Primitive groups and regular cycles of group elements

Pablo Spiga
University of Milano
pablo.spiga@unimib.it

Banff, July, 2013

Groups will be finite.

In this talk we are interested in permutation groups, that is, subgroups of the symmetric group $\mathrm{Sym}(\Omega)$.

Most of our work applies to a large class of permutation groups (transitive permutation groups G admitting a system of imprimitivity $\mathcal{B}$ with G acting primitively and faithfully on $\mathcal{B}$): for simplicity we restrict to the case of G itself being primitive.

The order $|g|$ of a permutation $g \in \mathrm{Sym}(\Omega)$ is the least common multiple of the cycle lengths of g (when g is written as the product of disjoint cycles).

The permutation g has a regular cycle (or orbit) if g has a cycle of length equal to $|g|$.

The element $g = (1, 2, 3)(5, 6, 7, 8)(7, 10)$ has no regular orbit.
The element $g = (1, 2)(3, 4, 5)(6, 7, 8, 9, 10, 11)$ has a regular orbit: the point 6 lies in a cycle of length $|g| = 6$.

Scope of this talk

In this talk we are interested in classifying the finite primitive groups G such that, for each $g \in G$, the permutation g has a regular cycle.

In particular

$$|g| = \text{length of a longest cycle of } g.$$

Examples: $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ in its natural action on the k-subsets of $\{1, \ldots, n\}$.

- [$k = 1$] The permutation $g = (1,2)(3,4,5)$, in its natural action on $\{1, \ldots, n\}$, has no regular cycles.
- [$k = 2$] The permutation $g = (1,2)(3,4,5)(6,7,8,9,10)$, in its natural action on the 2-subsets of $\{1, \ldots, n\}$, has no regular cycles.
- [Any k] Let n_k be the sum of the first k prime numbers. Every element of $\mathrm{Sym}(n)$ in its action on k-subsets of $\{1, \ldots, n\}$ has a regular cycle if and only if $n < n_{k+1}$.

As k tends to infinity, n_k is asymptotic to $k^2 \log(k)/2$ (the rate of convergence is quite slow).

More examples: Let $W = H \operatorname{wr} \mathrm{Sym}(\ell)$ be endowed of its natural primitive product action, with $H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$ acting on the k-subsets of $\{1, \ldots, m\}$. Then, for m sufficiently large compared to k, the group W contains elements with no regular cycles.

Theorem

Let G be a finite primitive group on Ω and let $g \in G$. Then either g has a regular cycle, or G preserves a product structure on $\Omega = \Delta^\ell$ with Δ isomorphic to the set of k-subsets of a set of size m and $\mathrm{Alt}(m)^\ell \lhd G \leq \mathrm{Sym}(m)\, wr\, \mathrm{Sym}(\ell)$.

(Here we allow $\ell = 1$.)

The proof is a combination of the work of two teams:

- Michael Giudici, Cheryl Praeger, P. S. (reducing the problem to the case of G being an almost simple group), and
- Simon Guest and P. S. (settling the case of G being an almost simple group).

The inspiration to this work comes from a discussion during a coffee break with Alex Zalesski. Alex is interested in

Question

Let G be a permutation group on Ω, let H be a subgroup of G and let K be a field. Under what conditions does the permutation KG-module $K\Omega$ restricted to H contain a regular KH-module (that is, $K\Omega$ contains a KH-submodule isomorphic to the group algebra KH).

[Siemons-Zalesski] For H cyclic, KH is a submodule of $K\Omega$ if and only if H has a regular orbit in its action on Ω.

Our theorem was known

- for some families of 2-transitive groups (two papers of Siemons and Zalesski), and when
- G is a simple classical group (in the very hard an technical work of Emmett and Zalesski).

In the second case the hypothesis of G being a simple classical group is fundamental (the proof is by induction on the size of the Jordan blocks of g). In particular, it does not apply to the general case of almost simple classical groups.

The proof does carry over to the case of G being contained in the group of inner-diagonal automorphisms of a simple classical group.

