WREATH PRODUCTS AND THE NON-COPRIME $k(GV)$ PROBLEM

NGUYEN N. HUNG, ATTILA MARÓTI, AND JUAN MARTÍNEZ MADRID

Abstract. Let $G = X \wr H$ be the wreath product of a nontrivial finite group X with k conjugacy classes and a transitive permutation group H of degree n acting on the set of n direct factors of X^n. If H is semiprimitive, then $k(G) \leq k^n$ for every sufficiently large n or k. This result solves a case of the non-coprime $k(GV)$ problem and provides an affirmative answer to a question of Garzoni and Gill for semiprimitive permutation groups. The proof does not require the classification of finite simple groups.

1. Introduction

Let G be a finite group. Let $k(G)$ be the number of conjugacy classes of G. This is equal to the number of complex irreducible representations of G. Bounding $k(G)$ is a classical problem with numerous applications in both group theory and representation theory. There are many results providing upper bounds for $k(G)$. The most notable one is the $k(GV)$ theorem, which states that $k(GV) \leq |V|$, where V is an elementary abelian group which is a finite and faithful G-module for a finite group G of order coprime to $|V|$ (see [19]).

In [10, Problem 1.1], Guralnick and Tiep put forward the non-coprime $k(GV)$ problem: without assuming the coprime condition, can one show that $k(GV) \leq |V|$? More precisely, can one characterize all finite groups GV such that $k(GV) > |V|$? There are many works on this problem. See [10], [14], [19, Chapter 13], [15], [9], [18], [6].

2020 *Mathematics Subject Classification.* Primary 20B05, 20E45.

Key words and phrases. Conjugacy classes, class number bound, wreath products, permutation groups, non-coprime $k(GV)$ problem.

The first author gratefully acknowledges the support of the AMS-Simons Research Enhancement Grant (AWD-000167 AMS) and the UA Faculty Research Grant (FRG 1747). The second author was supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K138596, No. K132951 and Grant No. K138828. The research of the third author was supported by Ministerio de Ciencia e Innovación (Grant PID2022-137612NB-I00 funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe"), and by Generalitat Valenciana CIAICO/2021/163 and CIACIF/2021/228. Finally, we are grateful to the referee for several helpful comments that significantly improved the exposition of the paper.

In case V is a (finite, faithful and) irreducible G-module for a finite group G (not necessarily of coprime order to $|V|$) the semidirect product GV is an affine primitive permutation group with socle V and degree $|V|$. On the other hand, when H is a primitive permutation group with non-abelian socle and of degree n, Garzoni and Gill [8] proved that either $k(H) < n/2$ and $k(H) = o(n)$ as $n \to \infty$, or H belongs to explicit families of examples.

In this paper we are interested in bounding $k(G)$ for $G = X \wr H$, the wreath product of a finite group X and a permutation group H of degree n acting on the set of direct factors of X^n. This is a case of the non-coprime $k(GV)$ problem when X is an elementary abelian group or, more generally, when $X = KW$ for some finite K-module W of a finite group K. The problem of bounding $k(X \wr H)$ is also related to [8] as described below.

Let $k := k(X)$. Schmid [19, Proposition 8.5d] proved that if H is a cyclic group of order n (acting regularly), then $k(G) = (k^n - k)/n + kn$ when n is a prime and $k(G) \leq k^n - k + kn$ in general. More recently, Garzoni and Gill [8, Lemma 4.3] showed that if H is a regular permutation group, then $k(G) = \frac{k^n}{n} + O(nk^{n/2})$. Moreover, they asked [8, Question 2] whether $k(G) = O(k^n)$ for any transitive permutation group H of degree n.

If n is even, $X = C_2$, $k = 2$ and $H = (C_2)^{n/2}$ such that $G = X \wr H$ is the direct product of $n/2$ copies of $C_2 \wr C_2$, then $k(G) = 5^{n/2} > k^n$. Furthermore, if $H = (C_2)^{n/2}$ is replaced by $H = C_2 \wr C_{n/2}$, then H acts transitively on the set of factors of X^n and $k(G) \geq 5^{n/2}/(n/2) > k^n$ for every sufficiently large n. This answers [8, Question 2] in the negative (for $k = 2$).

On the other hand, we provide an affirmative answer to the Garzoni-Gill question in the case where H is a primitive permutation group. In fact, our result extends to the broader class of transitive groups called *semiprimitive* permutation groups, defined as those permutation groups in which every normal subgroup is transitive or semiregular. (A permutation group is called *semiregular* if the stabilizer of any point is trivial.)

Theorem 1.1. *Let $G = X \wr H$ where X is a nontrivial finite group with k conjugacy classes and H is a transitive permutation group of degree n acting on the set of n direct factors of X^n. If H is semiprimitive, then $k(G) \leq k^n$ for every sufficiently large n or k.*

Our proof of Theorem 1.1 does not use the classification of finite simple groups.

In several cases we obtain an asymptotic formula for $k(G)$. For example, when H is an arbitrary transitive group of order at most $2^{\sqrt{n}/4}$ (see Theorem 2.4) or when H is primitive with known exceptions (see Theorem 2.5), then $k(G) = (1 + o(1))(k^n/|H|)$ as $n \to \infty$ or $k \to \infty$. It is not true in general that $k(G) = O(k^n/|H|)$; for instance, when $n \to \infty$ and $H = \mathsf{S}_n$, we have $k^n/|H| < 1$, yet $k(G) > k(H)$ remains large.

On the other hand, $k(G) \geq k^n/|H|$ even for an arbitrary permutation group H (see Lemma 2.1).

An important class of primitive permutation groups relevant to our proof is the so-called *large base* groups (see Definition 4.1). In Section 2, we establish the asymptotic formula for the case where H is not one of these large base groups. The specific cases $H \in \{\mathsf{A}_n, \mathsf{S}_n\}$ are addressed in Section 3, while the remaining large base groups are treated in Sections 4 and 5 using a different approach. This completes the proof of Theorem 1.1 for primitive H. Finally, in Section 6, we extend the machinery developed in the earlier sections to prove the result for all semiprimitive groups.

2. An asymptotic formula for $k(G)$

Let G, X, H, k, and n be as in the statement of Theorem 1.1. For the moment assume that H is an arbitrary permutation group of degree n. This group H has a natural action on $\mathrm{Irr}(X^n) = \mathrm{Irr}(X)^n$, the set of complex irreducible characters of X^n. Let $\chi_1, \dots, \chi_f$ be a list of representatives of the distinct orbits of H on $\mathrm{Irr}(X^n)$. Let $I_H(\chi)$ denote the inertia group in H of a character χ in $\mathrm{Irr}(X^n)$.

Lemma 2.1. *We have* $k(G) = \sum_{i=1}^{f} k(I_H(\chi_i))$.

