THE UNIVERSITY OF WESTERN AUSTRALIA

Coprime actions of finite groups

CHERYL E PRAEGER

CENTRE FOR THE MATHEMATICS OF SYMMETRY AND COMPUTATION

APRIL 2021

Begins with a question about groups acting on vector spaces

- ↘ Finite groups
- ↘ Finite spaces

- ↘ Ends with an answer to old question from 1935 about primitive permutation groups

Group actions on a vector space

Finite $H \leq GL(V)$ with $V = F^d$

- Traditionally $F = C$ complex numbers
- Then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$ with H irreducible on each V_i
- We say H is completely reducible on V

- Also true if $F = F_q$ with $q = p^s$ and with $|H|$ NOT divisible by the prime p
- Otherwise property may fail

Group actions on a vector space

- Traditionally $\boldsymbol{F} = \boldsymbol{C}$ complex numbers
- Then $\boldsymbol{V} = \boldsymbol{V_1} \oplus \boldsymbol{V_2} \oplus \cdots \oplus \boldsymbol{V_t}$ with $\boldsymbol{H}$ irreducible on each $\boldsymbol{V_i}$
- We say $\boldsymbol{H}$ is completely reducible on $\boldsymbol{V}$

- Also true if $\boldsymbol{F} = \boldsymbol{F_q}$ with $\boldsymbol{q} = \boldsymbol{p^s}$ and with $|\boldsymbol{H}|$ NOT divisible by the prime $\boldsymbol{p}$
- Otherwise property may fail

Finite $\boldsymbol{H} \leq \boldsymbol{GL}(\boldsymbol{V})$ with $\boldsymbol{V} = \boldsymbol{F^d}$

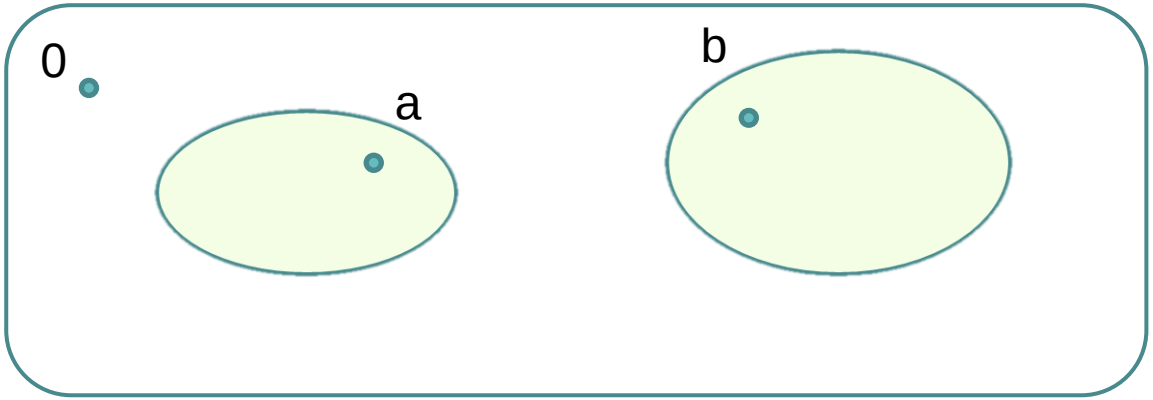
- Example $\boldsymbol{V} = \left(\boldsymbol{F_p}\right)^{\boldsymbol{2}}$, any $\boldsymbol{p}$
- $\boldsymbol{H} = \{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \mid x, y, z \in F, x, z \neq 0 \}$
- ONLY $\boldsymbol{H}$ -invariant subspaces are
- $\boldsymbol{V}, \{ (\boldsymbol{0}, \boldsymbol{0}) \}, \boldsymbol{and} \langle (\boldsymbol{1}, \boldsymbol{0}) \rangle$

