Finite Primitive Binary Permutation Groups In memoriam, Chat Ho, 1946–2005

Gregory Cherlin

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Sep. 24, 2021–ICJ

Welcome back!

Relational complexity—origins

Lachlan: Homogeneous structures in finite relational languages.

Finite $\rightarrow$ Parametrized families $\rightarrow$ Stable

Relational complexity—origins

Lachlan: Homogeneous structures in finite relational languages.

Finite $\to$ Parametrized families $\to$ Stable

Example

Finite homogeneous graphs.

Graphs	$[C_5]$	$[K_3 \otimes K_3]$	$[m \cdot K_n]$	$[K_n[m]]$
Groups	$[D_5]$	$[\mathrm{Sym}_3 \wr \mathrm{Sym}_2]$	$[\mathrm{Sym}_n \wr \mathrm{Sym}\, m]$	Same
Family	$\mathcal{F}_1$	$\mathcal{F}_2$	$\mathcal{F}_3$	$\mathcal{F}_4 = \mathcal{F}_3^c$

Relational complexity—origins

Lachlan: Homogeneous structures in finite relational languages.

Finite $\rightarrow$ Parametrized families $\rightarrow$ Stable

Hypotheses:
$M^k / \mathrm{Aut}(M)$ homogeneous (fixed relational complexity)
$M^k / \mathrm{Aut}(M)$ small (few k-types)

Relational complexity—origins

Lachlan: Homogeneous structures in finite relational languages.

Finite $\rightarrow$ Parametrized families $\rightarrow$ Stable

Hypotheses:
$M^k / \mathrm{Aut}(M)$ homogeneous (fixed relational complexity)
$M^k / \mathrm{Aut}(M)$ small (few k-types)

Requires CFSG. $(M, \mathrm{Aut}\, M)$ as permutation group.

Problems

- Estimate (or compute) relational complexity of interesting structures (combinatorics, linear algebra, group theory).
  - E.g., actions of $\mathrm{Sym}(n)$ on partitions of fixed shape; natural action of $\mathrm{A\Gamma L}(1, q)$; wreath products (Saracino)
- Describe all structures of low (or, possibly, high) relational complexity.
  - Beginning with relational complexity 2.

Problems

- Estimate (or compute) relational complexity of interesting structures (combinatorics, linear algebra, group theory).
  - E.g., actions of $\mathrm{Sym}(n)$ on partitions of fixed shape; natural action of $\mathrm{A\Gamma L}(1, q)$; wreath products (Saracino)
- Describe all structures of low (or, possibly, high) relational complexity.
  - Beginning with relational complexity 2.

Conjecture (Now, theorem)

The finite primitive binary structures are the following.

- *Structures with no relations ($\mathrm{Sym}(n)$ acting naturally);*
- *Oriented p-cycles (cyclic groups acting regularly), $s_2 = p - 1$;*
- *Affine space with an anisotropic quadratic form $Q(b - a)$ (dim 1 or 2), $s_2 := \lfloor (p - 1)/2 \rfloor$ or $q - 1$*

The binarity theorem

- Conjecture—-1989, computations in Cayley (Sims library); 2000, mentioned in a survey on Lachlan's work.
- 2016: reduction to the almost simple case via O'Nan-Scott theory (Cherlin; Wiscons).
- 2016–2021: almost simple case
  Dalla Volta, Gill, Liebeck, Spiga, concluding with exceptional and classical groups; Aschbacher theory and a variety of machine computations.

The binarity theorem

- Conjecture—-1989, computations in Cayley (Sims library); 2000, mentioned in a survey on Lachlan's work.
- 2016: reduction to the almost simple case via O'Nan-Scott theory (Cherlin; Wiscons).
- 2016–2021: almost simple case
  Dalla Volta, Gill, Liebeck, Spiga, concluding with exceptional and classical groups; Aschbacher theory and a variety of machine computations.

Of interest in the algebraic case as well—a natural approach is via ranked groups with the Algebraicity Conjecture.