Proof. Fix an index i. The character χ_i of X^n may be extended to its inertia group $I_G(\chi_i) = X \wr I_H(\chi_i)$ in G by [13, p. 154]. Thus the number of irreducible characters of $I_G(\chi_i)$ lying above χ_i is $k(I_H(\chi_1))$, by Gallagher's theorem [12, Corollary 6.17]. The identity now follows from Clifford's correspondence [12, Theorem 6.11]. □

For an element h of $H \leq \mathsf{S}_n$, let $\sigma(h)$ be the number of cycles in the disjoint cycle decomposition of h. For a finite group L acting on a finite set Ω, we denote the number of orbits of L on Ω by $n(L, \Omega)$.

Lemma 2.2. *We have*

$$n(H, \mathrm{Irr}(X^n)) = \frac{1}{|H|} \sum_{h \in H} k^{\sigma(h)}.$$

Proof. Let h be an arbitrary element of H. The number of characters in $\mathrm{Irr}(X^n)$ fixed by h is $k^{\sigma(h)}$. The statement follows from the orbit-counting lemma. □

Let Δ denote the union of all non-regular orbits of H acting on $\mathrm{Irr}(X^n)$. By the orbit-counting lemma, the number of non-regular orbits is

$$\frac{1}{|H|} \sum_{h \in H} |\,\mathrm{fix}(h, \Delta)| = \frac{|\Delta|}{|H|} + \frac{1}{|H|} \sum_{h \in H \setminus \{1\}} |\,\mathrm{fix}(h, \Delta)|,$$

where $\mathrm{fix}(h, \Delta)$ is the set of the fixed points of h on Δ. Let

$$\alpha(H) := \max_{1 \neq h \in H} \sigma(h)/n.$$

Then we get

$$|\Delta| \leq \sum_{h \in H \setminus \{1\}} k^{\alpha(H)n} \leq (|H|-1)k^{\alpha(H)n}.$$

Therefore, the number of non-regular orbits is at most

$$\frac{(|H|-1)k^{\alpha(H)n} + (|H|-1)k^{\alpha(H)n}}{|H|} < 2k^{\alpha(H)n}.$$

Now, up to reordering, let $\chi_1, ..., \chi_t$ be representatives of the non-regular orbits. In particular, $t \leq 2k^{\alpha(H)n}$. Moreover, by Lemma 2.1, we obtain

$$k(G) = \frac{k^n - |\Delta|}{|H|} + \sum_{i=1}^{t} k(I_H(\chi_i)).$$

It immediately follows that

$$k(G) < \frac{k^n}{|H|} + 2ek^{\alpha(H)n}, \tag{2.1}$$

where e denotes the maximum of $k(T)$ over all the subgroups T of H.

If H is regular (or more generally semiregular), then $\alpha(H) \leq 1/2$, $e \leq n$ and so $k(G) = \frac{k^n}{n} + O(nk^{n/2})$ by (2.1). This is the bound obtained by Garzoni and Gill mentioned above.

For any permutation group H, as $e \leq 5^{n/3}$ by [7, Theorem 1.1], we have $k(G) = O(k^n)$, provided that $5^{1/3} < k^{1-\alpha(H)}$, again by (2.1).

Lemma 2.3. *We have*

$$k(G) < \left(1 + \frac{1}{kn}\right)\frac{k^n}{|H|}$$

if one of the following conditions holds:

(i) $\alpha(H)n \leq n - \log_k(2kn|H|^2)$;
(ii) n *is bounded,* $k \to \infty$, *and* H *does not contain a transposition.*

Proof. In the first case, we have $(1-\alpha(H))n \geq \log_k(2kn|H|^2)$ and so

$$2kne \leq 2kn|H| \leq \frac{k^{(1-\alpha(H))n}}{|H|}.$$

This and (2.1) imply the desired inequality. If the second condition holds then $\alpha(H)n \leq n-2 \leq n - \log_k(2kn|H|^2)$, and the lemma follows as well. We note that if a primitive permutation group of degree n contains a transposition then it is S_n. □

Let H be a transitive permutation group of degree n. Let $\mu(H)$ be the *minimal degree* of H. This is the minimal number of points moved by any nonidentity element of H. Let $b(H)$ be the *minimal base size* of H. This is the smallest number of points whose joint stabilizer in H is the identity. We have $\mu(H)b(H) \geq n$ by [2, p. 80]. Since $b(H) \leq \log_2 |H|$, we obtain $\mu(H) \geq n/\log_2 |H|$.

For $h \in H$, let $\mathrm{fix}(h)$ denote the set of fixed points of h and let $\mathrm{fpr}(h) := |\mathrm{fix}(h)|/n$ be the *fixed point ratio* of h. It follows that

$$\mathrm{fpr}(h) \leq 1 - \frac{1}{\log_2 |H|} \tag{2.2}$$

for any nonidentity element h in H. We have

$$\sigma(h) \leq |\mathrm{fix}(h)| + \frac{n - |\mathrm{fix}(h)|}{2} = \frac{n + |\mathrm{fix}(h)|}{2} = \frac{n}{2}\left(1 + \mathrm{fpr}(h)\right) \tag{2.3}$$

for every $h \in H$. We get

$$\alpha(H)n \leq n - \frac{n}{2\log_2 |H|}$$

by (2.2) and (2.3).

The following theorem provides an affirmative answer to [8, Question 2] when H has small order.

Theorem 2.4. *If $|H| \leq 2^{\sqrt{n}/4}$, then $k(G) < (1 + \frac{1}{kn})(k^n/|H|)$.*

Proof. Let H be transitive of order at most $2^{\sqrt{n}/4}$. Observe that if

$$n - \frac{n}{2\log_2 |H|} \leq n - \log_k \left(2kn|H|^2\right), \tag{2.4}$$

then we are done by using Lemma 2.3. Inequality (2.4) is equivalent to the inequality $n \geq 2(\log_2 |H|)(\log_k(2kn|H|^2))$. Since the right-hand side is at most $10(\log_2 |H|)^2$ and $|H| \leq 2^{\sqrt{n}/4}$, inequality (2.4) is satisfied, finishing the proof of the theorem. □

We finish this section with the following.

Theorem 2.5. *If H is primitive and not isomorphic to any of the groups*

(i) A_n, S_n,
(ii) A_m, S_m *acting on the set of 2-element subsets of* $\{1, \dots m\}$ *with* $n = \binom{m}{2}$,
(iii) *a group H satisfying* $(\mathsf{A}_m)^2 \leq H \leq \mathsf{S}_m \wr \mathsf{S}_2$ *where* $n = m^2$,

then

$$\frac{k^n}{|H|} \leq k(G) < \left(1 + \frac{1}{kn}\right)\frac{k^n}{|H|}$$

for every sufficiently large n or k.

