Bases for permutation groups

Lecture 5

Tim Burness, University of Bristol

Today

- Jan Saxl's base-two project
- Summary of the main results
- The Saxl graph of a base-two permutation group
- Saxl graphs: Results and open problems

t.burness@bristol.ac.uk

https://seis.bristol.ac.uk/~tb13602/padova2021.html

Link

Base-two groups

Definition

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group with point stabilizer H. Then G is a **base-two** group if $b(G) = 2$.

$$\begin{aligned} G \text{ is base-two} &\iff H \cap H^g = 1 \text{ for some } g \in G \\ &\iff H \text{ has a regular orbit on } \Omega \\ &\iff Q(G,2) < 1 \end{aligned}$$

where $Q(G,2)$ is the probability that a random pair of points in Ω do **not** form a base for G.

Recall that

$$Q(G,2) \leqslant \sum_{i=1}^{k} |x_i^G| \,\mathrm{fpr}(x_i)^2 =: \widehat{Q}(G,2).$$

Note. Base-two groups arise naturally in many applications.

Jan's base-two project

Problem. Can we classify the finite primitive base-two groups?

Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabilizer H.

By the **O'Nan-Scott theorem**, G is one of the following:

Type	Description
Affine	$G = V{:}H \leqslant \mathrm{AGL}(V)$, $H \leqslant \mathrm{GL}(V)$ irreducible
Almost simple	$T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$
Diagonal type	$T^k \trianglelefteqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, $P \leqslant S_k$
Product type	$S^k \trianglelefteqslant G \leqslant L \wr P$, L primitive, $\mathrm{soc}(L) = S$, $P \leqslant S_k$
Twisted wreath	$G = T^k{:}P$, $P \leqslant S_k$

Progress

Let G be a **diagonal type** primitive group, so

$$T^k \trianglelefteqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$$

and either $P \leqslant S_k$ is primitive, or $k = 2$ and $P = 1$.

Theorem (Fawcett, 2013)

If $P \neq A_k, S_k$, then $b(G) = 2$.

Moreover, if $A_k \leqslant P$ then $b(G) = 2$ only if $2 < k < |T|$.

Let G be a **twisted wreath product**: $G = T^k{:}P$ with $P \leqslant S_k$ transitive.

Theorem (Fawcett, 2021)

P quasiprimitive $\implies b(G) = 2$

Base-two affine groups

Let $G = V{:}H \leqslant \mathrm{AGL}(V)$ be a primitive **affine** group, where $V = (\mathbb{F}_p)^d$ and $H \leqslant \mathrm{GL}(V)$ is irreducible. Note that

$$
\begin{aligned}
b(G) = 2 &\iff H \text{ has a regular orbit on the irreducible } \mathbb{F}_pH\text{-module } V \\
&\iff V \neq \bigcup_{1 \neq h \in H} C_V(h)
\end{aligned}
$$

where $C_V(h) = \{v \in V \,:\, v^h = v\}$ is the 1-eigenspace of h on V.

So the base-two project for affine groups is equivalent to a (hard!) problem in representation theory:

> 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.

The coprime case

Suppose H is **quasisimple** and $|H|$ is indivisible by p.

Theorem (Goodwin (2000); Köhler & Pahlings (2001))

In this setting, all the base-two affine groups $G = VH$ are known.

- This contributed to the solution of the $k(GV)$ **problem**, completed by **Gluck, Magaard, Riese & Schmid** in 2004.

  In turn, this proved a conjecture of Brauer on defect groups of blocks.

- The main technique is to show that in most cases,

$$\left| \bigcup_{1 \neq h \in H} C_V(h) \right| < |V|,$$

  which implies that H has a regular orbit on V.

A coprime example

Suppose $H = \mathrm{M}_{11}$, so $d \in \{10, 11, 16, 44, 45, 55\}$ and $p \geqslant 7$, $p \neq 11$.

Note that $C_V(h) \subseteq C_V(h^\ell)$ for all $h \in H$, $\ell \geqslant 1$. Write

$$\mathcal{P} = \{\text{prime order elements in } H\} = \bigcup_i y_i^H$$

Fact. H is generated by 4 conjugates of y_i, so $\dim C_V(y_i) \leqslant 3d/4$.

If H has no regular orbit on V, then $V = \bigcup_{x \in \mathcal{P}} C_V(x)$ and thus

$$p^d = |V| \leqslant \sum_i |y_i^H| \, |C_V(y_i)| < |H| p^{3d/4} = 7920 p^{3d/4}$$

For $d \geqslant 16$, this holds iff $(d, p) = (16, 7)$.

