PRIMITIVE PERMUTATION GROUPS AS PRODUCTS OF POINT STABILIZERS

MARTINO GARONZI, DAN LEVY, ATTILA MARÓTI, AND IULIAN I. SIMION

ABSTRACT. We prove that there exists a universal constant c such that any finite primitive permutation group of degree n with a non-trivial point stabilizer is a product of no more than $c \log n$ point stabilizers.

1. Introduction

Given a finite group G [1] and a subgroup H of G whose normal closure is G, one can show, by a straightforward elementary argument, that G is the setwise product of at least $\frac{\log|G|}{\log|H|}$ conjugates of H. A far reaching conjecture of Liebeck, Nikolov and Shalev states [8] that in the case that G is a non-abelian simple group, $\frac{\log|G|}{\log|H|}$ is in fact the right order of magnitude for the minimal number of conjugates of H whose product is G, namely, there exists a universal constant c such that for any non-abelian simple group G and any non-trivial $H \leq G$, the group G is the product of no more than $c\frac{\log|G|}{\log|H|}$conjugates of H. Later on, in [9], this conjecture was extended to allow H to be any subset of G of size at least 2. Some weaker versions of these conjectures are proved in [8, Theorem 2], [9, Theorem 3], and [4, Theorem 1.3].

Here we look for a universal upper bound on the minimal length of a product covering of a finite primitive permutation group by conjugates of a point stabilizer. We will prove the following logarithmic[2] bound:

Theorem 1. *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.*

Note that in most relevant cases, $\frac{\log|G|}{\log|H|} < \log|G:H| = \log n$ (see Lemma 2.1). Thus we do not know whether the bound provided by Theorem 1 is the best possible. In fact, on the basis of currently published results we don't even know if this bound can be improved for any particular O'Nan-Scott family of primitive groups. We believe that these questions deserve further investigation.

Date: May 5, 2016.

2000 *Mathematics Subject Classification.* 20B15, 20D40 .

Key words and phrases. primitive groups, products of conjugate subgroups.

MG acknowledges the support of the University of Brasilia.

AM was supported by the MTA Rényi Lendület Groups and Graphs Research Group and by OTKA grants K84233 and K115799.

IS acknowledges the support of the University of Padova (grants CPDR131579/13 and CPDA125818/12).

[1]All groups discussed are assumed to be finite.

[2]Throughout the paper, log stands for logarithm in base 2.

2. Preliminaries

We collect some preparatory results and notation.

Lemma 2.1. *Let G be a group and $H \leq G$ such that $|H| \geq 4$ and $|G : H| \geq 4$. Then $\log|G| / \log|H| \leq \log|G : H|$.*

Proof. Set $x := \log|G|$ and $y := \log|H|$. Then the desired inequality reads $x/y \leq x - y$, which is equivalent to $x \geq y + 1 + \frac{1}{y-1}$. Since $y \geq 2$ because $|H| \geq 4$, this is clearly satisfied if $x \geq y + 2$, which is equivalent to $|G : H| \geq 4$. □

Lemma 2.2. *Let G be an almost simple group with socle T. Let M be a maximal subgroup of G and let $M_0 := T \cap M$. Then $|M_0| \geq 6$.*

Proof. We can assume that $T \nleq M$. Since G is almost simple, we have $M_0 \neq 1$ ([2, Theorem 1.3.6]) whence $|M_0| \geq 2$. Moreover, $M_0 \trianglelefteq M$, so by maximality of M, the fact that T is simple, and $1 < M_0 < T$, we get that $M = N_G(M_0)$ and $M_0 = M \cap T = N_T(M_0)$. Suppose, by contradiction, that $2 \leq |M_0| \leq 5$. Then M_0 is contained in a Sylow p-subgroup P of T where $p \in \{2, 3, 5\}$ according to the case. If $M_0 < P$ then $M_0 < N_P(M_0) \leq N_T(M_0) = M_0$ - a contradiction. Thus M_0 is a Sylow p-subgroup of T. But $2 \leq |M_0| \leq 5$ implies that M_0 is abelian so $M_0 \leq C_T(M_0) \leq N_T(M_0) = M_0$. Thus $M_0 = Z(N_T(M_0))$, and by Burnside's p-complement theorem ([11, 10.21]), M_0 has a normal p-complement in T - a contradiction since T is simple. □

The following lemma is an easy corollary to a major result of [5]. Let x^G denote the conjugacy class of x in G.