1989

Deg	No	t	Normal	$G(n)$	$G^{(t)}$ orbs	Comments	types	Ar	T
2	1	2	–	(1)	1^2	$\mathrm{Sym}(2) = C_2$	$1_2]$	2	.03
3	1	1	–	(1)	1^3	$\mathrm{Alt}(3) = C_3$	$2_2]$	2	.03
	2	3	3G1	2G1	1^3	$\mathrm{Sym}(3) = D_3$	$1_3]$	2	.05
4	1	2	affine	3G1	1^4	Alt(4)	$2_3]$	3	.05
	2	4	affine	3G2	1^4	Sym(4)	$1_4]$	2	.09
5	1	1	–	(1)	1^5	C_5	$4_2]$	2	.03
	2		5G1	C_2	$1, 2^2$	D_5	$6_3]$	2	.08
	3	2	5G1	C_4	1^5	AGL(1,5)	$3_3]$	3	.06
	4	3	–	4G1	1^5	Alt(5)	$2_4]$	4	.09
	5	5	5G4	4G2	1^5	Sym(5)	$1_5]$	2	.12
6	1	2	–	5G2	$1^2, 2^2$	PSL(2,5)	$2, 2_3; 6_4]$	3	.12
	2	3	6G1	5G3	1^6	PGL(2,5)	$1, 1_3; 3_4]$	4	.10
	3	4	–	5G4	1^6	Alt(6)	$2_5]$	5	.11
	4	6	6G3	5G5	1^6	Sym(6)	$1_6]$	2	.17

Figure: Data, page 1, top. T: minutes
(Sims library, 406 groups)

1989

Binary Groups: C_p, D_p, Sym(n). There is also a family of 1-dimensional semilinear groups over F_q: with Galois action exactly C_2. We have as examples groups in degree 9, #2; degree 16, #2; degree 25, #9; degree 49, #11. There are no others up to degree 50.

For the alternating group on k-sets, conjecturally the arity should be $n-k$. In any case it is at least $n-k$; the example is given by fixing $k-1$ points and looking at k-sets formed from one additional point. For $k=2$, look at the sets as the edges in a graph. It is fairly easy to see that the arity is witnessed by acyclic graphs, and the bound $n-2$ then follows fairly easily for $n>3$.

Everything has been recomputed with the last version of the program except for two long computations in degree 45 #6-7. Alt(10) or Sym(10) on pairs, over 30 hours
Now < 5 secs on laptop

Figure: Closing remarks
(Colored and annotated)

Why primitive?

- All regular actions are binary.
- All transitive actions are quotients of regular actions.
- We have O'Nan-Scott theory and can hope to reduce to the almost simple case.

Why primitive?

- All regular actions are binary.
- All transitive actions are quotients of regular actions.
- We have O'Nan-Scott theory and can hope to reduce to the almost simple case.

However,

Why primitive?

- All regular actions are binary.
- All transitive actions are quotients of regular actions.
- We have O'Nan-Scott theory and can hope to reduce to the almost simple case.

However, we may certainly ask about transitive actions, in the following way.

1. What are the "indecomposable actions" of relational complexity k?
2. What operations of composition preserve relational complexity?

Indecomposable: First definition

Definition

The binary structure is *minimal* if it has no non-trivial proper binary quotient.

The known minimal binary structures:

- Primitive
- $\mathrm{SL}(2, q)$ on non-zero vectors.
- Potentially: Regular actions of many simple groups, excluding $\mathrm{PSL}(2, q)$, q even. (??)

Indecomposable: First definition

Definition

The binary structure is minimal if it has no non-trivial proper binary quotient.

The known minimal binary structures:

- Primitive
- $\mathrm{SL}(2, q)$ on non-zero vectors.
- Potentially: Regular actions of many simple groups, excluding $\mathrm{PSL}(2, q)$, q even. (??)

Non-minimal: binary quotient, binary equivalence classes, some sort of composition?

Indecomposable: second definition

Definition

A structure is quasi-primitive if it carries no definable equivalence relation such that the group of automorphisms acting trivially on the quotient acts transitively on the classes.

- Cheryl Praeger: O'Nan-Scott theorem for quasi-primitive groups.

Indecomposable: second definition

Definition

A structure is quasi-primitive if it carries no definable equivalence relation such that the group of automorphisms acting trivially on the quotient acts transitively on the classes.

- Cheryl Praeger: O'Nan-Scott theorem for quasi-primitive groups.

Problem

Does the quasi-primitive binary case reduce to the almost simple case?

In the almost simple case we have very few such examples so far—mainly primitive actions, $\mathrm{SL}_2(q)$ on non-zero vectors, regular actions of some simple groups, and orbits in products of such.

Methods

- O’Nan-Scott
- Aschbacher
- Tests for non-binarity

O'Nan-Scott

Fact

A primitive group is one of the following.

1. *Regular socle: affine (abelian) or exotic (non-abelian);*
2. *Regular non-abelian socle (exotic);*
3. *Diagonal: socle T^k with the diagonal fixing a point;*
4. *Almost simple;*
5. *Product action (e.g. wreath product) of types (3) or (4).*

O'Nan-Scott

Fact

A primitive group is one of the following.