Coprime orbits of a finite group $H \leq GL(V)$ with $V = F^d$ and F finite

- For $a \in V$, the H-orbit containing a is $a^H = \{ a^h \mid h \in H \}$
- For a, b in V the H-orbits a^H, b^H are coprime if

$$|a^H| > 1, \ |b^H| > 1 \text{ and } \gcd(|a^H|, |b^H|) = 1$$

Coprime actions on a vector space



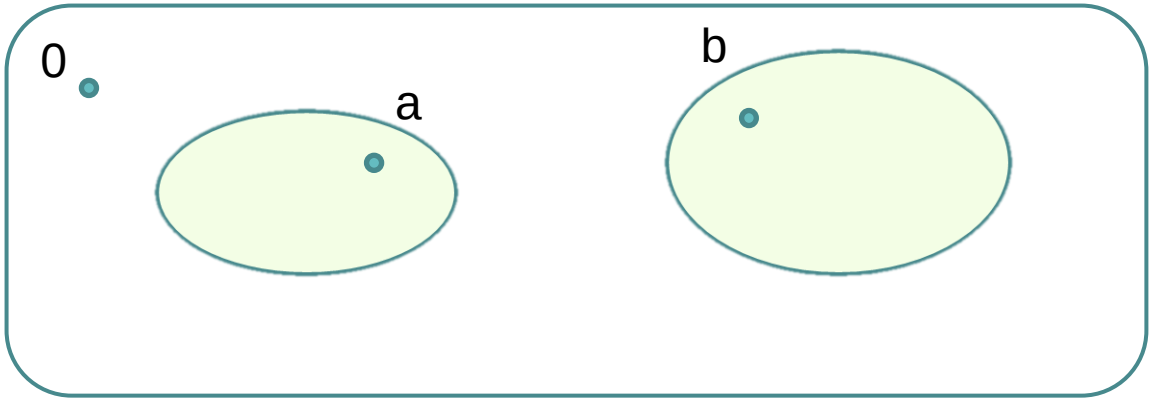
$F = F_2$ and $V = F^2 \oplus F^3$

- $H = GL(F^2) \times GL(F^3)$
- $H = \{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \mid A \in GL(F^2), B \in GL(F^3) \}$

- Nonzero $a_0 \in F^2, b_0 \in F^3$
- $a = (a_0, 0), b = (0, b_0)$
- Then $|a^H| = 3, |b^H| = 7$

Tiniest Example

- Coprime orbits and
- All remaining nonzero vectors form one more H-orbit
- $|(a+b)^H| = 21$



Joint work with Silvio Dolfi, Bob Guralnick and Pablo Spiga

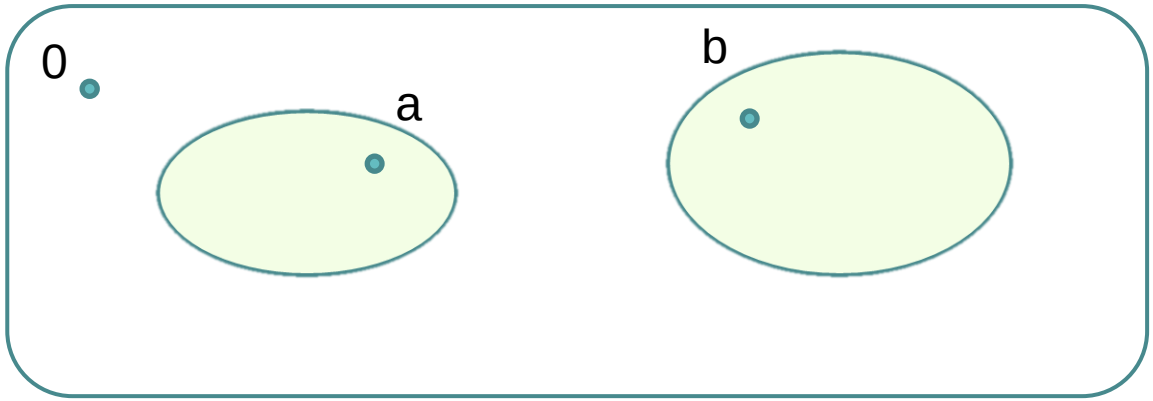


- Navarro's question: Suppose that (finite) H < GL(V) is completely reducible
- and suppose that H has coprime orbits in V of lengths m and n.
- Must H also have an orbit in V of length mn?