Two very basic lemmas

Lemma

Let G be a permutation group on Ω. Assume that for every $g \in G$, with $|g|$ square-free, g has a regular cycle. Then, for every $g \in G$, g has a regular cycle.

Let G be a finite permutation group on Ω and let x be in G. We let

$$\mathrm{Fix}_\Omega(x) = \{\omega \in \Omega \mid \omega^x = \omega\} \quad \text{and} \quad \mathrm{fpr}_\Omega(x) = \frac{|\mathrm{Fix}_\Omega(x)|}{|\Omega|}.$$

Lemma

Let G be a transitive permutation group on Ω and let g be in G. The element g has a regular cycle if and only if

$$\bigcup_{\substack{p \mid |g| \\ p \text{ prime}}} \mathrm{Fix}_\Omega(g^{|g|/p}) \subsetneq \Omega.$$

In particular, if

$$\sum_{\substack{p \mid |g| \\ p \text{ prime}}} \mathrm{fpr}_\Omega(g^{|g|/p}) < 1,$$

then g has a regular cycle.

Example: exceptional groups of Lie type.

Proposition

Let G be a finite primitive group with socle an exceptional group of Lie type. If $g \in G$, then g has a regular cycle.

Sketch.

Case-by-case analysis on the Lie type of G.
Step 1: obtain an upper bound $P(G)$ on the maximal number of prime divisors of $|g|$ (for $g \in G \setminus \{1\}$). This is easily achieved by controlling the structure of the maximal tori of G.
Step 2: Lawther, Liebeck and Seitz have obtained a very explicit upper bound $F(G)$ for $\max\{\mathrm{fpr}_\Omega(x) \mid x \neq 1\}$.
Step 3: Check when $P(G)F(G) < 1$. For the (very few) cases where $P(G)F(G) \geq 1$ fire up magma. □

For this naive strategy to work we need a very sharp upper bound on $\mathrm{fpr}_{\Omega}(x)$ that does not depend on $|x|$ (for $x \neq 1$) and a small number of distinct prime divisors of $|x|$ (for $x \in G$). This works very rarely.

Reduction to the almost simple case (Michael Giudici, Cheryl Praeger, P. S.)

According to the O'Nan-Scott theorem, a primitive group G either

- preserves a cartesian decomposition of Ω; or
- G is of affine type; or
- G is of diagonal type; or
- G is almost simple.

The general strategy is to deal (in turn) with each of these cases and arguing by induction.

Cartesian product decomposition

Theorem

Let $H \leq \mathrm{Sym}(\Delta)$ such that each $h \in H$ has a regular cycle. Then each $g \in H\, wr\, \mathrm{Sym}(\ell)$ acting on Δ^ℓ has a regular cycle.

The proof is combinatorial and (in part) constructive. Given $g = (h_1, \ldots, h_\ell)\sigma$, with $h_1, \ldots, h_\ell \in H$ and $\sigma \in \mathrm{Sym}(\ell)$, our proof exhibits "excplicitly" an element $\omega = (\delta_1, \ldots, \delta_\ell)$ of Δ^ℓ on which g induces a regular cycle. Here I am using the quotation marks because the construction depends on exhibiting excplicitly an element δ_i of Δ on which h_i induces a regular cycle. The definition of the element ω depends on the conjugacy class of g.

Affine groups

Here G is a subgroup of the affine general linear group $\mathrm{AGL}_d(q)$.

Lemma

Let $g \in \mathrm{GL}_d(q)$. Write $V = \mathbb{F}_q^d$ and

$$\mathcal{S}_g = \{v \in V \mid v \,\text{lies in a regular cycle of}\, g\}.$$

Then $\mathcal{S}_g$ spans the vector space V.

Corollary

Let $g \in \mathrm{AGL}_d(q)$. Then g has a regular cycle.

Diagonal groups

Theorem

Let G be a primitive group of diagonal type and let $g \in G$. Then g has a regular cycle.