Proof. The lower bound follows from Lemma 2.1. Without the classification of finite simple groups Sun and Wilmes [20, Corollary 1.6] proved that

$$|H| \leq \exp\left(O(n^{1/3}\log^{7/3} n)\right), \tag{2.5}$$

unless H is a family of primitive groups appearing in (i), (ii) or (iii) of the statement of the theorem. Since the right-hand side of (2.5) is less than $2^{\sqrt{n}/4}$ for every sufficiently large n, the result follows from Theorem 2.4 for every sufficiently large n. When n is bounded and $k \to \infty$, the statement follows from the paragraph after (2.3). □

3. Bounding $k(X \wr \mathsf{S}_n)$ and $k(X \wr \mathsf{A}_n)$

The goal of this section is to prove the main result in the case $H \in \{\mathsf{S}_n, \mathsf{A}_n\}$. This is the first exception singled out in Theorem 2.5.

We remark that although the main theorem of [7] depends on the classification of finite simple groups, a part of this result does not: if Y is a Young subgroup of S_n then both $k(Y)$ and $k(Y \cap \mathsf{A}_n)$ are at most $5^{n/3}$. This latter statement is used in the two proofs of Theorem 3.1 presented below.

Theorem 3.1. *Assume the hypothesis and notation of Theorem 1.1. If $H \in \{\mathsf{S}_n, \mathsf{A}_n\}$, then $k(G) \leq k^n$ for every sufficiently large n or k.*

Proof. Let n be bounded by an absolute constant. For every sufficiently large k and for any n at least 3, we have

$$k(G) \leq 2 \cdot k(X \wr \mathsf{A}_n) \leq 2 \cdot \left(1 + \frac{1}{kn}\right) \frac{k^n}{|\mathsf{A}_n|} < k^n$$

by Lemma 2.3. When $n = 2$ (and $H = \mathsf{S}_2$) the action is regular and this case was treated earlier (see [19, Proposition 8.5d], [8, Lemma 4.3] or Section 2). Let $n \geq 5$. Observe that $n(\mathsf{S}_n, \mathrm{Irr}(X)^n)$ is exactly the number of k-tuples $(x_1, ..., x_k) \in \mathbb{Z}^k_{\geq 0}$ such that $n = x_1 + \cdots + x_k$. (These tuples are often referred to as *weak k-compositions* of n, and their number is given by $\binom{n+k-1}{k-1}$.) We have

$$n(\mathsf{S}_n, \mathrm{Irr}(X)^n) = \binom{n+k-1}{k-1} \leq \min\left\{(n+1)^{k-1}, k \cdot \left(\frac{k+1}{2}\right)^{n-1}\right\}.$$

If k is bounded by an absolute constant, then

$$k(G) \leq 5^{n/3} \cdot 2 \cdot n(\mathsf{S}_n, \mathrm{Irr}(X)^n) \leq 5^{n/3} \cdot 2 \cdot (n+1)^{k-1} < k^n,$$

for every sufficiently large n, by Lemma 2.1 and [7]. Let $k \geq 100$. We have

$$k(G) \leq 5^{n/3} \cdot 2 \cdot k \cdot \left(\frac{k+1}{2}\right)^{n-1} \leq k^n,$$

and the proof is complete. □

We shall need a variation of [3, Lemma 2.1] in the next section.

Lemma 3.2. *For every ϵ and γ with $0 < \epsilon < 1$ and $0 < \gamma < 1$, there exists $N = N(\epsilon, \gamma)$ such that for any $n \geq N$ whenever $x \in \mathsf{S}_n$ satisfies $(1-(1-\epsilon)\gamma)n \leq \sigma(x)$, then $|x^{\mathsf{S}_n}| < 2 \cdot n^4 \cdot |\mathsf{S}_n|^{\gamma}$.*

Proof. According to [3, Lemma 2.1], whenever $x \in \mathsf{A}_n$ satisfies $(1-(1-\epsilon)\gamma)n \leq \sigma(x)$, then $|x^{\mathsf{S}_n}| \leq 2 \cdot |x^{\mathsf{A}_n}| < 2 \cdot |\mathsf{A}_n|^{\gamma} < 2 \cdot |\mathsf{S}_n|^{\gamma}$.

Let $x \in \mathsf{S}_n \setminus \mathsf{A}_n$ satisfy the inequality $(1-(1-\epsilon)\gamma)n \leq \sigma(x)$. In the disjoint cycle decomposition of x there is a cycle π of even length, say $2r$. Let c_r and c_{2r} be the number of cycles of lengths r and $2r$ respectively in the disjoint cycle decomposition of x. We have $|\mathbf{C}_{\mathsf{S}_n}(x)| = a \cdot r^{c_r} \cdot c_r! \cdot (2r)^{c_{2r}} \cdot c_{2r}!$ for some positive integer a. Let $y \in \mathsf{A}_n$ be the permutation obtained from x by replacing π by π^2. We have $|\mathbf{C}_{\mathsf{S}_n}(y)| = a \cdot r^{c_r+2} \cdot (c_r+2)! \cdot (2r)^{c_{2r}-1} \cdot (c_{2r}-1)!$. It is easy to see that $|\mathbf{C}_{\mathsf{S}_n}(y)| \leq n^4 \cdot |\mathbf{C}_{\mathsf{S}_n}(x)|$ from which it follows that $|x^{S_n}| \leq n^4 \cdot |y^{\mathsf{S}_n}|$. Since $\sigma(y) = \sigma(x)+1$, we have $(1-(1-\epsilon)\gamma)n \leq \sigma(y)$ by hypothesis and so $|y^{\mathsf{S}_n}| < 2 \cdot |\mathsf{S}_n|^{\gamma}$ by the first paragraph. This gives $|x^{\mathsf{S}_n}| < 2 \cdot n^4 \cdot |\mathsf{S}_n|^{\gamma}$. □

Theorem 3.1 can also be proved using Lemma 3.2, as follows.

Second proof of Theorem 3.1. Let ϵ and γ be such that $0 < \epsilon < 1$ and $0 < \gamma < 1$ such that $\delta := 1-(1-\epsilon)\gamma < 1 - \log_2(5)/3$. Let β be such that $\gamma < \beta < 1$. There exists by Lemma 3.2 an integer N such that whenever $n \geq N$ the inequality $\delta n \leq \sigma(x)$ (for $x \in \mathsf{S}_n$) implies $|x^{\mathsf{S}_n}| < |\mathsf{S}_n|^{\beta}$. It follows that the number of elements $x \in \mathsf{S}_n$ such that $\sigma(x) \geq \delta n$ is less than $|\mathsf{S}_n|^{\beta} p(n)$ where $p(n)$ denotes the number of partitions of n.