V

$a^H = \{ a^h \mid h \text{ in } H \}$

$b^H = \{ b^h \mid h \text{ in } H \}$

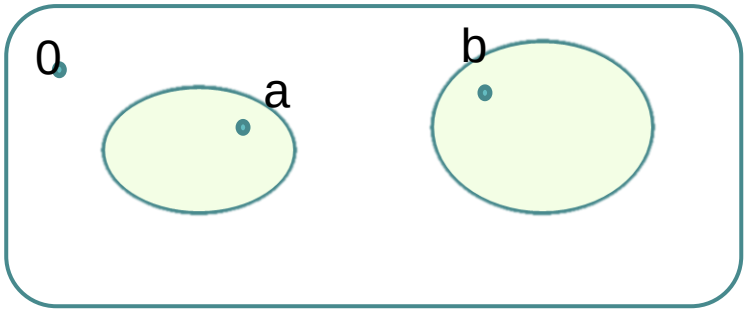


Cannot remove the condition "completely reducible"

Navarro's question: Suppose that H < GL(V) is completely reducible
[that is V = direct sum of irreducible FH-modules]
and that H has coprime orbits in V of lengths m and n.
Must H also have an orbit in V of length mn?

- $V = (F_p)^2$, any p, $H = \{ \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} \mid x, y \in F, \ x \neq 0 \}$
- Still: ONLY H-invariant subspaces are $V, \{(0,0)\}, and \ \langle (1,0) \rangle$
- Then H-orbit lengths: 1, p-1, and p-1 orbits of length p
- That is, H has coprime orbit lengths p, p-1 and no orbit of length p(p-1)

There are many examples



Some natural examples

- Take $V = U \oplus W$
- Take $K \leq GL(U)$ with orbit a_0^K of length m and
- $L \leq GL(W)$ with orbit b_0^L of length n where gcd(m, n) = 1

- Then $H = K \times L < GL(U \oplus W)$ has orbits
- $a^H = (a_0, 0)^H = (a_0, 0)^{K \times 1}$ of length m, $b^H = (0, b_0)^H = (0, b_0)^{1 \times L}$ of length n, and consider $a + b = (a_0, b_0)$
- $(a + b)^H = \{ (u, w) \mid u \in a_0^K,\ w \in b_0^L \}$ of length m n

- Question: do all examples of coprime H-orbits arise “more or less like this” ?

Summary of the outcomes: **what I'll discuss in the lecture**

- ↘ We answered Gabriel Navarro's question affirmatively
- ↘ We discovered a fact [to us, surprising] about finite irreducible linear groups
- ↘ Proofs used simple group classification + representation theory
- ↘ Results led us to study an old theme concerning permutation groups (going back to 1935)

Translate comments to results:

Theorem 1

Suppose that a finite group $H < GL(V)$ is completely reducible and that a^H and b^H are coprime H-orbits of lengths m and n. Then $(a+b)^H$ has length m n.

Theorem 2 [The "irreducible theorem".]

Suppose that a finite group $H < GL(V)$ is irreducible. Then H cannot have coprime orbits.

- Theorem 2 was unexpected, for us.
- Critical component of proof of Theorem 1
- Required careful use of simple group classification for its proof

“Irreducible Theorem 2”: Reduction to simple groups H

- Suppose “Irreducible Theorem 2” is true when H is a simple group
  - That is assume simple irreducible groups H do not have coprime orbits

- Try to prove Theorem 2 in general:
  - Assume H irreducible and H has coprime orbits. a^H and b^H
  - We need to get a contradiction, so
  - Assume that H has least order with these properties

  - Then H is not simple.
  - Let N be a nontrivial proper normal subgroup of H

“Irreducible Theorem 2”: Reduction – some hints

- H is irreducible and has coprime orbits a^H and b^H

- *Representation theory:* $V = \bigoplus_{i=1}^{r} W_i$ with W_i homogeneous FN-module
- Write $a = a_1 + \cdots + a_r$ and $b = b_1 + \cdots + b_r$
- Some a_i and b_k are non-zero as a, b non-zero.
- As H permutes the W_i transitively we can replace a, b by some H-images(and keep the same H-orbits) so that a_1 and b_1 are non-zero

