Factorizing finite primitive groups with point stabilizers

Martino Garonzi
University of Brasilia (UnB)

Joint work with
Attila Maróti, Dan Levy, Iulian Simion

Groups St. Andrews conference in Birmingham
08/08/2017

The idea of the subject matter is simple: suppose you have a finite group G and a maximal subgroup H of G that is not normal in G. Then H together with its conjugates generates G, so G is a product of a number of conjugates of H: there exist $x_1, \dots, x_m \in G$ such that

$$G = H^{x_1} H^{x_2} \cdots H^{x_m} = \{h_1^{x_1} h_2^{x_2} \cdots h_m^{x_m} \ : \ h_1, h_2, \dots, h_m \in H\}.$$

The question we pose here is what is the minimal m for which this is possible, in terms of the total number of conjugates of H, which is the index $n = |G : H|$. We proved a logarithmic bound.

Looking at G/H_G we may actually assume that G is a so-called primitive group.

All groups in this talk will be finite.

If $H \leq G$ and $H^G = G$ (meaning that the conjugates of H generate G) then G is the setwise product of some conjugates of H (this is an easy exercise), at least $\log|G|/\log|H|$ of them (this is because if G is a product of m conjugates of H then $|G| \leq |H|^m$).

The following is an open problem.

Conjecture (Liebeck, Nikolov, Shalev)

If G is a nonabelian simple group and $1 \neq H \leq G$ then G is the product of no more than $c \log|G|/\log|H|$ conjugates of H, where c is a universal constant.

Here we look for a logarithmic bound when G is a primitive group and H is a point stabilizer. What we prove is the following.

Theorem (G., Levy, Maróti, Simion)

There exists a universal constant c such that if G is any primitive permutation group of degree n with a non-trivial point stabilizer H then G is a product of at most $c \log n$ conjugates of H.

Definition

Let S_n, the symmetric group of degree n, act naturally on $\Omega = [n] = \{1, \dots, n\}$.

A ***primitive group*** *of degree n is a group $G \leq S_n$ such that there is no $S \subseteq \Omega$ with $1 < |S| < n$ such that for all $g \in G$ either $S = S^g$ or $S \cap S^g = \emptyset$. Such S is called a* ***block*** *of the action.*

In other words, G is primitive if it does not have nontrivial blocks.

Note that any orbit of G is a block. This implies that if $n \geq 3$ then the action of G is transitive.

Primitive groups play the role of the “irreducible” permutation groups.

Let G be a primitive group and let $H \leq G$ be a point stabilizer of the action of G. In other words $H = \{g \in G \ : \ \alpha^g = \alpha\}$ where $\alpha \in \Omega$.

The given action (at least when $n \geq 3$) is equivalent to the action of right multiplication on the set $\{Hx \ : \ x \in G\}$, so we can identify this set with Ω.

H is maximal in G. This is because if $H \leq K \leq G$ then $\{Hx \ : \ x \in K\}$ is a block.

Also, H is core-free in G, meaning that $\bigcap_{g \in G} H^g = \{1\}$. This is because the action of G on Ω is faithful.

So basically we want to study the factorizations of a finite group as a product of conjugates of a maximal subgroup.

Our result is the following.

Theorem

There exists a constant c such that if G is any primitive permutation group of degree n with nontrivial point stabilizer H then G is the product of at most $c \log n$ conjugates of H (point stabilizers).

We sketch the proof of this result. The strategy is to use the O'Nan-Scott theorem, which is a classification theorem of primitive permutation groups. This theorem is long to state in full detail. We will consider all the possibilities separately and the statement of the classification theorem will be implicit in this sketch.

Let $\gamma_{cp}^{H}(G)$ denote the minimal m such that there are m conjugates of H whose product is G.

Let $[n] = \Omega = \{1, \ldots, n\}$, $H = G_\alpha$ the stabilizer of $\alpha \in \Omega$. Then $n = |G : H|$.

Let B be the socle of G, that is, the subgroup of G generated by the minimal normal subgroups of G. B is a direct power T^k of a simple group (this is not true in general, but it is true for primitive groups).

We have $B \trianglelefteq G$, and an orbit of B in Ω is a block for G. This implies that B acts transitively. Now if $g \in G$ then by transitivity there is some $b \in B$ with $\alpha^{gb} = \alpha$, so $gb \in H$. This argument shows that $G = BH$. This easily implies that if B is contained in a product of t conjugates of H then G is a product of t conjugates of H. In other words

$$\gamma_{cp}^{H}(G) \leq \gamma_{cp}^{B_\alpha}(B)$$

where $B_\alpha = B \cap G_\alpha$. We can use this bound if $B_\alpha \neq \{1\}$, that is, if B does not act regularly.

This means that B is abelian. Equivalently, G has only one minimal normal subgroup $B = V$ and it is abelian. This implies that $V \cong {C_p}^l$ for some prime p and some positive integer l.

