2)$ has the common neighbour property, though $Q(G) \rightarrow 1$ as $q \rightarrow \infty$.

Some other evidence:

- **Chen & Du 2020+; Burness & H, 2021+:** $\mathrm{soc}(G) = L_2(q)$ ✓
- **Burness & H, 2021+:** G almost simple with G_α soluble ✓

Recall. $\Sigma(\alpha)$ is the union of regular G_α -orbits.

BG conjecture: $\Sigma(\alpha)$ meets the union of regular G_β -orbits.

Conjecture (Burness & H, 2022+)

G primitive and $\alpha, \beta \in \Omega \implies \Sigma(\alpha)$ meets **every** regular G_β -orbit.

Future work

- Other invariants of the Saxl graph

Future work

- Other invariants of the Saxl graph

Burness & H, 2021+: Results on clique and independence numbers

Future work

- Other invariants of the Saxl graph
 - **Burness & H, 2021+:** Results on clique and independence numbers
- Generalisations of Saxl graphs

Future work

- Other invariants of the Saxl graph
 - **Burness & H, 2021+:** Results on clique and independence numbers
- Generalisations of Saxl graphs
- Bases for affine groups

Future work

- Other invariants of the Saxl graph
 - **Burness & H, 2021+:** Results on clique and independence numbers
- Generalisations of Saxl graphs
- Bases for affine groups
 - **Seress 1996:** $b(G) \leq 4$ if G is primitive and soluble

Future work

- Other invariants of the Saxl graph
 - **Burness & H, 2021+:** Results on clique and independence numbers
- Generalisations of Saxl graphs
- Bases for affine groups
 - **Seress 1996:** $b(G) \leq 4$ if G is primitive and soluble
- Distinguishing numbers for transitive groups

Future work

- Other invariants of the Saxl graph
Burness & H, 2021+: Results on clique and independence numbers
- Generalisations of Saxl graphs
- Bases for affine groups
Seress 1996: $b(G) \leq 4$ if G is primitive and soluble
- Distinguishing numbers for transitive groups
Seress 1996: $D(G) \leq 5$ if G is soluble

Thank you!