Lemma 2.3. *Let T be a non-abelian simple group. Then there exist $\alpha, \beta \in T$ such that $T = \alpha^T \beta^T S$, where S is any subset of T of size at least 2. In particular, there exist $\alpha, \beta \in T$ such that $T = \alpha^T \beta^T \gamma^T$ where $\gamma := \beta^{-1}\alpha^{-1}$.*

Proof. By [5, Theorem 1.4] there exist $\alpha, \beta \in T$ with $\alpha^T \beta^T \cup \{1\} = T$. If $\alpha^T \beta^T = T$ then we are done. Otherwise, $\alpha^T \beta^T = T - \{1\}$, and since for any $s \in T$ we have $(T - \{1\}) s = T - \{s\}$, we get that for any $s_1 \neq s_2 \in S$ we have $\alpha^T \beta^T s_1 \cup \alpha^T \beta^T s_2 = T$ and $T = \alpha^T \beta^T S$ follows. For proving $T = \alpha^T \beta^T \gamma^T$ (for the same choice of $\alpha, \beta \in T$) we can assume $\alpha^T \beta^T = T - \{1\}$. Hence $\gamma \neq 1$, implying $|\gamma^T| \geq 2$. Now $T = \alpha^T \beta^T \gamma^T$ follows by taking $S = \gamma^T$ in the first claim. □

Notation 1. *We denote by $\gamma_{\mathrm{cp}}^H(G)$ the minimal positive integer m such that there exist m conjugates of $H \leq G$ whose product is G ($\gamma_{\mathrm{cp}}^H(G) = \infty$ if G is not a product of conjugates of H).*

For the proof of Theorem 1 we use the classification of finite primitive permutation groups as given by the O'Nan-Scott theorem, for which we adopt the formulation and notation of [10]. Thus G is assumed to be a primitive permutation group on a set Ω of size $n = |G : H|$ where $H = G_\alpha$ is the stabilizer of some $\alpha \in \Omega$. The socle of G is denoted $B \cong T^k$ with $k \geq 1$, where T is a simple group. Since B acts transitively on Ω (being a non-trivial normal subgroup of a primitive group), we have $G = BG_\alpha = BH$. Suppose that B is contained in the product of t conjugates of H. Then G is a product of t conjugates of H (see [3, Lemma 7(2)]). Moreover, since $B_\alpha = B \cap H \leq H$, we get that B is certainly contained in the product of $\gamma_{\mathrm{cp}}^{B_\alpha}(B)$ conjugates of H. These considerations show that $\gamma_{\mathrm{cp}}^{G_\alpha}(G) \leq \gamma_{\mathrm{cp}}^{B_\alpha}(B)$ while

$n = |G : G_\alpha| = |B : B_\alpha|$ and so in the cases where B does not act regularly on Ω we will prove our claim by exhibiting a suitable upper bound on $\gamma_{\mathrm{cp}}^{B_\alpha}(B)$ (if B acts regularly, $B_\alpha = 1$ and $\gamma_{\mathrm{cp}}^{B_\alpha}(B) = \infty$). Also note that since for any integer m there are only finitely many isomorphism types of finite groups A such that $|A| \leq m$, for all primitive groups G satisfying $|G| \leq m$ we get that $\gamma_{\mathrm{cp}}^{B_\alpha}(B)$ is bounded above by some constant depending on m, and so we may assume, that $|B| = |T|^k > m$ for any fixed choice of m.

3. **Type** I. G is an affine primitive permutation group

Proposition 3.1. *Let G be an affine primitive permutation group with a non-trivial point stabilizer H. Then G is a product of at most $1 + c_A \log|G : H|$ conjugates of H, where $0 < c_A \leq 3/\log 5 < 1.3$ is a universal constant.*

In order to prove Proposition 3.1, we review some basic properties of affine primitive permutation groups. If G is an affine primitive permutation group, then it has exactly one minimal normal subgroup V, which is abelian so $V \cong C_p^l$ for some prime p and some natural number l. Moreover $G = VH$ and, viewing V as the vector space over $\mathbb{F}_p$, then H acts by conjugation irreducibly as a group of linear transformations on V. When convenient we will use additive notation for V.

