

**Permutation representations
of finite simple groups:
Orbits of cyclic subgroups**

Milano, 13 May 2009

Johannes Siemons, UEA Norwich

Let $n \geq k$ be integers, k not a prime power. Consider a cyclic subgroup

$$C \subseteq \text{Sym}_n$$

in the symmetric group on $\{1..n\}$, of order k . Then the size of any C -orbit α^C divides k . We say that C has a **regular orbit** if $|\alpha^C| = |C|$ for some $\alpha \in \{1..n\}$.

Let $n \geq k$ be integers, k not a prime power. Consider a cyclic subgroup

$$C \subseteq \text{Sym}_n$$

in the symmetric group on $\{1..n\}$, of order k . Then the size of any C -orbit α^C divides k . We say that C has a **regular orbit** if $|\alpha^C| = |C|$ for some $\alpha \in \{1..n\}$.

We are interested in the following question: If C has no regular orbit on $\{1..n\}$, does there exist a simple group G , not an alternating group, such that

$$C \subset G \subset \text{Sym}_n?$$

The answer is that there should be no such simple group.

The answer is that there should be no such simple group.

Questions of this kind belong to a project in which Alex has been a leading force: **Recognition of finite simple groups by the properties of a single element.**

The answer is that there should be no such simple group.

Questions of this kind belong to a project in which Alex has been a leading force: **Recognition of finite simple groups by the properties of a single element.**

To recognize an almost simple permutation group by a single element becomes feasible due to the O'Nan Scott Theorem: If G is maximal, not containing Alt_n , with

$$G \subset \text{Sym}_n$$

then G belongs to one of 5 well-understood classes, or otherwise, is almost simple.

Therefore, given $g \in \text{Sym}_n$ with regular orbits, can we identify the primitive almost simple groups G with

$$\langle g \rangle \subset G \subset \text{Sym}_n?$$

The problem I first mentioned is a key step towards answering such questions. I will report about joint work with Alex Zaleskii.

Therefore, given $g \in \text{Sym}_n$ with regular orbits, can we identify the primitive almost simple groups G with

$$\langle g \rangle \subset G \subset \text{Sym}_n?$$

The problem I first mentioned is a key step towards answering such questions. I will report about joint work with Alex Zaleskii.

Initial Comments [1]: Let $C, B \subseteq A$ be finite groups. Then C has a regular orbit on the cosets of B in A if and only if

$$C \cap B^a \subseteq K$$

for some $a \in A$, where K is the core of B in A .

For cyclic C let the **square-free part** of the action be the subgroup C' such that if the prime p divides $|C : C \cap K|$ then p divides $|C' : C' \cap K|$ but not p^2 . A simple reduction is

Lemma: C has a regular orbit on the cosets of B in A if and only if C' has a regular orbit on this set.

There is much work on intersections of conjugacy classes of subgroups, and in some sense this is the main task in tackling the problem.

[2] : Let (G, Ω) be an action of the group G on the set Ω . Denote $F := \mathbb{C}$ and consider the permutation module $F\Omega$ for FG . For cyclic groups the permutation module is crucial in detecting regular orbits.

[2]: Let (G, Ω) be an action of the group G on the set Ω . Denote $F := \mathbb{C}$ and consider the permutation module $F\Omega$ for FG . For cyclic groups the permutation module is crucial in detecting regular orbits.

Lemma (Brauer, 1940): *Two $n \times n$ permutation matrices are conjugate in $GL(n, \mathbb{C})$ if and only if the corresponding permutations are similar (the same up to renaming) in Sym_n .*

In other words: for cyclic C we have $F\Omega \cong F\Delta$ as FC -modules if and only if $(C, \Omega) \cong (C, \Delta)$ as G -sets. This lemma turns out to be very useful for our purposes.

It is a **special case of a Theorem of Burnside**, we will come back to this later.

Example: Look at two elements of order 6. First take $g = (1, 2)(3, 4, 5)(6)$. It has eigenvalues λ_i , μ_j and ν satisfying $\lambda_i^2 = \mu_j^3 = \nu = 1$. Correspondingly,

$$F\Omega = 3I_1 + I_2 + I_3 + I_4.$$

It is a **special case of a Theorem of Burnside**, we will come back to this later.