1. *Regular socle: affine (abelian) or exotic (non-abelian);*
2. *Regular non-abelian socle (exotic);*
3. *Diagonal: socle T^k with the diagonal fixing a point;*
4. *Almost simple;*
5. *Product action (e.g. wreath product) of types (3) or (4).*

Remark

O'Nan-Scott in ranked groups: Macpherson-Pillay. No exotic type except possibly in the almost simple case!

Problem

O'Nan-Scott in the quasi-primitive case for ranked groups?

Elimination of affine case

Lemma

If a, b are conjugate then they are conjugate by an involution in the linear group.

Basic step.

$(0, a, -a^g) \sim (0, a^g, -a)$ by binarity (and translation by $a^g - a$). This gives an element swapping a, a^g. This can be iterated … $\square$

Elimination of affine case

Odd characteristic

- $EG = (1)$;
- OG is cyclic;
- F_2G is cyclic or dihedral.

For the first point one resorts to CFSG—exclude Q_8 and Alt_4 and consider what remains.

Elimination of affine case

Odd characteristic

- $EG = (1)$;
- OG is cyclic;
- F_2G is cyclic or dihedral.

For the first point one resorts to CFSG—exclude Q_8 and Alt_4 and consider what remains.

Characteristic 2

CFSG again.

Preliminaries: no element of order 4, $FG = 1$ (or done); and G is generated by involutions.

Bender: G is a product of simple groups of type $\mathrm{PSL}_2(q)$ ($q = 2^d$), J_1, or ${}^2G_2(3^{2n+1})$—and in our case, just one.

…Now what?

Elimination of affine case

Odd characteristic

- $EG = (1)$;
- OG is cyclic;
- F_2G is cyclic or dihedral.

For the first point one resorts to CFSG—exclude Q_8 and Alt_4 and consider what remains.

Characteristic 2

CFSG again.

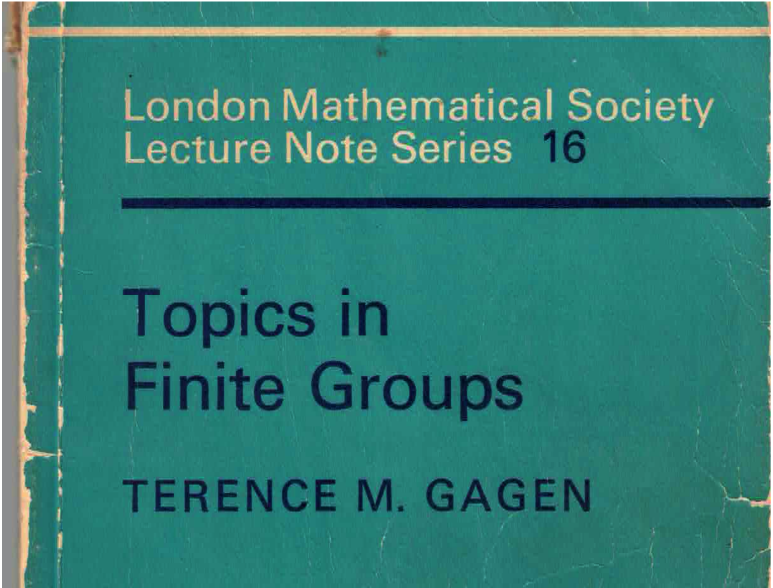
Preliminaries: no element of order 4, $FG = 1$ (or done); and G is generated by involutions.

Bender: G is a product of simple groups of type $\mathrm{PSL}_2(q)$ ($q = 2^d$), J_1, or ${}^2G_2(3^{2n+1})$—and in our case, just one.

…Now what?

E.g. for $\mathrm{PSL}_2(q)$, force the action on the projective line to be realized inside A; binarity forces Sym_{q+1} into the group, #.

Chat Ho, Tübingen, 1978-79



10. **A GENERALIZATION OF THE FITTING SUBGROUP**

Definition. Let X be any group, $F(X)$, the Fitting subgroup of X. We define $F^*(X) = \text{socle } (F(X).C_X(F(X)) \bmod F(X))$. Define $E(X)$ to be the terminal member of the derived series of $F^*(X)$.

It is easy to see that $F(X)C_X(F(X))/F(X)$ has no solvable normal subgroup. For then we could choose a p-group $P \subseteqq C_X(F(X))$ such that $PF(X)/F(X)$ is minimal normal in $X/F(X)$ and then $PF(X)$ is a nilpotent normal subgroup of X. Thus $F(X)C_X(F(X))/F(X)$ has no solvable normal subgroup and its socle is a direct product of non-abelian simple groups. It is easy to see that $F^*(X) = F(X)E(X)$ and that $C_X(F^*(X)) \subseteqq F^*(X)$. Since this is actually the most important property of the group $F^*(X)$ - being easily true when X is solvable - we verify this in the following

Lemma 10. 1. (a) $F^*(X) = F(X)E(X)$.
(b) $[F(X), E(X)] = 1$.
(c) $C_X(F^*(X)) \subseteqq F^*(X)$.