Lemma 3.2. *Let G be an affine primitive permutation group with point stabilizer H and minimal normal subgroup $V \cong C_p^l$. Let $h \in H$ and $v \in V$. Set $w := v^{h^{-1}} - v$ and $k := \lceil \log p \rceil$. Then $\langle w \rangle$ is contained in a product of $k+1$ conjugates of H.*

Proof. We can assume $w \neq 0_V = 1_G$ for which the claim clearly holds. Then w is of order p, and any element of $\langle w \rangle$ is of the additive form sw where the integer s satisfies $0 \leq s \leq p-1$. Since $k := \lceil \log p \rceil$, the base 2 representation of s takes the form $s = \sum_{j=0}^{k-1} b_j 2^j$ ($b_j \in \{0,1\}$ for all $0 \leq j \leq k-1$). Now note that $w = v^{h^{-1}} - v = v^{-1} h v h^{-1} \in H^v H$. Similarly, for any $c \in \mathbb{F}_p$ we have $cw = (cv)^{h^{-1}} - cv \in H^{cv} H$. Thus, identifying the powers 2^j with elements of $\mathbb{F}_p$, we see that $sw \in (H^v H)\left(H^{2v} H\right)\left(H^{2^2 v} H\right) \cdots \left(H^{2^{k-1} v} H\right)$, for any $0 \leq s \leq p-1$, where we pick 0_V from the j-th factor $\left(H^{2^j v} H\right)$ in the product if $b_j = 0$ and $2^j w$ if $b_j = 1$. However, also note that since V is abelian, $\left(H^{2^j v} H\right) \cap V$ is invariant under conjugation by any element of V. Hence, for any choice of $u_0, ..., u_{k-2} \in V$ we have

$$sw \in \Pi_H := (H^v H)^{u_0} \left(H^{2v} H\right)^{u_1} \left(H^{2^2 v} H\right)^{u_2} \cdots \left(H^{2^{k-2} v} H\right)^{u_{k-2}} \left(H^{2^{k-1} v} H\right).$$

Finally, for the choice $u_{k-2} = 2^{k-1} v$, $u_{k-3} = u_{k-2} + 2^{k-2} v$ and in general $u_{k-j} = u_{k-j+1} + 2^{k-j+1} v$ for all $2 \leq j \leq k$ where $u_{k-1} := 0_V$, we get that Π_H is equal to a product of $k+1$ conjugates of H. $\square$

Lemma 3.3. *For each prime number p define $f(p) := \lceil \log p \rceil / \log p$. Then $f(p)$ has a global maximum at $p = 5$. Consequently*

$$\lceil \log p \rceil \leq (3/\log 5) \log p, \text{ for every prime } p. \tag{3.1}$$

Proof. First check that $1+1/\log 11 < 1.29 < 3/\log 5$. Then, using this, we get:

$$f(p) \leq (\log p + 1)/\log p = 1 + 1/\log p < 3/\log 5 = f(5),\ \forall p \geq 11,$$

and for $p = 2,3,7$ we verify explicitly that $f(p) < f(5)$. Hence $f(p)$ has a global maximum $f(5) = 3/\log 5$ at $p = 5$. Finally, $\lceil \log p \rceil = f(p) \log p \leq f(5) \log p$. □

Proof of Proposition 3.1. Using the notation introduced after the statement of the proposition, $\log |G : H| = \log |V| = \log p^l = l \log p$. Using Inequality 3.1, we obtain:

$$1 + l\lceil \log p \rceil \leq 1 + (3/\log 5) l \log p = 1 + (3/\log 5) \log |G : H|.$$

Thus, it is enough to show that G is a product of at most $1+ l\lceil \log p \rceil$ conjugates of H.

Fix a non-zero vector $v \in V$. If v is central in G then $V = \langle v \rangle$ by minimality of V. It follows that H is a non-trivial normal subgroup of $HV = G$ since V is central - a contradiction to H being core-free. Therefore v is not central, and there is some $h \in H$ with $v^{h^{-1}} \neq v$. Set $w := v^{h^{-1}} - v$.