Example: Look at two elements of order 6. First take $g = (1, 2)(3, 4, 5)(6)$. It has eigenvalues λ_i , μ_j and ν satisfying $\lambda_i^2 = \mu_j^3 = \nu = 1$. Correspondingly,

$$F\Omega = 3I_1 + I_2 + I_3 + I_4.$$

On the other hand, if $g = (1, 2, 3, 4, 5, 6)$ then its eigenvalues are the 6 distinct roots of unity and

$$F\Omega = I_1 + I_2 + I_3 + I_4 + I_5 + I_6.$$

The key observation is therefore that the cyclic C of order k has an orbit of length $k = |C|$ if and only if the module for a primitive k^{th} root of unity appears in $F\Omega$. Our version of the Burnside-Brauer Lemma is

The key observation is therefore that the cyclic C of order k has an orbit of length $k = |C|$ if and only if the module for a primitive k^{th} root of unity appears in $F\Omega$. Our version of the Burnside-Brauer Lemma is

Lemma (Siemons & Zalesski, 2002): *Let C be a cyclic permutation group on Ω . Then the number of regular orbits of C on Ω is the multiplicity of the regular module FC in $F\Omega$.*

PLAN FOR REMAINDER OF THIS TALK

- **Main Theorem**
- **Idea of the Proof**
- **Embeddings of Permutation Groups**

Main Theorem

Let G be an almost simple group, $X \subseteq G \subseteq \text{Aut } X$, with socle X . We are interested in the following two lists:

L1: G has a doubly transitive permutation representation:

- $\text{PSL}(n, q)$ on points/hyperplanes of projective space,
- Symplectic group $\text{Sp}(2n, 2)$ on Ω^+ and Ω^- ,
- Unitary group $\text{PSU}(3, q)$ on 1-dim isotropic subspaces,
- Suzuki group $\text{Sz}(q) = {}^2\text{B}_2(q)$ on points of inversive plane,
- Ree group $R(q) = {}^2\text{G}_2(q)$ on points of Ree unital,
- M_{11} , M_{12} , M_{22} , M_{23} , M_{24} , HS of degree 176, and Co_3 of degree 276.

L2: G is a classical group, not already listed in L1:

- Symplectic groups $\mathrm{PSp}(2n, q)$,
- Unitary groups $\mathrm{PSU}(n, q)$,
- Orthogonal groups $\mathrm{O}(2n + 1, q)$, $\mathrm{O}^+(2n, q)$, $\mathrm{O}^-(2n, q)$.

L2: G is a classical group, not already listed in L1:

- Symplectic groups $\text{PSp}(2n, q)$,
- Unitary groups $\text{PSU}(n, q)$,
- Orthogonal groups $\text{O}(2n + 1, q)$, $\text{O}^+(2n, q)$, $\text{O}^-(2n, q)$.

Let L be the union of L1 and L2 but remove any group whose socle is an alternating group. A group in L acts **non-trivially** on the set Δ if its socle is not the identity group on Δ .

L2: G is a classical group, not already listed in L1:

- Symplectic groups $\text{PSp}(2n, q)$,
- Unitary groups $\text{PSU}(n, q)$,
- Orthogonal groups $\text{O}(2n + 1, q)$, $\text{O}^+(2n, q)$, $\text{O}^-(2n, q)$.

Let L be the union of L1 and L2 but remove any group whose socle is an alternating group. A group in L acts **non-trivially** on the set Δ if its socle is not the identity group on Δ .

Theorem (Emmett, Siemons & Zaleski, 2000, '02, '10): *Let G be in L and suppose that G acts non-trivially on the set Δ . Then every cyclic subgroup of G has a regular orbit on Δ .*

It is expected that the theorem holds more generally for all almost simple groups with socle not equal to an alternating group.

It is expected that the theorem holds more generally for all almost simple groups with socle not equal to an alternating group.

Primitive groups in which cyclic subgroups do not have a regular orbit seem to be rare, unless the group is related to some action of an alternating group.

For instance, by direct computation one can see that in a primitive groups of degree < 50 all cyclic subgroups have regular orbits, unless the action is related to an alternating group.

Idea of the Proof

A mixture of the two techniques already mentioned is needed: intersections of conjugacy classes of subgroups and embeddings of permutation modules.

Idea of the Proof

A mixture of the two techniques already mentioned is needed: intersections of conjugacy classes of subgroups and embeddings of permutation modules.

1. Embeddings: Let G be in L_1 , acting doubly transitively on the set Ω . Suppose that G also acts non-trivially on some other set Δ . Consider the corresponding FG -modules $F\Omega$ and $F\Delta$. Let

$$\varphi: F\Omega \rightarrow F\Delta$$

be a non-zero FG -homomorphism. Then its kernel can only be 0 , I or $F\Omega - I$.

Proposition: *Let G be doubly transitive on Ω and let Δ be a transitive G -set. Then exactly one of the following is true:*

- (i) There exists an injective FG -homomorphism $\varphi: F\Omega \rightarrow F\Delta$,*
- (ii) $G = G_\omega \cdot G_\delta$ for all $\omega \in \Omega$ and $\delta \in \Delta$.*

Proposition: *Let G be doubly transitive on Ω and let Δ be a transitive G -set. Then exactly one of the following is true:*

- (i) There exists an injective FG -homomorphism $\varphi: F\Omega \rightarrow F\Delta$,*
- (ii) $G = G_\omega \cdot G_\delta$ for all $\omega \in \Omega$ and $\delta \in \Delta$.*

In particular, in the embedding case (i), if a cyclic subgroup C has a regular orbit on Ω then C has a regular orbit on Δ , by the Lemma on cyclic permutation modules. So we are done in this case.