By Lemma 2.2 we have

$$n(\mathsf{S}_n, \mathrm{Irr}(X)^n) = \frac{1}{|\mathsf{S}_n|}\sum_{h \in \mathsf{S}_n} k^{\sigma(h)} = \frac{1}{|\mathsf{S}_n|}\sum_{\substack{h \in \mathsf{S}_n \\ \sigma(h) < \delta n}} k^{\sigma(h)} + \frac{1}{|\mathsf{S}_n|}\sum_{\substack{h \in \mathsf{S}_n \\ \sigma(h) \geq \delta n}} k^{\sigma(h)}$$

$$< k^{\delta n} + \frac{1}{|\mathsf{S}_n|}k^n + |\mathsf{S}_n|^{\beta-1}p(n)k^{n-1}.$$

Since $p(n) < 13.01^{\sqrt{n}}$ by [5], it follows that

$$n(\mathsf{S}_n, \mathrm{Irr}(X)^n) < \frac{k^n}{2 \cdot 5^{n/3}}$$

for every sufficiently large n or k. By Lemma 2.1 and [7], it follows that

$$k(G) = k(X \wr H) \leq 2 \cdot 5^{n/3} n\left(\mathsf{S}_n, \mathrm{Irr}(X)^n\right) < 2 \cdot 5^{n/3}\frac{k^n}{2 \cdot 5^{n/3}} = k^n$$

for every sufficiently large n or k, as wanted. □

In order to finish the proof of Theorem 1.1 for primitive groups, we may assume that $n \to \infty$. This follows from Theorem 3.1 and the paragraph following (2.3).

4. Bounding the number of orbits of S_m on $\mathrm{Irr}(X^{\binom{m}{\ell}})$

To complete the proof of Theorem 1.1 for primitive groups, it remains to address the families of groups listed in (ii) and (iii) of Theorem 2.5. These exceptional primitive permutation groups, together with the groups in (i), fall into a broader class of groups, which we will analyze collectively. We remark that tackling each specific family individually does not significantly simplify the proof.

Definition 4.1. We say that H is a *large base permutation group* of degree n if $(\mathsf{A}_m)^t \leq H \leq \mathsf{S}_m \wr \mathsf{S}_t$ with $t \geq 1$ and $m \geq 5$, where the action of S_m is on ℓ-element subsets of $\{1, \ldots, m\}$ with $1 \leq \ell < m/2$ and the wreath product has the product action of degree $n = \binom{m}{\ell}^t$.

Notation 4.2. We will fix the following notation when working with large base groups:

(i) Ω is the set of ℓ-subsets of $\{1, \ldots, m\}$,

(ii) $B_t := \mathrm{Irr}(X)^{\binom{m}{\ell}^t}$,

(iii) $B := B_1 = \mathrm{Irr}(X)^{\binom{m}{\ell}}$.

The goal of this section is to obtain an asymptotic bound for $n(\mathsf{S}_m, B)$. From this point on we change notation. For a permutation π in S_m, we denote the number of cycles in the disjoint cycle decomposition of π by $\sigma(\pi)$, while $\sigma'(\pi)$ will denote the number of cycles in the disjoint cycle decomposition of π acting on the set of ℓ-element subsets of $\{1, \ldots, m\}$.

Given $j \in \{1, \ldots, m\}$, we write

$$\mathcal{S}(j, m) := |\{\pi \in \mathsf{S}_m | \sigma(\pi) = j\}|.$$

This number $\mathcal{S}(j, m)$ is often referred to as the Stirling number of the first kind.

Lemma 4.3. $\mathcal{S}(j, m) < (m!)^{0.41}$ *for every sufficiently large m and $j > 3m/4$.*

Proof. In Lemma 3.2, let us take $\gamma = 2/5$ and $1 - (1 - \epsilon)\gamma = 3/4$ (that is, $\epsilon = 3/8$). Assume that $m \geq N(\epsilon, \gamma)$ and $j > 3m/4$. The set $\{\pi \in \mathsf{S}_m | \sigma(\pi) = j\}$ is a union of conjugacy classes of S_m. Since all elements in $\{\pi \in \mathsf{S}_m | \sigma(\pi) = j\}$ satisfy that $\sigma(\pi) = j > 3m/4 = (1 - (1 - \epsilon)\gamma)m$, we deduce that

$$\mathcal{S}(j, m) \leq 2m^4 p(m) |\mathsf{S}_m|^{\gamma} < 2m^4 13.01^{\sqrt{m}} |\mathsf{S}_m|^{2/5},$$

and the lemma follows. □

Lemma 4.4. *For $\pi \in \mathsf{S}_m$, let $\mathrm{fix}(\pi)$ denote the set of ℓ-subsets of $\{1, \ldots m\}$ that are fixed under π. There exists a positive integer N such that*

$$|\mathrm{fix}(\pi)| < \frac{3}{4}\binom{m}{\ell}$$

for every $m \geq N$, $1 \leq \ell < m/2$, and $\sigma(\pi) \leq 3m/4$.

Remark 4.5. We choose the constant 3/4 in the bound to streamline the proofs. The same argument shows that, for any positive constance ϵ, there exists $\delta > 0$ such that $|\operatorname{fix}(\pi)| < \epsilon\binom{m}{\ell}$ whenever $\sigma(\pi) \leq \delta m$. We also note that a strong bound for $|\operatorname{fix}(\pi)|$ is given in [4, Lemma 3.2], from which our result can alternatively be deduced. We thank the referee for pointing out this reference.

Proof of Lemma 4.4. For each i with $1 \leq i \leq m$, let α_i be the number of cycles in π of length i. We have $\sigma(\pi) = \sum_i \alpha_i$ and $m = \sum_i i\alpha_i$. Let $\mathcal{P}(\ell)$ denote the set of partitions of the integer ℓ. For each $\lambda \in \mathcal{P}(\ell)$, let λ_i denote the number of parts of λ equal to i. Then

$$|\operatorname{fix}(\pi)| = \sum_{\lambda \in \mathcal{P}(\ell)} \binom{\alpha_1}{\lambda_1} \cdot \binom{\alpha_2}{\lambda_2} \cdots$$

Using the well-known estimate $\binom{a}{b} \cdot \binom{c}{d} \leq \binom{a+c}{b+d}$, we obtain

$$|\operatorname{fix}(\pi)| \leq \sum_{\lambda \in \mathcal{P}(\ell)} \binom{\sum \alpha_i}{\sum \lambda_i} = \sum_{\lambda \in \mathcal{P}(\ell)} \binom{\sigma(\pi)}{l(\lambda)}, \tag{4.1}$$

where $l(\lambda)$ is the number of parts of λ.