We claim that there are l elements $h_1, \ldots, h_l \in H$ such that $B := \{w^{h_1}, \ldots, w^{h_l}\}$ is a vector space basis of $V = C_p^l$. Note that since $w \neq 0_V$, this claim is immediate for $l = 1$, and hence we assume $l \geq 2$. Suppose by contradiction that $1 \leq m < l$ is the maximal integer such that there exist $h_1, h_2, \ldots, h_m \in H$ for which $B = \{w^{h_1}, \ldots, w^{h_m}\}$ is linearly independent. It follows that for any $h \in H$, $w^h \in Span(B)$. Thus $Span(B) = Span(\{w^h | h \in H\})$. This shows that $Span(B)$ is a proper non-trivial H-invariant subspace of V, contradicting the fact that H acts irreducibly on V. Thus there exists a basis of V of the form $B := \{w^{h_1}, \ldots, w^{h_l}\}$.

For each $v \in V$ there exist $s_1, ..., s_l \in \mathbb{F}_p$ for which $v = \Sigma_{i=1}^{l} s_i w^{h_i}$. Applying Lemma 3.2 to each w^{h_i} separately, we get that each $v \in V$ belongs to $\Pi_1 \cdots \Pi_l$, where each Π_i is a product of $\lceil \log p \rceil + 1$ conjugates of H. But, as in the proof of Lemma 3.2, this shows that $V \subseteq \Pi_1^{u_1} \cdots \Pi_{l-1}^{u_{l-1}} \Pi_l$ for any choice of $u_1, ..., u_{l-1} \in V$, and one can choose these elements so that the product $\Pi_1^{u_1} \cdots \Pi_{l-1}^{u_{l-1}} \Pi_l$ is a product of at most $l\lceil \log p \rceil + 1$ conjugates of H. □

From Proposition 3.1 it follows that if G is an affine primitive permutation group then $\gamma_{\mathrm{cp}}^{H}(G) \leq c_I \log n$ where the constant c_I satisfies $0 < c_I < 2.3$.

4. **Type** II. G is an almost simple primitive permutation group

In this case we have $k = 1$ and $B = T$. Note that T is a non-abelian simple group acting transitively on Ω. Furthermore, T does not act regularly on Ω by [10].

First suppose that $|G| < n^9$. By [9, Theorem 3], since T_α is a subset of T of size at least 2 (because T does not act regularly), there exists a constant c_1 such that T is a product of less than $c_1 \log |T|$ conjugates of T_α. Now $|T| \leq |G| < n^9$ implies that $\gamma_{\mathrm{cp}}^{T_\alpha}(T) < 9 \cdot c_1 \log n$.

Assume that $|G| \geq n^9$. By [7] one of the following holds:

(1) $T = A_m$, where $m \geq 5$ and either
  (a) Ω is the set of all subsets of size k of $\{1, \ldots, m\}$, $n = \binom{m}{k}$ or
  (b) Ω is the set of all partitions of $\{1, \ldots, m\}$ into a subsets of size b where $ab = m$, $a > 1$, $b > 1$; $n = m!/((b!)^a a!)$.

(2) T is a classical simple group acting on an orbit of subspaces of the natural module, or (in the case $T = PSL(d,q)$) on pairs of subspaces of complementary dimensions.

Since $n = |G : G_\alpha| = |T : T_\alpha|$, and since G is almost simple, we have by [1, Lemma 2.7 (i)] that $|G : T| \leq |\mathrm{Out}(T)| < n$. This gives $|T| > n^8 = \left(\frac{|T|}{|T_\alpha|}\right)^8$, implying $\frac{\log|T|}{\log|T_\alpha|} < \frac{8}{7} < 2$. If T_α is maximal in T, we can conclude from [8, Theorem 2] that there exist a universal constant c_2 and a universal function $f : \mathbb{N} \to \mathbb{N}$, such that for all T satisfying $|T| > f(2)$ it holds that $\gamma_{\mathsf{cp}}^{T_\alpha}(T) \leq c_2 \frac{\log|T|}{\log|T_\alpha|}$. Now we claim that this conclusion is in fact valid even if T_α is not maximal in T. More precisely, we claim that [8, Theorem 2] is valid for all subgroups belonging to the families listed in [8, Lemma 3.1] in the case $T = A_m$, and in [8, Lemma 4.3] in the case that T is a classical group. Note that these families include the (T, T_α) of [7] listed above. Our claim is based on a close examination of the use of the maximality assumption in the proof of [8, Theorem 2]. We find that the maximality assumption is used only in two places. First, in appealing to [8, Theorem 1] in order to discard cases of simple groups of Lie type of small Lie rank. Here we replace [8, Theorem 1] by [4, Theorem 1.3], which applies to any subset of T of size at least 2. The second use of the maximality assumption is to identify the possible isomorphism types for maximal subgroups of the remaining simple groups, according to the O'Nan-Scott classification in the alternating case and the Aschbacher classification in the classical case. These are precisely the families listed in [8, Lemma 3.1] and in [8, Lemma 4.3]. The rest of the proof of Theorem 2 of [8] carries through even when the subgroups in question are not actually maximal.