Let $v \in V$ be a nonzero vector. Since H is not normal in G, V is not central. Let $h \in H$ be such that $v^h \neq v$ and let $w := v^{h^{-1}} - v$. Then $w \neq 0$. Since H acts irreducibly on V, there exists a base B of V of the form $B = \{w^{h_1}, \ldots, w^{h_l}\}$ where $h_1, \ldots, h_l \in H$, so that

$$\langle w^{h_1} \rangle \cdots \langle w^{h_l} \rangle = V.$$

Since $n = p^l$ we are left to show that $\langle w \rangle$ is contained in a product of at most $c \log p$ conjugates of H. Now,

$$w = v^{h^{-1}} - v = v^{-1} h v h^{-1} \in H^v H$$

so in principle $\langle w \rangle = \{sw \ : \ s \in \mathbb{F}_p\}$ is contained in a product of $2p$ conjugates of H. However we can get this p to $\log p$ by using the base 2 representation of p using $\log p$ binary digits.

O'NAN-SCOTT TYPE II. **ALMOST SIMPLE CASE**.

This means that $B = T^k$ is nonabelian and $k = 1$, in other words $B = T$ is a nonabelian simple group. Up to technicalities, in this case the result is a consequence of the existing partial results concerning the Liebeck-Nikolov-Shalev conjecture.

O'NAN-SCOTT TYPE III(A). **DIAGONAL TYPE CASE.**

This means that B_α is the diagonal subgroup of $B = T^k$, $B_\alpha = \Delta = \{(t,t,\dots,t) \ : \ t \in T\}$.

Then $n = |G : G_\alpha| = |B : B_\alpha| = |T|^{k-1}$. Since $\gamma_{cp}^{H}(G) \leq \gamma_{cp}^{B_\alpha}(B)$ it is enough to find a linear bound of $\gamma_{cp}^{B_\alpha}(B)$ in terms of k.

We claim that $\gamma_{cp}^{B_\alpha}(B) \leq 3k-2$. As it is easily seen, this gives the bound we are interested in.

For this we need a result of Guralnick and Malle, namely that there are some α, β, γ in T such that $\alpha^T \beta^T \gamma^T = T$ where x^T denotes the conjugacy class of $x \in T$ in T. Setting $B = T^k = T_1 \times \cdots \times T_k$ and $\tau_i : T \to T_i$ the canonical embedding, $a = \alpha^{-1}$, $b = \beta^{-1}\alpha^{-1}$ we have that $D_i := \Delta\Delta^{\tau_i(a)}\Delta^{\tau_i(b)}\Delta$ contains T_i.

Therefore $B = T_1 T_2 \cdots T_k = \Delta T_2 \cdots T_k \subseteq D_2 \cdots D_k$ and this is a product of $3(k-1)+1 = 3k-2$ conjugates of Δ.

O'NAN-SCOTT TYPE III(B). **PRODUCT ACTION TYPE**.

Let R be a primitive permutation group of type II or III(a) on a set Γ. For $l > 1$ let $W = R \wr \mathrm{Sym}(l)$ and take W to act on $\Omega = \Gamma^l$ in its natural product action. Then for $\gamma \in \Gamma$ and $\alpha = (\gamma, \dots, \gamma) \in \Omega$ we have $W_\alpha = R_\gamma \wr \mathrm{Sym}(l)$ and $n = |\Gamma|^l$. If K is the socle of R then the socle of W is $B = K^l$ and $B_\alpha = (K_\gamma)^l \neq \{1\}$.

G is primitive of type III(b) if $B \leq G \leq W$ and acts transitively on the l factors of $B = K^l$. By cases II, III(a) K is a product of at most $c \log |K : K_\gamma|$ conjugates of K_γ. Now $n = |\Omega| = |\Gamma|^l$ and so K is transitive on Γ, $|\Gamma| = |K : K_\gamma|$. Hence

$$\gamma_{cp}^{H}(G) \leq \gamma_{cp}^{B_\alpha}(B) \leq c \log |K : K_\gamma| \leq cl \log |K : K_\gamma| = c \log n.$$

O'NAN-SCOTT TYPE III(C). **TWISTED WREATH PRODUCT TYPE.**

Let P be a transitive permutation group of degree k and let $Q \leq P$ be a point stabilizer. Let $\varphi : Q \to \mathrm{Aut}(T)$ be a homomorphism such that $\varphi(Q)$ contains all the inner automorphisms of T. Let B_0 be the set of functions $f : P \to T$ such that $f(pq) = f(p)^{\varphi(q)}$ for all $p \in P$, $q \in Q$. Then B_0 is a group with pointwise multiplication and $B_0 \cong T^k$.

P acts on B_0 as follows: if $f \in B_0$ and $p \in P$ define $f^p(x) := f(px)$ for all $x \in P$. The semidirect product $G := B_0 \rtimes P$ is called the twisted wreath product (of P and T). If P is maximal in G then the action of G on the set of right cosets of P is primitive and G belongs to class III(c).

By the Guralnick-Malle result we can write $T_i = t_{i1}^{T_i} t_{i2}^{T_i} t_{i3}^{T_i}$ where $B_0 = T^k = T_1 \cdots T_k$. Let $O_{ij} := \{p^{-1} t_{ij} p \ : \ p \in Q_i\}$ for $j = 1, 2, 3$. Since $Inn(T) \leq \varphi(Q)$, $O_{ij} \supseteq t_{ij}^{T_i}$, so setting $X_{ij} = t_{ij}^{-1} O_{ij}$ we have $X_{i1} X_{i2} X_{i3} = T_i$ and $X_{ij} \subseteq P^{t_{ij}} P$. Therefore $B_0 = T_1 \cdots T_k$ is contained in a product of $6k$ conjugates of P. Since $n = |G : P| = |B_0| = |T|^k$ this gives the result.