- *Little more argument gives:*
- N-orbit lengths $|a_1^N|$ and $|b_1^N|$ in W_1 are > 1 and divide $|a^H|$ and $|b^H|$ resp., hence coprime

“Irreducible Theorem 2”: Reduction – some more hints

- Hence $|a_1^N|$ and $|b_1^N|$ are coprime N-orbits in W_1 but maybe N not irreducible on W_1

- *After yet more argument find:*
  - irreducible FN-submodule U of W_1
  - And vectors $a_0, b_0 \in U$ such that a_0^N and b_0^N are coprime N=orbits in U

- Then because N < H and because |H| is minimal for a linear irreducible group with coprime orbits, we get a contradiction.

Sufficient to prove “Irreducible Theorem 2” for simple groups H

How did we prove "Irreducible Theorem" for the simple groups

- **Assume:** H irreducible with coprime orbits a^H and b^H of lengths m and n
- And H is [nonabelian] simple

- Stabilisers H_a of a, H_b of b, have coprime indices $m = |H : H_a|$ and $n = |H : H_b|$
- So get "coprime factorisation" $H = H_a H_b$

- [Our first proof involved classifying all maximal coprime factorisations of the simple groups – followed by a horrible analysis]

- Representation Theoretic Lemma: Suppose that
  - H < GL(V) is irreducible
  - H=AB is a coprime factorisation
  - **Each element h in H is conjugate to h^{-1} in Aut(H)**
- Then either A fixes no non-zero vector or B fixes no non-zero vector

So for our simple group H, one of A or B cannot be the stabilizer of a vector!
So "purple condition" cannot hold

Using these ingredients

- Each classical simple group and each alternating group satisfies:

  Each element h in H is conjugate to h^{-1} in Aut(H)

- So Lemma implies H must be Sporadic or Exceptional

- Exceptional Lie type groups: all maximal factorisations classified [Hering, Liebeck, Saxl]
  - none are coprime [how lucky is that!]

- Sporadic simple groups: all factorisations classified [Giudici]
  - Only coprime ones are for M_{11}, M_{23} or M_{24}
  - Irritating ad hoc analysis completes proof

- So Irreducible linear groups do not have coprime orbits on vectors

Using “Irreducible Theorem” to prove Navarro’s Conjecture

- **Assume:** H finite and completely reducible on V with coprime orbits a^H and b^H of lengths m and n

- **Some Reductions:**
  - Some delicate argument allows us to reduce to the case:

  - V= FH(a) + FH(b) [not necessarily a direct sum] where
  - FH(a), is smallest H-invariant subspace containing a
  - FH(b), is smallest H-invariant subspace containing b

Using “Irreducible Theorem” to prove Navarro’s Conjecture

↘ **Good Case:** $FH(a) \cap FH(b) = 0$

- Here $(a+b)^H = a^H + b^H$ and has length m n – what we want!

↘ **Bad Case:** $FH(a) \cap FH(b)$ contains irreducible FH-submodule S

- With a lot of care we find $a_S, b_S \in S$ such that
- a_S^H and b_S^H are coprime H-orbits for the irreducible H-action on S

- Contradiction to the “Irreducible Theorem”! And completes the proof.

Another way of thinking about the “Irreducible Theorem”

- Let T(V) be the group of translations of V $t_v: x \to x + v$

- If H < GL(V) irreducible then G := T(V).H is primitive permutation group on V of affine type,
- and H is the stabiliser of 0, and H-orbits are “suborbits” [orbits of point stabiliser H]

- “Irreducible Theorem” says finite affine primitive groups cannot have coprime subdegrees [subdegrees: lengths of stabiliser orbits]

Primitive permutation group: Only trivial invariant partitions of the point set.