Proposition: *Let G be doubly transitive on Ω and let Δ be a transitive G -set. Then exactly one of the following is true:*

- (i) There exists an injective FG -homomorphism $\varphi: F\Omega \rightarrow F\Delta$,*
- (ii) $G = G_\omega \cdot G_\delta$ for all $\omega \in \Omega$ and $\delta \in \Delta$.*

In particular, in the embedding case (i), if a cyclic subgroup C has a regular orbit on Ω then C has a regular orbit on Δ , by the Lemma on cyclic permutation modules. So we are done in this case.

In case (ii) all factorizations are known by the results of Liebeck, Praeger and Saxl. The list of factorizations is short, thankfully.

2. Intersections of conjugacy classes: Let G be in L1, acting doubly transitively on Ω and $\omega \in \Omega$. Let $C = \langle g \rangle$ be cyclic, square-free without loss. One needs to show that

$$C \cap (G_\omega)^a = 1$$

for some $a \in G$.

2. Intersections of conjugacy classes: Let G be in L1, acting doubly transitively on Ω and $\omega \in \Omega$. Let $C = \langle g \rangle$ be cyclic, square-free without loss. One needs to show that

$$C \cap (G_\omega)^a = 1$$

for some $a \in G$.

This requires case by case analysis. In the linear situation induction over the number of Jordan blocks of g on the underlying vector space can be used. Similar comments apply to the factorization case. This completes the list L1.

The groups in L2 all have rank 3 actions. However, as yet this can not be used. So also here intersection type arguments are needed. Technically quite involved!

Embeddings

Comment 1: As an example, let $G = PSL(n, p)$ acts on $\Omega =$ points of projective space. Let Δ be any other G -set, and assume that we are in the embedding case. Take some $g \in G$.

Embeddings

Comment 1: As an example, let $G = PSL(n, p)$ acts on $\Omega =$ points of projective space. Let Δ be any other G -set, and assume that we are in the embedding case. Take some $g \in G$.

How does g act on Δ ? For instance, if g is a transvection then some part of Δ looks exactly like Ω : many fixed points, with the remainder all cycles of length p .

Embeddings

Comment 1: As an example, let $G = PSL(n, p)$ acts on $\Omega =$ points of projective space. Let Δ be any other G -set, and assume that we are in the embedding case. Take some $g \in G$.

How does g act on Δ ? For instance, if g is a transvection then some part of Δ looks exactly like Ω : many fixed points, with the remainder all cycles of length p .

Similarly, let g be a Singer cycle. Again, some part of Δ looks exactly like Ω : at least one cycle of length $(p^n - 1)/(n - 1)$, with other shorter cycles, etc.

Embeddings

Comment 1: As an example, let $G = PSL(n, p)$ acts on $\Omega =$ points of projective space. Let Δ be any other G -set, and assume that we are in the embedding case. Take some $g \in G$.

How does g act on Δ ? For instance, if g is a transvection then some part of Δ looks exactly like Ω : many fixed points, with the remainder all cycles of length p .

Similarly, let g be a Singer cycle. Again, some part of Δ looks exactly like Ω : at least one cycle of length $(p^n - 1)/(n - 1)$, with other shorter cycles, etc.

QUESTION 1: Is it possible to identify G from such orbit statistics?

Comment 2: Moving on from cyclic subgroups of G , **does a nilpotent subgroup** have regular orbits?

Comment 2: Moving on from cyclic subgroups of G , **does a nilpotent subgroup** have regular orbits?

Theorem (B Bailey Hargraves, 1980): *Let V be a finite-dimensional space over $GF(q)$. Suppose that $D \subseteq GL(V)$ is nilpotent with $(|D|, q) = 1$. Then D has a regular orbit on V , apart from a short list of exceptions.*

Comment 2: Moving on from cyclic subgroups of G , **does a nilpotent subgroup** have regular orbits?

Theorem (B Bailey Hargraves, 1980): *Let V be a finite-dimensional space over $GF(q)$. Suppose that $D \subseteq GL(V)$ is nilpotent with $(|D|, q) = 1$. Then D has a regular orbit on V , apart from a short list of exceptions.*

So let $G = PSL(n, p)$ act on $\Omega =$ points of projective space, and suppose that a nilpotent $D \subset G$ has a regular orbit on Ω . Let again Δ be an arbitrary G -set, in the embedding case.

Comment 2: Moving on from cyclic subgroups of G , **does a nilpotent subgroup** have regular orbits?