Here the proof is very technical and at a critical juncture we need a theorem of Potter: an automorphism of a non-abelian simple group cannot invert more than $4/15$ of its group elements (the equality is met only for $\mathrm{Alt}(5)$).

Corollary

Let T be a non-abelian simple group and let σ be an automorphism of T. Then σ induces at least one regular orbit in its action on T.

Almost simple groups G (Simon Guest, P. S.)

The proof is (again) a case-by-case analysis depending on the non-abelian simple socle of G.
The socle of G is a sporadic simple group: the proof uses detailed description of the maximal subgroups of G and the following observation:

Lemma

Let G be a transitive group on Ω and let g be in $G \setminus \{1\}$. Assume that the derived subgroup of G is transitive. Then, there exists a non-principal constituent χ of the permutation character of G with

$$\mathrm{fpr}_\Omega(g) \leq \frac{1 + |\chi(g)|}{1 + \chi(1)}.$$

- The socle of G is an exceptional group of Lie type: done (bounds on fixed-point-ratios and estimate on element orders);
- The socle of G is an alternating group: the proof is a combination of combinatorial methods (for the actions on uniform partitions) and of bounds on fixed-point-ratios (for the actions on the cosets of a primitive subgroup).

The socle of G is an almost simple classical group

Definition

Let G be an almost simple classical group with socle G_0 and with natural module V over a field of prime characteristic p. A subgroup H of G is a *subspace subgroup* if for each maximal subgroup M of G_0 containing $H \cap G_0$ one of the following holds:

(a) M is the stabilizer in G_0 of a proper non-zero subspace U of V, where U is totally singular, or non-degenerate, or, if G_0 is orthogonal and $p = 2$, a non-singular 1-space (U can be any subspace if $G_0 = \mathrm{PSL}(V)$);

(b) $M = \mathrm{O}^{\pm}_{2m}(q)$ and $(G_0, p) = (\mathrm{Sp}_{2m}(q)', 2)$.

Theorem (Burness)

Let G be a finite almost simple classical group acting transitively and faithfully on a set Ω with point stabilizer $G_\omega \leq H$, where H is a maximal non-subspace subgroup of G. Then

$$\mathrm{fpr}_\Omega(x) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota},$$

for all elements $x \in G$ of prime order (where ι and n depend on the Lie type of G).

Using this theorem we reduced the general problem to subspace actions.

A reduction for subspace actions

Lemma

Let G be a finite group with two permutation representations on the finite sets Ω_1 and Ω_2. For $i \in \{1,2\}$, let π_i be the permutation character for the action of G on Ω_i, and suppose that $\pi_1 \leq \pi_2$. Given $g \in G$, if g has a cycle of length $|g|$ on Ω_1, then g has a cycle of length $|g|$ also on Ω_2.

In a nutshell: to prove our theorem we may consider only those actions having a permutation character that is minimal.

Theorem (Frohart, Guralnick, Magaard)

Let G be an almost simple classical group with natural module V of dimension n. If G is linear, assume that G does not contain a graph automorphism. Let $k \in \{2, \ldots, n-1\}$, and let K be the stabilizer of a nondegenerate or totally singular k-subspace of V. Let P be the stabilizer of a singular 1-space of V. Then $1_P^G \leq 1_K^G$ unless one of the following holds.

(1) *K is the stabilizer of a maximal totally singular subspace of V.*

(2) *K is the stabilizer of a 2-subspace containing no singular points or the orthogonal complement of such.*

The rest of the proof uses results of Guralnick and Kantor: for a classical group in one of its subspace actions, they bound $\mathrm{fpr}_{\Omega}(x)$ depending on the conjugacy class of x.

Corollary

Let G be a finite primitive group on Ω and let $g \in G$. Then either $|g| \leq |\Omega|$, or G preserves a product structure on $\Omega = \Delta^{\ell}$ with Δ isomorphic to the set of k-subsets of a set of size m and $\mathrm{Alt}(m)^{\ell} \lhd G \leq \mathrm{Sym}(m)\, wr\, \mathrm{Sym}(\ell)$.

(Here we allow $\ell = 1$.)