I. Assume first that $\ell \leq \sigma(\pi)/2$. Then $\binom{\sigma(\pi)}{l(\lambda)} \leq \binom{\sigma(\pi)}{\ell}$ for every $\lambda \in \mathcal{P}(\ell)$. It follows from (4.1) that

$$|\operatorname{fix}(\pi)| \leq p(\ell) \cdot \binom{\sigma(\pi)}{\ell}.$$

Assume furthermore that $m > \ell + \sigma(\pi)$. We then have

$$\begin{aligned}\binom{m}{\ell} &= \frac{m(m-1)\cdots(\sigma(\pi)+1)}{(m-\ell)(m-1-\ell)\cdots(\sigma(\pi)+1-\ell)} \cdot \binom{\sigma(\pi)}{\ell} \\ &= \frac{m(m-1)\cdots(m-\ell+1)}{\sigma(\pi)(\sigma(\pi)-1)\cdots(\sigma(\pi)-\ell+1)} \cdot \binom{\sigma(\pi)}{\ell} \\ &\geq \left(\frac{4}{3}\right)^{\ell} \cdot \binom{\sigma(\pi)}{\ell},\end{aligned}$$

where the last inequality follows from the hypothesis on $\sigma(\pi)$. The lemma then follows if $(4/3)^{\ell-1} > p(\ell)$. This is true when $\ell \geq 59$, by using the bound for the partition function in [5].

We therefore may assume that $\ell \leq 58$. By (4.1) and the hypothesis,

$$|\operatorname{fix}(\pi)| \leq \sum_{\lambda \in \mathcal{P}(\ell)} \binom{[3m/4]}{l(\lambda)}. \tag{4.2}$$

Thus, we are done if

$$\sum_{\lambda \in \mathcal{P}(\ell)} \binom{[3m/4]}{l(\lambda)} < \frac{3}{4}\binom{m}{\ell}.$$

For each fixed ℓ with $\ell \leq 58$, we observe that the right-hand side is a polynomial (in m) of degree ℓ, while the left-hand side is a polynomial of degree at most ℓ and if equal to ℓ then with smaller leading coefficient. Therefore the inequality holds for every sufficiently large m, and we are done.

Now assume that $m \leq \ell + \sigma(\pi)$. Then

$$\binom{m}{\ell} \geq \left(\frac{m}{m-\ell}\right)^{m-\sigma(\pi)} \cdot \binom{\sigma(\pi)}{\ell} \geq \left(\frac{m}{m-\ell}\right)^{m/4} \cdot \binom{\sigma(\pi)}{\ell} \geq \left(\frac{4}{3}\right)^{m/4} \cdot \binom{\sigma(\pi)}{\ell}.$$

As above, the desired inequality follows from these bounds for every sufficiently large m.

II. Next we consider the case $\ell > \sigma(\pi)/2$. Then $\binom{\sigma(\pi)}{l(\lambda)} \leq \binom{\sigma(\pi)}{[\sigma(\pi)/2]}$ for every $\lambda \in \mathcal{P}(\ell)$. As in the previous case, it follows from (4.1) that

$$|\operatorname{fix}(\pi)| \leq p(\ell) \cdot \binom{\sigma(\pi)}{[\sigma(\pi)/2]}.$$

On the other hand, by the hypothesis on $\sigma(\pi)$ and ℓ, we have

$$\binom{m}{\ell} = \frac{(m-[\sigma(\pi)/2])\cdots(m-\ell+1)}{\ell(\ell-1)\cdots([\sigma(\pi)/2]+1)} \cdot \binom{m}{[\sigma(\pi)/2]}$$
$$\geq \left(\frac{5}{4}\right)^{\ell-[\sigma(\pi)/2]} \cdot \binom{m}{[\sigma(\pi)/2]}.$$

The lemma now follows by similar estimates as in the previous case, but for $\binom{m}{[\sigma(\pi)/2]}$ instead of $\binom{m}{\ell}$. □

Proposition 4.6. *Let X be a nontrivial finite group with k conjugacy classes. There exists a positive integer N (independent of k) such that*

$$n(\mathsf{S}_m, B) < 2\max\left\{k^{\frac{7}{8}\binom{m}{\ell}}, (m!)^{-0.58}k^{\binom{m}{\ell}}\right\}.$$

for every $m \geq N$ and $1 \leq \ell < m/2$.

Proof. Recall from Notation 4.2 that Ω is the set of ℓ-subsets of $\{1,\ldots,m\}$. Let $\pi \in \mathsf{S}_m$. Let $\operatorname{fix}(\pi)$ denote the set of ℓ-subsets fixed by π, as in Lemma 4.4. Note that

$$\sigma'(\pi) \leq |\operatorname{fix}(\pi)| + \frac{1}{2}\left(\binom{m}{\ell} - |\operatorname{fix}(\pi)|\right) = \frac{1}{2}\left(\binom{m}{\ell} + |\operatorname{fix}(\pi)|\right). \tag{4.3}$$

Furthermore, by Lemma 2.2,

$$n(\mathsf{S}_m, B) = \frac{1}{|\mathsf{S}_m|} \sum_{\pi \in \mathsf{S}_m} k^{\sigma'(\pi)}.$$

We decompose this into two smaller sums, depending on whether $\sigma(\pi)$ is smaller or larger than $3m/4$:

$$n(\mathsf{S}_m, B) = n_1(\mathsf{S}_m, B_1) + n_2(\mathsf{S}_m, B_1),$$

where

$$n_1(\mathsf{S}_m, B) = \frac{1}{|\mathsf{S}_m|} \sum_{\sigma(\pi) \leq 3m/4} k^{\sigma'(\pi)} \text{ and } n_2(\mathsf{S}_m, B) = \frac{1}{|\mathsf{S}_m|} \sum_{\sigma(\pi) > 3m/4} k^{\sigma'(\pi)}.$$

By using (4.3), we get

$$n_1(\mathsf{S}_m, B) \leq \frac{1}{m!} \sum_{\sigma(\pi) \leq 3m/4} k^{\frac{1}{2}\left(\binom{m}{\ell} + |\operatorname{fix}(\pi)|\right)},$$

and it follows from Lemma 4.4 that

$$n_1(\mathsf{S}_m, B) \leq k^{\frac{7}{8}\binom{m}{\ell}}$$

for every $m \geq N_1$ for some positive integer N_1.

We now work on $n_2(\mathsf{S}_m, B)$. Recall that $\mathcal{S}(j, m)$ denotes the number of elements of S_m with precisely j cycles. So

$$n_2(\mathsf{S}_m, B) \leq \frac{1}{m!} \sum_{j > 3m/4} \mathcal{S}(j, m) k^{\binom{m}{\ell}}.$$

Using the bound for $\mathcal{S}(j, m)$ in Lemma 4.3, we deduce that

$$n_2(\mathsf{S}_m, B) \leq \frac{1}{4} m (m!)^{-0.59} k^{\binom{m}{\ell}}$$

for every $m \geq N_2$ for some positive integer N_2. Now taking $N_3 := \max\{N_1, N_2\}$, we arrive at

$$n(\mathsf{S}_m, B) \leq k^{\frac{7}{8}\binom{m}{\ell}} + \frac{1}{4} m (m!)^{-0.59} k^{\binom{m}{\ell}}$$

for every $m \geq N_3$, and the result readily follows. □

5. Large base groups

In this section we complete the proof of Theorem 1.1 for primitive permutation groups by proving the following.