Proof. (a) is clear.
(b) $F(X)C_X(F(X))/C_X(F(X))$, being a homomorphic image of a

Chat Ho, Tübingen, 1978-79

Of the various awards Chat acquired, he was probably proudest of his Alexander von Humboldt fellowship and his Senior Men's Table Tennis Championship. ...We always knew of Professor Ho's presence in the department because we could hear his unique laughter when he talked in the corridors. He was a lovable individual whose presence will be sorely missed. `https://math.ufl.edu/alumni/in-memory-of-chat-yin-ho/`

Elimination of exotics (Wiscons)

Exotic (regular nonabelian socle): theory relies on the Schreier conjecture, only known via CFSG.
$G := A.H$ where A is now non-abelian and H acts. In fact $A = T^k$ and H acts faithfully on the k copies of T (in particular $k > 1$ here (via Schreier)).
(This case disappears in the context of ranked groups, apart from the almost simple case with non-algebraic socle.)

Elimination of exotics (Wiscons)

Exotic (regular nonabelian socle): theory relies on the Schreier conjecture, only known via CFSG.
$G := A.H$ where A is now non-abelian and H acts. In fact $A = T^k$ and H acts faithfully on the k copies of T (in particular $k > 1$ here (via Schreier)).

A lemma in the affine case shows A can be inverted by an element of H. That would dispose of the non-abelian case—but in fact we need to work more "locally."

Elimination of exotics (Wiscons)

Exotic (regular nonabelian socle): theory relies on the Schreier conjecture, only known via CFSG.
$G := A.H$ where A is now non-abelian and H acts. In fact $A = T^k$ and H acts faithfully on the k copies of T (in particular $k > 1$ here (via Schreier)).

A variant of the earlier swapping lemma shows: if a, a^h commute then a, a^h can be swapped by H.
This leads (with a little help from Feit-Thompson) to

$$(t_1, \ldots, t_k) \sim_H (t_1^{-1}, \ldots, t_k^{-1}) \text{ [}k\text{-tuples]}$$

with $t_1 \neq t_1^{-1}$ for a contradiction,

Elimination of exotics (Wiscons)

Exotic (regular nonabelian socle): theory relies on the Schreier conjecture, only known via CFSG.
$G := A.H$ where A is now non-abelian and H acts. In fact $A = T^k$ and H acts faithfully on the k copies of T (in particular $k > 1$ here (via Schreier)).

A variant of the earlier swapping lemma shows: if a, a^h commute then a, a^h can be swapped by H.
This leads (with a little help from Feit-Thompson) to

$$(t_1, \ldots, t_k) \sim_H (t_1^{-1}, \ldots, t_k^{-1}) \text{ [}k\text{-tuples]}$$

with $t_1 \neq t_1^{-1}$ for a contradiction,
$\star$ Diagonal along similar lines, with subtleties

Reduction of products

(Y, H) primitive of diagonal or almost simple type and socle M, $G \leq H \wr \mathrm{Sym}_m$ acts on Y^m and contains M^m. Furthermore, the subgroup G_1 induced by G on the first factor is again primitive, with socle M, and no greater relational complexity. So now diagonal is ruled out and only almost simple remains.

Reduction of products

(Y, H) primitive of diagonal or almost simple type and socle M, $G \leq H \wr \mathrm{Sym}_m$ acts on Y^m and contains M^m. Furthermore, the subgroup G_1 induced by G on the first factor is again primitive, with socle M, and no greater relational complexity. So now diagonal is ruled out and only almost simple remains.

Finally, if G_1 is $\mathrm{Sym}(n)$ acting naturally then $\mathrm{Alt}(n)^m$ acts on Y^m and an explicit construction produces 4-tuples in Y^m which are 2-equivalent but non-conjugate.

Almost simple case

- Sporadics
- Alternating and Lie rank 1.
- Exceptional
- Classical
  - Aschbacher theory [does this pass to the ranked category?]