Finally, by Lemma 2.1 and Lemma 2.2 we get that $\gamma_{\mathsf{cp}}^{H}(G) \leq c_{II} \log n$ for some universal constant $c_{II} > 0$, for all primitive almost simple G.

5. **Type III(a)**. G IS A PRIMITIVE PERMUTATION GROUP OF DIAGONAL TYPE.

Here B_α is the diagonal subgroup of B (Δ in the notation of Proposition 5.1 below) and $n = |G : G_\alpha| = |T|^{k-1}$, where $k \geq 2$.

Proposition 5.1. *Let T be a non-abelian simple group, k a positive integer, $B := T^k$. Set $\Delta := \{(t,t,\ldots,t) \ : \ t \in T\} \leq B$. Then $k \leq \gamma_{\mathsf{cp}}^{\Delta}(B) \leq 3k-2$.*

Proof. Suppose B is a product of m conjugates of Δ. Then $\Delta \cong T$ implies $|T|^k = |B| \leq |\Delta|^m = |T|^m$. This proves $k \leq \gamma_{\mathsf{cp}}^{\Delta}(B)$. For proving $\gamma_{\mathsf{cp}}^{\Delta}(B) \leq 3k-2$, choose $\alpha, \beta, \gamma \in T$ as in Lemma 2.3. Set $a := \alpha^{-1}$ and $b := \gamma$. Then $T = \alpha^T \beta^T \gamma^T = (a^{-1})^T (ab^{-1})^T b^T$.

Let $i \in \{1, \ldots, k\}$. Let $\tau_i : T \to T^k$ be the map that sends $t \in T$ to the element of T^k that has t in the i-th component and 1 elsewhere. We denote $T_i := \tau_i(T)$. Consider $D_i := \Delta \Delta^{\tau_i(a)} \Delta^{\tau_i(b)} \Delta$. We prove that $D_i \supseteq T_i$. An element of D_i has the form

$$(xyzw,\ xyzw,\ \ldots,\ xyzw,\ \underbrace{xy^a z^b w}_{i\text{-th entry}},\ xyzw,\ \ldots,\ xyzw)$$

where $x, y, z, w \in T$ are arbitrary. In order to prove that $D_i \supseteq T_i$, choose arbitrary $x, y, z \in T$ and $w = (xyz)^{-1}$. Then for the i-th component we have

$$\begin{aligned} xy^a z^b w = xy^a z^b (xyz)^{-1} = xa^{-1}yab^{-1}zbz^{-1}y^{-1}x^{-1} \\ = (xa^{-1}x^{-1})((xy)\left(ab^{-1}\right)\left(y^{-1}x^{-1}\right))((xyz)\, b\left(z^{-1}y^{-1}x^{-1}\right)) \\ \in (a^{-1})^T (ab^{-1})^T b^T = T. \end{aligned}$$

Since $\{(x, xy, xyz)\,|x, y, z \in T\} = T^3$, we can deduce $D_i \supseteq T_i$.