In fact, H has a regular orbit on V in every case.

The modular case

Theorem (Hall, Liebeck & Seitz, 1992)

Suppose $G = VH$, H quasisimple and $V = (\mathbb{F}_p)^d$. Then either $b(G) = 2$, or one of the following holds:

- H is a group of Lie type in characteristic p;
- $H = A_n$, $p \leqslant n$ and V is the fully deleted permutation module; or
- (H, V) is one of finitely many cases (undetermined).

Theorem

- **Fawcett, O'Brien & Saxl, 2016:** $H/Z(H)$ alternating
- **Fawcett, Müller, O'Brien & Wilson, 2019:** $H/Z(H)$ sporadic
- **Lee, 2020:** $H/Z(H)$ Lie type in characteristic $r \neq p$
- **Lee, 2021:** $H/Z(H)$ Lie type in characteristic p (in progress)

Almost simple groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle G_0 and point stabilizer H.

Progress on the base-two problem:

- **B, 2020:** H solvable ✓
- **James, 2006:** G standard with G_0 alternating ✓
- **B et al. 2010/11:** G_0 alternating or sporadic ✓
- G **standard with** G_0 **classical:** In progress (there are examples)
- G **non-standard,** G_0 **Lie type:** Partial results (e.g. G_0 classical, $H \in \mathcal{S}$); work in progress

Note. There are essentially no results for **product type** groups.

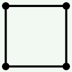
The Saxl graph

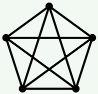
Definition (B & Giudici, 2020)

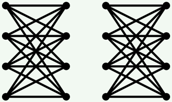
Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two permutation group.

The **Saxl graph** of G, $\Sigma(G)$: vertices Ω, $\alpha \sim \beta \iff G_{\alpha,\beta} = 1$.

Examples

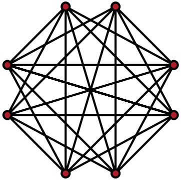
- $G = D_8$, $\Omega = \{1, 2, 3, 4\}$: $\Sigma(G) = C_4 =$ 

- $G = D_{10}$, $\Omega = \{1, 2, 3, 4, 5\}$: $\Sigma(G) = K_5 =$ 

- $G = D_8 \times D_8$, $\Omega = \{1, 2, 3, 4\}^2$: $\Sigma(G) = K_{4,4} \oplus K_{4,4} =$ 

Some further examples

- Let $G = \mathrm{GL}_2(q)$ and $\Omega = (\mathbb{F}_q)^2 \setminus \{0\}$. Here $\alpha \sim \beta$ iff $\{\alpha, \beta\}$ is linearly independent, so $\Sigma(G)$ is the **complete multipartite graph** with $q+1$ parts of size $q-1$. For example, if $q = 3$:



- Let $G = \mathrm{PGL}_2(q)$ and let Ω be the set of distinct pairs of 1-spaces in $V = (\mathbb{F}_q)^2$. Then $\{\alpha, \beta\}$ is a base for G, where

$$\alpha = \{\langle e_1 \rangle, \langle e_2 \rangle\}, \;\; \beta = \{\langle e_1 \rangle, \langle e_1 + e_2 \rangle\}$$

  In fact, two vertices in $\Sigma(G)$ are adjacent iff they share a common 1-space, so $\Sigma(G)$ is the **Johnson graph** $J(q+1, 2)$.

Orbitals

Suppose $b(G) = 2$ and fix $\alpha \in \Omega$.

Let $\Omega_1, \ldots, \Omega_r$ be the regular orbits of G_α on $\Omega \setminus \{\alpha\}$, where $\Omega_i = \beta_i^{G_\alpha}$.

G acts naturally on $\Omega \times \Omega$: let Δ_i be the G-orbit of (α, β_i).

Then Δ_i is an **orbital** of G and the associated **orbital graph** $\Gamma(\Delta_i)$ has vertex set Ω and $\gamma \sim \delta \iff (\gamma, \delta) \in \Delta_i$.

Observation. The Saxl graph

$$\Sigma(G) = \Gamma(\Delta_1) \cup \cdots \cup \Gamma(\Delta_r)$$

is the **generalised orbital graph** of G corresponding to the regular G_α-orbits.

First properties

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive base-two group with point stabilizer H.