Bounds, GLoS 2021

Definition

base—trivial point stabilizer
$b(G)$—minimal base size
$B(G)$—maximal size of a minimal base
$H(G)$—maximal size of an independent set
$I(G)$—maximal size of an irredundant ordered base

Lemma (Height estimates)

$$b \leq B \leq H \leq I \leq b \cdot \log deg$$

$$RC \leq H + 1 \leq 9 \log deg \text{ with few notable exceptions}$$

Non-binarity tests—structural

- Complexity does not increase when restricting to an equivalence class for a parametrically definable equivalence relation.
  (Pointwise stabilizers; subgroups containing a point stabilizer).
- If some subset can be enumerated by 2-equivalent tuples which are not conjugate, the group is not binary.
  E.g. if the induced action is 2-transitive but not the full symmetric group.

Example

G, point stabilizer M. Suppose

- $A \leq M$, $A \simeq \mathrm{SL}_n(q)$, $n \geq 2$;
- $A \leq S \leq G$, S a central quotient of $\mathrm{SL}_{n+1}(q)$, $S \not\leq M$;

Then G contains the natural doubly transitive action of A on some $V(n,q)$ (orbit of complement to $G \cap A$).

Some subgroup theoretic criteria

$\star$ Elementary abelian subgroups $V = \langle g, h \rangle$ of order p^2:.
If

- p divides $|\Omega|$, $|M|$, p^2 does not divide $|M|$ and $\langle g \rangle, \langle h \rangle, \langle gh \rangle$ are conjugate, and g fixes a point, or
- g, h, gh^{-1} conjugate with fixed point sets of maximal size (for p-elements), not all fixed by V.

then G is not binary (by a previous criterion, ultimately).

$\star$ Frobenius subgroups:
$F \lhd G$ acting as $A \rtimes C$ on a subset as a Frobenius group with A cyclic and C not an elementary abelian 2-group. Then G is not binary (via explicit triples in A of the form $(1, a, a^t)$ with a a generator.).
A variant allows a wide range of subgroups under particular numerical conditions.

Then what?

Eventually, systematic application of these methods leaves over a large finite number of groups (some of every kind). Then there are 6 computational methods.

Then what?

Eventually, systematic application of these methods leaves over a large finite number of groups (some of every kind). Then there are 6 computational methods.

1. The number of k-types is bounded in terms of 2-types. The orbit counting can be checked using character theory numerically.
2. There are standard routines for comparing G to the automorphism group of the binary structure.
3. Just check everything: all the 3-types, and perhaps all (or a random sample of) the 4-types.

This takes us up to degree 10^7.

Computations: Larger groups

4. Binary actions of the point stabilizer may be few, and ruled out numerically.
   E.g. Sym_5 has non-trivial binary actions other than regular only: ordered k-tuples for $1 \leq k \leq 4$; on ordered partitions of type $(1, 2, 2)$; and the action of degree 2 (which can be discarded here); so the relevant degrees are divisible by 5. With the trivial orbit, this means $|\Omega|$ cannot be divisible by 5 (Sym_5 contains the Sylow 5-subgroup).
5. Conjugacy classes of prime elements can be explored numerically, and prior criteria applied thoroughly.
6. When M is exotically small one tends to find points a, b, c such that the stabilizer of a, b is trivial and (with luck) there is a non-trivial intersection $M_a \cap M_b M_c$.This gives a counterexample to binarity using triples (a, b, c) and (a, b, c^g) for g in the intersection.

A few problems

The main questions are in the algebraic category—which perhaps should precede the finite case.
This certainly lends itself to an investigation in the ranked category if one assumes the Algebraicity Conjecture.
But—

A few problems

…staying in the ranked category:

Questions

- For connected groups, is the relational complexity bounded as a function of the rank?
  Or more directly, is the height bounded?
- Binary groups: reduce to almost simple case? (Affine case in particular.)
- Is there an O'Nan-Scott Theory for "quasi-primitive" groups of finite Morley rank?
- What can we say about maximal definable subgroups of quasisimple algebraic groups?
- O'Nan-Scott theory in definably primitive groups …
  6 problems, Macpherson-Pillay (5.1–5.5, 5.7)

A few problems

Questions

- O'Nan-Scott theory in definably primitive groups ...
  6 problems, Macpherson-Pillay (5.1–5.5, 5.7)

5.1: Aff Absolutely irreducible over finite $\mathbb{F}_q$?

"The only serious obstacle [apart from Algebraicity] to a classification of definably primitive groups of finite Morley rank."

5.2,5.3: Aff Fine structure when the base field is infinite (cf. Poizat, *Études Wagnériennes* re 5.2).

5.4: AS Simple regular normal?

5.5: D,P Diagonal or product actions with algebraic socle

5.7: ? Are there definably primitive groups which are imprimitive and not affine? [finite point stabilizer]

Similar: Conjugacy theorem? (Frattini).