It follows that $B = T_1 \cdots T_k = \Delta T_2 \cdots T_k \subseteq \Delta D_2 \cdots D_k = D_2 \cdots D_k$. Therefore

$$\begin{aligned} B &= D_2 \cdots D_k = (\Delta\Delta^{\tau_2(a)}\Delta^{\tau_2(b)}\Delta) \cdots (\Delta\Delta^{\tau_k(a)}\Delta^{\tau_k(b)}\Delta) \\ &= (\Delta\Delta^{\tau_2(a)}\Delta^{\tau_2(b)}) \cdots (\Delta\Delta^{\tau_k(a)}\Delta^{\tau_k(b)})\Delta, \end{aligned}$$

and B is a product of $3(k-1)+1 = 3k-2$ conjugates of Δ. □

By Proposition 5.1 we have $\gamma^{\Delta}_{\mathsf{cp}}(B) \le 3k-2$. On the other hand

$$\log|G : G_\alpha| = (k-1)\log|T| \ \ge (k-1)\log 60 > 5\,(k-1)\,.$$

Comparing the numbers we see that B is the product of less than $\log|G : G_\alpha|$ conjugates of B_α, and so we have $\gamma^{H}_{\mathsf{cp}}(G) \le c_{III(a)} \log n$ with $0 < c_{III(a)} \le 1$.

6. **Type III(b)**. G is a primitive permutation group of product action type.

Let R be a primitive permutation group of type II or III(a) on a set Γ. For $\ell > 1$, let $W = R \wr S_\ell$, and take W to act on $\Omega = \Gamma^\ell$ in its natural product action. Then for $\gamma \in \Gamma$ and $\alpha = (\gamma, \ldots, \gamma) \in \Omega$ we have $W_\alpha = R_\gamma \wr S_\ell$, and $n = |\Gamma|^\ell$. If K is the socle of R then the socle B of W is K^ℓ, and $B_\alpha = (K_\gamma)^\ell \ne 1$. If G is primitive of type III(b), then G satisfies $B \le G \le W$ and acts transitively on the ℓ factors of $B = K^\ell$. In particular, $soc(G) = soc(W) = K^\ell$. By the discussion of cases II and III(a) we know that K is the product of at most $\max\left\{c_{II}, c_{III(a)}\right\} \cdot \log|K : K_\gamma|$ conjugates of K_γ. Since $B = K^\ell$ and $B_\alpha = (K_\gamma)^\ell$, we get that B is the product of at most $\max\left\{c_{II}, c_{III(a)}\right\} \cdot \log|K : K_\gamma|$ conjugates of B_α. Now $|G : G_\alpha| = |\Gamma|^\ell$, and, since K acts transitively on Γ, $|\Gamma| = |K : K_\gamma|$. Hence

$$\log n = \log|G : G_\alpha| = \log|\Gamma|^\ell = \ell\log|K : K_\gamma|,$$

and we have proved that $\gamma^{H}_{\mathsf{cp}}(G) \le c_{III(b)} \log n$ with $0 < c_{III(b)} \le \max\left\{c_{II}, c_{III(a)}\right\}$.

7. **Type III(c)**. G is a primitive permutation group of twisted wreath product type.

Let P be a transitive permutation group of degree k, acting on $\{1, ..., k\}$, and let $Q \le P$ be the stabilizer of 1. Let $\varphi : Q \to$Aut(T) be a homomorphism such that $\varphi(Q)$ contains all the inner automorphisms of T. Let

$$B_0 = \{f : P \to T \ : \ f(pq) = f(p)^{\varphi(q)} \ \forall p \in P,\ q \in Q\}.$$

Then B_0 is a group with pointwise multiplication. let $L = \{l_1, ..., l_k\} \subseteq P$ be an arbitrary fixed left transversal of Q in P. By definition of B_0, a function $f \in B_0$ is determined by its values on L. On the other hand, the values of f on L can be arbitrary, and therefore we get $B_0 \cong T^k$. More specifically, for $\ell \in L$ and $t \in T$ define $f_{t,\ell} : P \to T$ by:

$$f_{t,\ell}(x) := \begin{cases} t^{\varphi(\ell^{-1}x)} & \text{if } x \in \ell Q, \\ 1 & \text{if } x \notin \ell Q \end{cases} \quad \forall x \in P.$$