Theorem 5.1. *Let X be a non-trivial finite group and let $k := k(X)$. Let $t \geq 1$, $m \geq 5$, $1 \leq \ell < m/2$, and $(t, \ell) \neq (1, 1)$. Let H be a large base primitive permutation group of degree $n := \binom{m}{\ell}^t$, as in Definition 4.1. Let $G = X \wr H$. Then $k(G) \leq k^n$ for every sufficiently large k or n.*

Recall that Ω denotes the set of ℓ-subsets of $\{1,...,m\}$. For $\pi \in \mathsf{S}_m$, let $\sigma'(\pi)$ be the number of its cycles as a permutation on Ω. For $x \in \mathsf{S}_m \wr \mathsf{S}_t$, let $\gamma(x)$ be the number of its cycles as a permutation on Ω^t. (Of course, $\gamma(x) = \sigma'(x)$ when $t = 1$.) Recall also that $(\mathsf{S}_m)^t$ has a natural product action on $B_t = \mathrm{Irr}(X)^{\binom{m}{\ell}^t}$ and $n((\mathsf{S}_m)^t, B_t)$ denotes the number of its orbits.

In the next proposition we will need a general bound $f(n)$ for the number of conjugacy classes of a permutation group of degree n which does not rely on the classification of finite simple groups. Kovács and Robinson [16, Theorem 1.2] proved that $f(n)$ may be taken to be 5^{n-1}.

Proposition 5.2. *Assume the notation and hypothesis of Theorem 5.1. Then*

$$k(G) < 5^{mt}\left(2^t n((\mathsf{S}_m)^t, B_t) + k^{2n/3}\right).$$

Proof. Let $D := (\mathsf{S}_m)^t \cap H$ be the 'diagonal' subgroup of H. By Lemma 2.2, the number of orbits of H acting on $B_t = \mathrm{Irr}(X^n)$ is

$$n(H, B_t) = \frac{1}{|H|}\sum_{x\in H} k^{\gamma(x)} = \frac{1}{|H|}\sum_{x\in D} k^{\gamma(x)} + \frac{1}{|H|}\sum_{x\in H\setminus D} k^{\gamma(x)}. \tag{5.1}$$

For $x \in H$, we write $\mathrm{fix}(x)$ to denote the set of elements in Ω^t fixed by x. By (2.3) we have

$$\gamma(x) \leq \frac{n}{2}(1 + \mathrm{fpr}(x)),$$

where $\mathrm{fpr}(x) = |\,\mathrm{fix}(x)|/n$ is the fixed point ratio of x. Let $x \in H \setminus D$ and let us write $x = (x_1, \ldots, x_t)\pi \in H$ for $x_1, \ldots, x_t \in \mathsf{S}_m$ and $1 \neq \pi \in \mathsf{S}_t$. We know that π must contain a cycle of length r for some $r \geq 2$. A straightforward computation shows that $\mathrm{fix}(x) \leq |\Omega|^{t-(r-1)}$ (see also [1, Proposition 6.1] for a similar argument) and thus

$$\mathrm{fpr}(x) \leq |\Omega|^{1-r} \leq (r+1)^{-1} \leq 1/3,$$

where the second inequality holds since $|\Omega| \geq 5$. Thus, the second term in the far-right-hand-side sum in (5.1) is bounded by $k^{2n/3}$.

On the other hand, for the first term, we have

$$\frac{1}{|H|}\sum_{x\in D} k^{\gamma(x)} \leq \frac{1}{|\mathsf{A}_m|^t}\sum_{x\in D} k^{\gamma(x)} \leq \frac{1}{|\mathsf{A}_m|^t}\sum_{x\in (\mathsf{S}_m)^t} k^{\gamma(x)} = 2^t n((\mathsf{S}_m)^t, B_t).$$

We have shown that

$$n(H, B_t) \leq 2^t n((\mathsf{S}_m)^t, B_t) + k^{2n/3}.$$

Note that $H \leq \mathsf{S}_m \wr \mathsf{S}_t$ and $\mathsf{S}_m \wr \mathsf{S}_t$ may be viewed as a subgroup of S_{mt}. It follows that every subgroup of H has at most 5^{mt} classes, by [16, Theorem 1.2]. The desired bound now follows by using Lemma 2.1. $\square$

The next lemma relates the number of orbits of the product action of $(\mathsf{S}_m)^t$ (on B_t) and that of S_m (on B_1). This allows us to use the results in Section 4 on bounding $n(\mathsf{S}_m, B_1)$ to obtain similar bounds for $n((\mathsf{S}_m)^t, B_t)$, which in turn provides corresponding bounds for $k(G)$ by using Proposition 5.2.

Lemma 5.3. $n((\mathsf{S}_m)^t, B_t) = n(\mathsf{S}_m, B_1)^t$.

Proof. Observe that $B_t = (B_1)^t$ and an element $x = (x_1, \dots, x_t) \in (\mathsf{S}_m)^t$ fixes $(\chi_1, \dots, \chi_t) \in B_t$ if and only if each $x_i \in \mathsf{S}_m$ fixes $\chi_i \in B_1$ for every i. Now,

$$\begin{aligned} n((\mathsf{S}_m)^t, B_t) &= \frac{1}{|\mathsf{S}_m|^t} \sum_{x \in (\mathsf{S}_m)^t} |\operatorname{fix}(x, B_t)| \\ &= \frac{1}{|\mathsf{S}_m|^t} \sum_{x_1 \in \mathsf{S}_m} \cdots \sum_{x_t \in \mathsf{S}_m} |\operatorname{fix}(x_1, B_1)| \cdots |\operatorname{fix}(x_t, B_1)| \\ &= \frac{1}{|\mathsf{S}_m|^t} \left(\sum_{x_1 \in \mathsf{S}_m} |\operatorname{fix}(x_1, B_1)| \right)^t \\ &= n(\mathsf{S}_m, B_1)^t, \end{aligned}$$

and the lemma follows. □

We are now ready to prove the main result of this section.

Proof of Theorem 5.1. By Proposition 5.2 and Lemma 5.3, we have

$$k(G) < 5^{mt} \left(2^t n(\mathsf{S}_m, B_1)^t + k^{2n/3} \right). \tag{5.2}$$

Obviously, $n(\mathsf{S}_m, B_1) \leq |B_1| = k^{\binom{m}{\ell}}$. Hence

$$k(G) < 5^{mt} 2^t k^{\binom{m}{\ell} t} + 5^{mt} k^{2n/3}.$$

It is straightforward to see that, as $(t, \ell) \neq (1, 1)$, both terms on the right-hand side are less than $\frac{1}{2} k^{\binom{m}{\ell}^t}$ for every sufficiently large t. We assume from now on that t is bounded.