Coprime subdegrees of primitive permutation groups

- Can finite primitive permutation groups have coprime subdegrees?
- Yes: pretty well studied
- Famous Example: Janko group J_1 on 266 points
  - Stabiliser PSL(2,11) has orbit lengths: 1 + 11 + 12 + 110 + 132
- Famous old result: Marie Weiss 1935
  - G finite primitive (and not cyclic of prime order)
  - If subdegrees are $1 = n_1 < n_2 \leq \ldots \leq n_r$ then $\gcd(n_i, n_r) > 1$ for $i > 1$

Coprime subdegrees of primitive permutation groups

- Peter Neumann's 1973 reinterpretation of proof of Marie Weiss
  - G finite primitive (and not cyclic of prime order)
  - If subdegrees are $1 = n_1 < n_2 \leq \ldots \leq n_r$ and if k of the n_i are pairwise coprime then rank $r \geq 2^k$
- Janko group example: r = 5, k = 2
  - Peter Cameron showed r=4, k=2 not possible
  - So Janko example has minimum rank r

- **Questions:**
  - What kinds of primitive groups can have coprime subdegrees? [affine no, almost simple yes, ...]
  - How big can Neumann's k be?

Theorem: Types of primitive groups with coprime subdegrees

↘ Affine	no	
↘ Almost simple	yes	
↘ Diagonal	no	
↘ Product type	yes	[build from almost simple examples]
↘ Twisted wreath	yes	[but only managed to construct one ex]

- ↘ **We asked a Question:** Are there a infinitely many Twisted wreath groups with coprime subdegrees?
- ↘ **Answered: yes!** [Chua, Giudici, Morgan, 2019]

CGM's examples involve T=PSL(2,q) and diagonals

Our Twisted Wreath Example

- TW groups G=N.H, acting on N; [N acts regularly, and H by conjugation]

- T = PSL(2,7)
- N = T^m with m = 168 so action on 168^{168} points!
- G = N.H with H = T wr S_2
- H permutes the simple direct factors of N with coset action of H on its index 168 subgroup L = Diag(T x T).2

- We constructed orbits of the stabiliser H of lengths
- 49 and 576 – note gcd(49,576)=1
- And confirmed by computer existence of a suborbit of length 49 x 576

How about Navarro's question does not carry over in general

Warning: If a primitive group G has coprime subdegrees m and n there is not necessarily one of length mn.

Example [Giudici]: G = HS primitive on 3850 points, with stabiliser 2^4.Sym(6) has subdegrees

1 + 15 + 32 + 90+ 120 + 160 + 192 + 240 + 240 + 360 + 960 + 1440

[none of length 15 x 32 = 480]

How big can k be? [k pairwise coprime subdegrees]

- At first we thought to try proving that k must be bounded
- Then we got brave: and proved that k is at most 2!

Theorem: It is not possible for a finite primitive permutation group to have a pairwise coprime triple of subdegrees

- Proof reduces to proving a slightly stronger result about simple group actions
- [actions occurring as normal subgroups of almost simple primitive groups – not necessarily primitive]

Thank you for listening

- Irreducible linear groups do not have coprime orbits
- Primitive permutation groups do not have coprime subdegree triples
- For completely reducible linear groups coprime orbit lengths m, n imply an mn orbit
- For permutation groups …?

Photo. Courtesy: Joan Costa joancostaphoto.com

Thank you

Photo. Courtesy: Joan Costa joancostaphoto.com

Assumption “primitive” cannot be removed

Example: $G = F_1 \times F_2 \times \ldots \times F_r$ with each F_i a Frobenius group

- $F_i = N_i K_i$ acts on $|N_i|$ points
- With stabiliser K_i having all nontrivial subdegrees $n_i := |K_i|$
- G acts in product action on $N = N_1 \times N_2 \times \ldots \times N_r$
- With stabiliser $K = K_1 \times K_2 \times \ldots \times K_r$
- K has pairwise coprime orbit lengths $n_1 , n_2 , \ldots , n_r$

The construction suggests an “independence” of these subdegrees

Definition: Call a subdegree d of a transitive group G faithful if a stabiliser acts faithfully on some orbit of length d

Faithful subdegrees

Definition: Call a subdegree d of a transitive group G faithful if a stabiliser acts faithfully on some orbit of length d

Theorem: A finite transitive permutation group G cannot have a triple of pairwise coprime faithful subdegrees.

Moreover, if the Fitting subgroup is nontrivial, then G cannot have a pair of coprime faithful subdegrees.

In particular finite linear groups cannot have “faithful coprime orbits”