We claim that $f_{t,\ell} \in B_0$. Indeed, let $p \in P$, $q \in Q$, and consider $f_{t,\ell}(pq)$. If $pq \notin \ell Q$ then $p \notin \ell Q$ and $f(pq) = f(p) = 1$ so $f(pq) = f(p)^{\varphi(q)}$ holds. If $pq \in \ell Q$ then $p \in \ell Q$ and there exists $q_0 \in Q$ such that $p = \ell q_0$. Hence

$$\begin{aligned} f_{t,\ell}(pq) &= f_{t,\ell}(\ell q_0 q) = t^{\varphi(\ell^{-1}\ell q_0 q)} = t^{\varphi(q_0 q)} = t^{\varphi(q_0)\varphi(q)} \\ &= \left(t^{\varphi(q_0)}\right)^{\varphi(q)} = f_{t,\ell}(\ell q_0)^{\varphi(q)} = f(p)^{\varphi(q)}. \end{aligned}$$

Furthermore, if $\ell = l_i$ then $f_{t,\ell}$ corresponds to the element of T^k that has t in the i-th component and 1 elsewhere. To see this we just have to check that $f_{t,l_i}(l_j)$ satisfies $f_{t,l_i}(l_j) = t$ if $i = j$ and $f_{t,l_i}(l_j) = 1$ if $i \neq j$ and this is immediate from the definition. Thus we can construct an explicit isomorphism $B_0 \to T^k$ which maps $\{f_{t,l_i} | t \in T\}$ onto T_i, where T_i is the i-th direct factor of T^k, $1 \leq i \leq k$. From now on we identify $\{f_{t,l_i} | t \in T\}$ with T_i. Furthermore, P acts on B_0 in the following way: if $f \in B_0$ and $p \in P$ define $f^p(x) := f(px)$ for all $x \in P$. The semidirect product $G := B_0 \rtimes P$ with respect to this action is called the twisted wreath product (of P and T). Then G acts transitively by right multiplication on the set Ω of size $n = |B_0|$ of all right cosets of P. This action is not always primitive. If it is, G belongs to class III(c). In this case $B = B_0 \cong T^k = T_1 \times \cdots \times T_k$ is a normal subgroup (the unique minimal one) in G and acts regularly on Ω, and we take $G_\alpha = P$. We have $n = |T|^k$.

Set, for each $1 \leq i \leq k$, $Q_i := l_i Q l_i^{-1}$. We prove that Q_i leaves T_i invariant with respect to the action of P on B_0. For this we have to show that if $p \in Q_i$, namely, $p = l_i q l_i^{-1}$ for some $q \in Q$, then, for all $x \in P$, $x \in l_i Q$ if and only if $px \in l_i Q$. But $px \in l_i Q$ means $l_i q l_i^{-1} x \in l_i Q$, and this is true if and only if $q l_i^{-1} x \in Q$, which, since $q \in Q$, is equivalent to $l_i^{-1} x \in Q$, which is equivalent to $x \in l_i Q$.

Thus the action of P on B_0 induces an action of Q_i on T_i for each $1 \leq i \leq k$. Note that for $p = l_i q l_i^{-1} \in Q_i$ and $x = l_i q_0 \in l_i Q$, we get

$$\begin{aligned} f_{t,l_i}^p(x) &= f_{t,l_i}(px) = t^{\varphi(l_i^{-1}px)} = t^{\varphi(l_i^{-1}l_i q l_i^{-1} l_i q_0)} \\ &= t^{\varphi(q q_0)} = \left(t^{\varphi(q)}\right)^{\varphi(q_0)} = f_{t^{\varphi(q)},l_i}(x). \end{aligned}$$

Since $f_{t,l_i}^p(x) = f_{t^{\varphi(q)},l_i}(x)$ clearly holds also for any $x \notin l_i Q$ we get $f_{t,l_i}^p = f_{t^{\varphi(q)},l_i}$ and so Q_i acts on T_i as $\varphi(Q)$.

By Lemma 2.3 there exist $t_{i,1}, t_{i,2}, t_{i,3} \in T_i$ for each $1 \leq i \leq k$ such that $T_i = t_{i,1}^{T_i} t_{i,2}^{T_i} t_{i,3}^{T_i}$. For each $j \in \{1,2,3\}$ set $O_{i,j} := \left\{p^{-1} t_{i,j} p | p \in Q_i\right\}$. In $G := B_0 \rtimes P$, the action of P on B_0 is the restriction of the conjugation action of G on itself, and hence $O_{i,j}$ is the orbit of $t_{i,j}$ under the action of Q_i on T_i. Since, by assumption, $\mathrm{Inn}(T) \leq \varphi(Q)$, $O_{i,j}$ is a normal subset of T_i, and in particular contains $t_{i,j}^{T_i}$, the conjugacy class of $t_{i,j}$ in T_i. Set $X_{i,j} := t_{i,j}^{-1} O_{i,j}$, $1 \leq j \leq 3$. Since the $O_{i,j}$'s are normal sets,