Next, using Proposition 4.6 together with (5.2), we have that there exists a positive integer N such that, for every $m \geq N$,

$$\begin{aligned} k(G) &< 5^{mt} 4^t (\max\{k^{\frac{7}{8}\binom{m}{\ell}}, (m!)^{-0.58} k^{\binom{m}{\ell}}\})^t + 5^{mt} k^{2n/3} \\ &\leq 5^{mt} 4^t k^{\frac{7t}{8}\binom{m}{\ell} t} + 5^{mt} 4^t (m!)^{-0.58t} k^{\binom{m}{\ell} t} + 5^{mt} k^{2n/3}. \end{aligned}$$

With t being bounded, each of these three terms is less than $\frac{1}{3} k^{\binom{m}{\ell}^t}$, and therefore $k(G) \leq k^n$, for every sufficiently large m.

We now assume that both t and m are bounded, or equivalently, that n is bounded. Given the hypothesis that H is a primitive group that is different from S_n, it follows that H does not contain a transposition. In this case, the remark following (2.3) shows that $k(G) < k^n$ for all sufficiently large k. This completes the proof. $\square$

For primitive groups H, Theorem 1.1 follows from Theorems 2.5, 3.1 and 5.1.

6. Semiprimitive groups

In this section we complete the proof of Theorem 1.1 by proving it for semiprimitive groups which are not primitive.

Proof of Theorem 1.1. Let H be a semiprimitive permutation group. This is a transitive permutation group all of whose normal subgroups are transitive or semiregular. We may assume at this point that H is not primitive. The group H acts on the set Ω of factors of X^n. Let

$$Y := X^{n/r}$$

for some divisor $r \leq n/2$ of n such that H acts primitively on the set $\overline{\Omega}$ of factors of Y^r. Let the kernel of this action be K. Since this is an intransitive normal subgroup of H, it must be semiregular on Ω.

Let h be an element of H. Let the number of cycles of h acting on Ω and $\overline{\Omega}$ be denoted by $\sigma_\Omega(h)$ and $\sigma_{\overline{\Omega}}(h)$, respectively. Observe that $\sigma_\Omega(h) \leq (n/r) \cdot \sigma_{\overline{\Omega}}(h)$.

We have

$$\begin{aligned}\alpha(H) := \max_{1 \neq h \in H} \frac{\sigma_\Omega(h)}{n} &= \max\left\{\max_{1\neq h \in K} \frac{\sigma_\Omega(h)}{n}, \max_{h \in H\setminus K} \frac{\sigma_\Omega(h)}{n}\right\} \\ &\leq \max\left\{\frac{1}{2}, \max_{h\in H\setminus K}\frac{\sigma_{\overline{\Omega}}(h)}{r}\right\}.\end{aligned}$$

It follows that if r is bounded by an absolute constant, then $\alpha(H)$ is a fixed number less than 1 and so $k(G) \leq k^n$ for every sufficiently large n or k by (2.1). We may therefore assume that $r \to \infty$, in particular, $n \to \infty$.

If H/K is not a large base group (see Definition 4.1), then

$$|H| = |H/K||K| \leq |H/K| \cdot n = \exp(O(n^{1/3} \log^{7/3} n))$$

by (2.5). In this case the result follows from Theorem 2.4.

For general H/K, we have

$$\begin{aligned} n(H, \mathrm{Irr}(X^n)) = \frac{1}{|H|}\sum_{h\in H} k^{\sigma_\Omega(h)} = \frac{1}{|H|}\Big(\sum_{h\in H\setminus K} k^{\sigma_\Omega(h)} + \sum_{h \in K} k^{\sigma_\Omega(h)}\Big) \leq \\ \leq \frac{1}{|H|}\Big(|K| \sum_{1\neq \bar{h}\in H/K} k^{\sigma_{\overline{\Omega}}(\bar{h})\cdot(n/r)} + k^n + (|K|-1)k^{n/2}\Big) < \\ < n\left(H/K, \mathrm{Irr}(Y^r)\right) + \frac{k^n}{|H|} + \frac{nk^{n/2}}{|H|}, \end{aligned}$$

where $n(H/K, \mathrm{Irr}(Y^r))$ is the number of orbits of $R = H/K$ on $\mathrm{Irr}(Y^r) = \mathrm{Irr}(Y)^r$ where the action of R is defined from the action of the primitive permutation group R acting on the set of factors of Y^r (that is, R acts primitively on the set of factors of $\mathrm{Irr}(Y)^r$).

The number $k(G)$ is equal to the sum of the numbers of conjugacy classes of $n(H, \mathrm{Irr}(X^n))$ inertia subgroups, by Lemma 2.1. As before, let e be the maximum of these numbers. Since K is semiregular, at most $\sum_{1\neq h\in K} k^{\sigma_\Omega(h)} < (n/r)k^{n/2}$ of the inertia subgroups intersect K nontrivially. These numbers contribute less than $e(n/r)k^{n/2} \leq (n/r)^2 \cdot 5^{r/3}k^{n/2}$ to $k(G)$. (For $H/K \in \{\mathsf{S}_r, \mathsf{A}_r\}$ this follows from [17] and from the statement in the second paragraph of Section 3, otherwise $|H/K| \leq 5^{r/3}$ for every sufficiently large r by [20, Corollary 1.6].) Since $r \leq n/2$, we have $(n/r)^2 \cdot 5^{r/3}k^{n/2} \leq n^2 \cdot 5^{n/6}k^{n/2}$ and this is less than $k^n/16$ for every sufficiently large n. Thus we have

$$\begin{aligned} k(G) &\leq e_K \cdot n\left(H, \mathrm{Irr}(X^n)\right) + \frac{k^n}{16} \\ &< e_K \cdot n\left(H/K, \mathrm{Irr}(Y^r)\right) + \frac{e_K \cdot k^n}{|H|} + \frac{e_K \cdot nk^{n/2}}{|H|} + \frac{k^n}{16}, \end{aligned}$$

where e_K denotes the maximum of the numbers of conjugacy classes of those inertia subgroups of H which intersect with K trivially. Note that e_K is at most the maximum of the numbers of classes of subgroups of H/K.

Recall that we are done when H/K is not a large base group, and so we assume in the remainder of the proof that H/K is a large base group. We shall follow the notation in Definition 4.1 and Notation 4.2, with Y and r in place of X and n, respectively. In particular, $(\mathsf{A}_m)^t \leq H/K \leq \mathsf{S}_m \wr \mathsf{S}_t$ for some $t \geq 1$ and $m \geq 5$. Also, $r = \binom{m}{\ell}^t$.