Theorem (B Bailey Hargraves, 1980): *Let V be a finite-dimensional space over $GF(q)$. Suppose that $D \subseteq GL(V)$ is nilpotent with $(|D|, q) = 1$. Then D has a regular orbit on V , apart from a short list of exceptions.*

So let $G = PSL(n, p)$ act on $\Omega =$ points of projective space, and suppose that a nilpotent $D \subset G$ has a regular orbit on Ω . Let again Δ be an arbitrary G -set, in the embedding case.

QUESTION 2: Does C have a regular orbit on Δ ?

Here the lemma for permutation modules of cyclic groups can not be applied any longer. Instead we need to recall a theorem of Burnside that is not so well-known any longer.

If G acts on Ω and if $U \subseteq G$ let $\text{fix}_\Omega(U)$ be the number of elements $\omega \in \Omega$ fixed by **all** elements of U . (This function extends the permutation character to subgroups.)

Here the lemma for permutation modules of cyclic groups can not be applied any longer. Instead we need to recall a theorem of Burnside that is not so well-known any longer.

If G acts on Ω and if $U \subseteq G$ let $\text{fix}_\Omega(U)$ be the number of elements $\omega \in \Omega$ fixed by **all** elements of U . (This function extends the permutation character to subgroups.)

Theorem (Burnside, 1911): *Let (G, Ω) and (G, Δ) be permutation actions. Then $(G, \Omega) \cong (G, \Delta)$ if and only if $\text{fix}_\Omega(U) = \text{fix}_\Delta(U)$ for all subgroups U in G .*

Here the lemma for permutation modules of cyclic groups can not be applied any longer. Instead we need to recall a theorem of Burnside that is not so well-known any longer.

If G acts on Ω and if $U \subseteq G$ let $\text{fix}_\Omega(U)$ be the number of elements $\omega \in \Omega$ fixed by **all** elements of U . (This function extends the permutation character to subgroups.)

Theorem (Burnside, 1911): *Let (G, Ω) and (G, Δ) be permutation actions. Then $(G, \Omega) \cong (G, \Delta)$ if and only if $\text{fix}_\Omega(U) = \text{fix}_\Delta(U)$ for all subgroups U in G .*

THANK YOU

Proof: Let G_1, \dots, G_t be a system of representative for the conjugacy classes of subgroups of G . Let $\Omega_i := G/G_i$ be the corresponding G -sets, obtained by right multiplication. Suppose

$$\Omega = \sum n_i \Omega_i \text{ and } \Omega' = \sum n'_i \Omega_i$$

are G -sets with $\text{fix}_\Omega(U) = \text{fix}_{\Omega'}(U)$ for all subgroups U in G .

Proof: Let G_1, \dots, G_t be a system of representative for the conjugacy classes of subgroups of G . Let $\Omega_i := G/G_i$ be the corresponding G -sets, obtained by right multiplication. Suppose

$$\Omega = \sum n_i \Omega_i \text{ and } \Omega' = \sum n'_i \Omega_i$$

are G -sets with $\text{fix}_\Omega(U) = \text{fix}_{\Omega'}(U)$ for all subgroups U in G .

Let J be the set of all i for which $n_i \neq n'_i$. Select $j \in J$ so that G_j is maximal (wrt subconjugacy) among all G_i with $i \in J$. Then

$$0 = \text{fix}_\Omega(G_j) - \text{fix}_{\Omega'}(G_j) = \sum_{i \in J} (n_i - n'_i) \cdot \text{fix}_{\Omega_i}(G_j).$$

Proof: Let G_1, \dots, G_t be a system of representative for the conjugacy classes of subgroups of G . Let $\Omega_i := G/G_i$ be the corresponding G -sets, obtained by right multiplication. Suppose

$$\Omega = \sum n_i \Omega_i \text{ and } \Omega' = \sum n'_i \Omega_i$$

are G -sets with $\text{fix}_\Omega(U) = \text{fix}_{\Omega'}(U)$ for all subgroups U in G .

Let J be the set of all i for which $n_i \neq n'_i$. Select $j \in J$ so that G_j is maximal (wrt subconjugacy) among all G_i with $i \in J$. Then

$$0 = \text{fix}_\Omega(G_j) - \text{fix}_{\Omega'}(G_j) = \sum_{i \in J} (n_i - n'_i) \cdot \text{fix}_{\Omega_i}(G_j).$$

Now $\text{fix}_{\Omega_i}(G_j) \neq 0$ only if G_j is subconjugate to G_i . So, only if $i = j$ by maximality. Hence

$$0 = \sum_{i \in J} (n_i - n'_i) \cdot \text{fix}_{\Omega_i}(G_j) = (n_j - n'_j) \cdot \text{fix}_{\Omega_j}(G_j) > 0$$

which means that $J = \emptyset$.