$$T_i = t_{i,1}^{-1} t_{i,2}^{-1} t_{i,3}^{-1} t_{i,1}^{T_i} t_{i,2}^{T_i} t_{i,3}^{T_i} \subseteq t_{i,1}^{-1} t_{i,2}^{-1} t_{i,3}^{-1} O_{i,1} O_{i,2} O_{i,3} = X_{i,1} X_{i,2} X_{i,3}.$$

Moreover $X_{i,j} = \{t_{i,j}^{-1}p^{-1}t_{i,j}p \ : \ p \in Q_i\} \subseteq P^{t_{i,j}}P$ for $j = 1,2$, and $X_{i,3} = t_{i,3}^{-1}O_{i,3} = O_{i,3}t_{i,3}^{-1} = \{p^{-1}t_{i,3}pt_{i,3}^{-1} \ : \ p \in Q_i\} \subseteq PP^{t_{i,3}^{-1}}$. It follows that

$$T_i = X_{i,1}X_{i,2}X_{i,3} \subseteq P^{t_{i,1}}PP^{t_{i,2}}PP^{t_{i,3}^{-1}}.$$

Thus $B = T_1 \cdots T_k$ is contained in a product of at most $5k$ conjugates of P, and since $n = |T|^k$ we have $k = \log n / \log |T|$. Hence

$$\gamma_{\mathtt{cp}}^P(G) \leq 5k = 5 \log n / \log |T| \leq \frac{5}{\log 60} \log n < \log n.$$

We have proved that if G is a primitive group of twisted wreath product type then $\gamma_{\mathtt{cp}}^H(G) \leq c_{III(c)} \log n$ where $0 < c_{III(c)} < 1$.

This completes the proof of Theorem 1.

Acknowledgement: We would like to thank N. Nikolov for a useful discussion.

References

[1] M. Aschbacher, R.M. Guralnick, On abelian quotients of primitive groups, *Proc. of the AMS* **107** (1989) no. I, 89-95.

[2] J.N. Bray, D.F. Holt, C.M. Roney-Dougal, The Maximal Subgroups of the Low-Dimensional Finite Classical Groups, LMS 407, Cambridge University Press, (2013)

[3] M. Garonzi, D. Levy, Factorizing a finite group into conjugates of a subgroup, *J. Algebra* **418** (2014), 129-141.

[4] N. Gill, L. Pyber, I. Short, E. Szabó, On the product decomposition conjecture for finite simple groups, Groups Geom. Dyn. **7** (2013), 867-882.

[5] R.M. Guralnick, G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.*, **25**(1):77–121, 2012.

[6] P. Kleidman, M.W. Liebeck, The subgroup structure of the finite classical groups, LMS Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[7] M.W. Liebeck, On minimal degrees and base sizes of primitive permutation groups, *Arch. Math. (Basel)* **43** (1984), no. 1, 11–15.

[8] M.W. Liebeck, N. Nikolov, A. Shalev, A conjecture on product decompositions in simple groups, *Groups Geom. Dyn.* **4** (2010), no. 4, 799–812.

[9] M.W. Liebeck, N. Nikolov, A. Shalev, Product decompositions in finite simple groups, *Bull. Lond. Math. Soc.* **44** (2012), no. 3, 469–472.

[10] M.W. Liebeck, C.E. Praeger, and J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Austral. Math. Soc. Ser. A*, **44**(3):389–396, 1988.

[11] J. S. Rose. *A course on group theory.* Cambridge University Press, 1978.

(Martino Garonzi) Departamento de Matematica, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília - DF 70910-900, Brasil

E-mail address: mgaronzi@gmail.com

(Dan Levy) The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel

E-mail address: danlevy@mta.ac.il

(Attila Maróti) MTA Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: maroti.attila@renyi.mta.hu

(Iulian I. Simion) Department of Mathematics, University of Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: iulian.simion@math.unipd.it