Since H is not abelian, we have $e_K \leq (5/8)|H|$ by [11]. It follows that

$$\frac{e_K \cdot k^n}{|H|} + \frac{e_K \cdot nk^{n/2}}{|H|} + \frac{k^n}{16} \leq \frac{3}{4}k^n$$

for every sufficiently large n. Note that H/K can be viewed as a subgroup of S_{mt}, and so $e_K \leq 5^{mt}$ by [16, Theorem 1.2]. To establish $k(G) \leq k^n$ for sufficiently large n or k, it is now sufficient to show that

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq \frac{k^n}{4 \cdot 5^{mt}} \tag{6.1}$$

for every sufficiently large r, or equivalently, every sufficiently large m or t.

Let $(t, \ell) = (1, 1)$. In this case we may replace the above bound $e_K \leq 5^{mt}$ by $e_K \leq 5^{mt/3}$ as discussed above. We have

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq 2 \cdot \binom{r + k^{n/r} - 1}{r} \leq 2 \cdot 3^r \Big(\frac{r + k^{n/r} - 1}{r}\Big)^r < 2 \cdot 3^r \Big(\frac{k^{n/r}}{r} + 1\Big)^r.$$

If $k^{n/r}/r \geq 1$, then

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq 2 \cdot 6^r \left(\frac{k^n}{r^r}\right) < k^n/(4 \cdot 5^{mt/3})$$

for every sufficiently large $r = m$. Let $k^{n/r} \leq r$. Then $n(H/K, \mathrm{Irr}\,(Y^r)) \leq 4^r$. This is less than $k^n/(4 \cdot 5^{r/3})$ for every sufficiently large r, unless $n = 2r$ and $k = 2$. In the exceptional case $n(H/K, \mathrm{Irr}\,(Y^r)) \leq (r+3)(r+2)(r+1)/3$, which is again less than $k^n/(4 \cdot 5^{r/3})$ for every sufficiently large r. Let $(t, \ell) \neq (1, 1)$.

First, arguing as in the proof of Proposition 5.2 and using Lemma 5.3, we have

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq 2^t n\left((\mathsf{S}_m)^t, B_t\right) + k(Y)^{2r/3} = 2^t n\left(\mathsf{S}_m, B_1\right)^t + k(Y)^{2r/3}.$$

When $t \to \infty$, one may use the obvious bound $n\left(\mathsf{S}_m, B_1\right) \leq |B_1| = k(Y)^{\binom{m}{\ell}}$ to achieve (6.1). So we assume that t is bounded.

Next, using Proposition 4.6, we deduce that

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq 4^t k(Y)^{\frac{7}{8}\binom{m}{\ell}t} + 4^t (m!)^{-0.58t} k(Y)^{\binom{m}{\ell}t} + k(Y)^{2r/3}.$$

for every sufficiently large m. As $k(Y) = k^{n/r}$, it follows that

$$n(H/K, \mathrm{Irr}\,(Y^r)) \leq 4^t k^{\frac{7}{8r}\binom{m}{\ell}tn} + 4^t (m!)^{-0.58t} k^{\frac{1}{r}\binom{m}{\ell}tn} + k^{2n/3}.$$

With $n \geq 2r = 2\binom{m}{\ell}^t$, $m \to \infty$, and t being bounded, it is straightforward to verify that this sum is less than the right-hand side of (6.1), and the proof is complete. □

Acknowledgement

This work was carried out while the first and third authors were visiting Budapest. They gratefully acknowledge the hospitality of the Alfréd Rényi Institute of Mathematics.

References

[1] T. C. Burness and R. M. Guralnick, Fixed point ratios for finite primitive groups and applications. *Adv. Math.* **411** (2022), Paper No. 108778. 12

[2] J. D. Dixon and B. Mortimer, Permutation groups. Grad. Texts in Math. 163, Springer - Verlag, New York 1996. 5

[3] D. Dona, A. Maróti, and L. Pyber, Growth of products of subsets in finite simple groups. *Bull. Lond. Math. Soc.* **56** (2024), no. 8, 2704–2710. 6, 7

[4] S. Eberhard and D. Garzoni, Random generation with cycle type restrictions, *Algebr. Comb.* **4** (2021), no. 1, 1–25. 9

[5] P. Erdős, On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. of Math.* (2) **43** (1942), 437–450. 7, 9

[6] J. Fulman and R. M. Guralnick, Enumeration of conjugacy classes in affine groups. *Algebra Number Theory* **18** (2024), no. 6, 1189–1219. 1

[7] M. Garonzi and A. Maróti, On the number of conjugacy classes of a permutation group. *J. Combin. Theory Ser. A* **133** (2015), 251–260. 4, 6, 7

[8] D. Garzoni and N. Gill, On the number of conjugacy classes of a primitive permutation group. *Proc. Roy. Soc. Edinburgh Sect. A* **153** (2023), no. 1, 115–136. 2, 5, 6
[9] R. M. Guralnick and A. Maróti, On the non-coprime $k(GV)$-problem. *J. Algebra* **385** (2013), 80–101. 1
[10] R. M. Guralnick and P. H. Tiep, The non-coprime $k(GV)$ problem. *J. Algebra* **293** (2005), no. 1, 185–242. 1
[11] W. H. Gustafson, What is the probability that two group elements commute? *Amer. Math. Monthly* **80** (1973), 1031–1034. 15
[12] M. I. Isaacs, *Character theory of finite groups*. Dover Publications, Inc., New York, 1994. 3
[13] G. James and A. Kerber, *The representation theory of the symmetric group*. Encyclopedia Math. Appl. **16**, Addison-Wesley Publishing Co., Reading, MA, 1981. 3
[14] T. M. Keller, Inductive arguments for the non-coprime $k(GV)$-problem. *Algebra Colloq.* **13** (2006), no. 1, 35–39. 1
[15] T. M. Keller, Counting characters in linear group actions. *Israel J. Math.* **171** (2009), 367–384. 1
[16] L. G. Kovács, G. R. Robinson, On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), no. 2, 441–460. 12, 15
[17] H. Nagao, On a conjecture of Brauer for p-solvable groups. *J. Math. Osaka City Univ.* **13** (1962), 35–38. 15
[18] G. Navarro, Some remarks on global/local conjectures. Finite simple groups: thirty years of the atlas and beyond, 151–158. Contemp. Math., 694 American Mathematical Society, Providence, RI, 2017. 1
[19] P. Schmid, *The solution of the $k(GV)$ problem*. ICP Adv. Texts Math. **4**, Imperial College Press, London, 2007. 1, 2, 6
[20] X. Sun and J. Wilmes, Structure and automorphisms of primitive coherent configurations. ArXiv:1510.02195. 5, 15

Department of Mathematics, The University of Akron, Akron, OH 44325, USA
Email address: hungnguyen@uakron.edu

Hun-Ren Alfréd Rényi Institute of Mathematics, Reáltanoda Utca 13-15, H-1053, Budapest, Hungary
Email address: maroti@renyi.hu

Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain
Email address: Juan.Martinez-Madrid@uv.es