- $G \leqslant \mathrm{Aut}(\Sigma(G))$: $\{\alpha, \beta\}$ is a base $\iff$ $\{\alpha^g, \beta^g\}$ is a base
- In particular, $\Sigma(G)$ is vertex-transitive with no isolated vertices
- G primitive $\implies$ $\Sigma(G)$ is connected
- G 2-transitive $\implies$ $\Sigma(G)$ is complete
- G Frobenius $\iff$ $\Sigma(G)$ is complete
- $\Sigma(G)$ has valency $r|H|$, where r is the no. of regular orbits of H on Ω

Note. $\Sigma(G)$ connected $\not\Rightarrow$ G primitive (e.g. $G = D_8$, $\Omega = \{1, 2, 3, 4\}$)

Valency

Theorem (B & Giudici, 2020)

Let G be a finite transitive base-two group of degree n.

Then $\Sigma(G)$ has prime valency p iff one of the following holds:

- $G = C_p \wr C_2$, $n = 2p$, $\Sigma(G) = K_{p,p}$.
- $G = S_3$, $n = p + 1 = 3$, $\Sigma(G) = K_3$.
- $G = \mathrm{AGL}_1(2^f)$, $n = p + 1 = 2^f$, $\Sigma(G) = K_{p+1}$.

Chen & Huang (2020) have determined all the almost simple primitive groups with **prime-power** valency Saxl graphs

e.g. $G = \mathrm{PGL}_2(q)$, $q = 2^m + 1$ Fermat prime, $\Sigma(G) = J(q+1, 2)$,
valency $= 2(q-1) = 2^{m+1}$

Eulerian cycles

Recall. An **Eulerian cycle** is a cycle that uses each edge exactly once.

By a famous theorem of Euler, a connected graph has an Eulerian cycle iff the degree of every vertex is even.

Theorem (B & Giudici (2020); Chen & Huang (2020))

Let G be an almost simple primitive base-two group with socle G_0 and point stabilizer H. Then one of the following holds:

- $\Sigma(G)$ is Eulerian
- $G = \mathrm{M}_{23}$, $H = 23{:}11$ and $\Sigma(G)$ is not Eulerian
- $G_0 = \mathrm{L}_n^{\epsilon}(q)$, $n \geqslant 3$ is a prime and H is of type $\mathrm{GL}_1^{\epsilon}(q^n)$.

Question. Is $(G, H) = (\mathrm{M}_{23}, 23{:}11)$ the only non-Eulerian example?

Connectedness

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

If $\Sigma(G)$ is connected, let $\mathrm{diam}(G)$ be the diameter of $\Sigma(G)$.

By explicit constructions, we proved the following result:

Theorem (B & Giudici, 2020)

There exist finite transitive base-two groups G such that

- $\Sigma(G)$ has arbitrarily many connected components; or
- $\Sigma(G)$ is connected and $\mathrm{diam}(G)$ is arbitrarily large.

Example. If $G = (D_8)^k$ and $\Omega = \{1, 2, 3, 4\}^k$, then $\Sigma(G)$ has 2^{k-1} connected components.

Probabilistic methods

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two transitive permutation group of degree n and let $v(G)$ be the valency of $\Sigma(G)$. Recall that

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

and set $t := \max\{m \in \mathbb{N} \,:\, Q(G,2) < \frac{1}{m}\} \geqslant 1$.

Lemma

If $t \geqslant 2$, then $\Sigma(G)$ has all the following properties:

- Any t vertices in $\Sigma(G)$ have a common neighbour.
- $\Sigma(G)$ is connected with diameter at most 2.
- The clique number of $\Sigma(G)$ is at least $t+1$.
- $\Sigma(G)$ is Hamiltonian.

Lemma

If $t \geqslant 2$, then $\Sigma(G)$ has all the following properties:

- Any t vertices in $\Sigma(G)$ have a common neighbour.
- $\Sigma(G)$ is connected with diameter at most 2.
- The clique number of $\Sigma(G)$ is at least $t+1$.
- $\Sigma(G)$ is Hamiltonian.

Proof of the lemma. Since $Q(G,2) < 1/t$ we have $v(G) > n(1-1/t)$ and we deduce that the intersection of the neighbour sets of any t vertices is nonempty. This proves the first three parts.

For Hamiltonicity, we use a theorem of **Dirac (1952)**, which states that a graph with n vertices is Hamiltonian if every vertex has degree at least $n/2$.

Conjecture (Lovász, 1969). There are only 5 connected vertex-transitive finite graphs that are not Hamiltonian.

Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group with $b(G) = 2$.

Recall. $Q(G,2) \leqslant \widehat{Q}(G,2) = \sum_i |x_i^G| \, \mathrm{fpr}(x_i)^2$ and in many cases we prove that $b(G) = 2$ by establishing the bound $\widehat{Q}(G,2) < 1$.

If we can force $\widehat{Q}(G,2) < 1/2$, then any two vertices in $\Sigma(G)$ have a common neighbour and thus $\mathrm{diam}(G) = 2$.

Example

Suppose G is non-standard with socle A_m. Using **Magma** and fixed point ratio estimates, we calculate that either

- $Q(G,2) < 1/2$, or
- $G = S_7$, $H = \mathrm{AGL}_1(7)$ and $Q(G,2) = 13/20$.

In all cases, any two vertices in $\Sigma(G)$ have a common neighbour.

The main conjecture

Let G be a finite primitive base-two group.

Conjecture (B & Giudici, 2020)

- Either G is a Frobenius group and $\Sigma(G)$ is complete, or $\mathrm{diam}(G) = 2$.
- Any two vertices in $\Sigma(G)$ have a common neighbour.

Example

Let $G = \mathrm{PGL}_2(q)$ and let Ω be the set of pairs of 1-dimensional subspaces of $(\mathbb{F}_q)^2$. Here

$$Q(G,2) = 1 - \frac{v(G)}{|\Omega|} = 1 - \frac{4(q-1)}{q(q+1)} \to 1 \text{ as } q \to \infty$$

but $\Sigma(G) = J(q+1,2)$ still has the common neighbour property!

Some evidence

- All primitive groups of degree $n \leqslant 4095$
- All non-standard groups with socle A_m
- "Most" almost simple sporadic groups
- All almost simple groups with socle $\mathrm{L}_2(q)$ **(Chen & Du, 2020)**
- All almost simple groups with solvable point stabilizers **(B & Huang, in progress)**
- Asymptotic results for many diagonal and twisted wreath type groups **(Fawcett, 2013/21)**

Some open problems

- **Connectedness.** Is there a characterization of the transitive groups with connected Saxl graph?

  What happens when G is quasiprimitive?

- **Clique number.** Let (G_n) be a sequence of base-two primitive groups with $|G_n| \to \infty$. Does $\omega(G_n) \to \infty$?

  Note. This is true if $Q(G_n, 2) \to 0$ as $n \to \infty$. Also note that $\omega(J(q+1, 2)) = q$.

- **Automorphisms.** There are examples with $\mathrm{Aut}(\Sigma(G)) = G$. Can they be classified?

- **Cycles.** Eulerian cycles? Hamiltonicity?

- **Other invariants.** Chromatic number? Independence number? etc.


Grazie a tutti!

Some references

- Burness, Giudici: *On the Saxl graph of a permutation group*, Math. Proc. Cam. Phil. Soc. **168** (2020), 219–248.
- Burness, Huang: *On the Saxl graphs of primitive groups with soluble stabilisers*, in preparation
- Chen, Du: *On the Burness-Giudici Conjecture* (arXiv:2008.04233)
- Chen, Huang: *On valency problems of Saxl graphs* (arXiv:2012.13747)
- Fawcett: *The base size of a primitive diagonal group*, J. Algebra **375** (2013), 302–321.
- Fawcett: *Bases of twisted wreath products* (arXiv:2102.02190)
- Fawcett, Müller, O'Brien, Wilson: *Regular orbits of sporadic simple groups*, J. Algebra **522** (2019), 61–79.
- Fawcett, O'Brien, Saxl: *Regular orbits of symmetric and alternating groups*, J. Algebra **458** (2016), 21–52.

- Goodwin: *Regular orbits of linear groups with an application to the $k(GV)$-problem. I, II*, J. Algebra **227** (2000), 395–432, 433–473.
- Hall, Liebeck, Seitz: *Generators for finite simple groups, with applications to linear groups*, Quart. J. Math. Oxford **43** (1992), 441–458.
- James: *Partition actions of symmetric groups and regular bipartite graphs*, Bull. London Math. Soc. **38** (2006), 224–232.
- Köhler, Pahlings: *Regular orbits and the $k(GV)$-problem*, in Groups and computation, III (Columbus, OH, 1999), 209–228, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.
- Lee: *Regular orbits of quasisimple linear groups I* (arXiv:1911.05785)
- Lee: *Regular orbits of quasisimple linear groups II* (arXiv:2006.14954)
- Lee: *Regular orbits of quasisimple linear groups III*, in preparation.