A PROOF OF PYBER'S BASE SIZE CONJECTURE

HÜLYA DUYAN, ZOLTÁN HALASI, AND ATTILA MARÓTI

Abstract. Building on earlier papers of several authors, we establish that there exists a universal constant $c > 0$ such that the minimal base size $b(G)$ of a primitive permutation group G of degree n satisfies $\log |G|/\log n \leq b(G) < 45(\log |G|/\log n) + c$. This finishes the proof of Pyber's base size conjecture. The main part of our paper is to prove this statement for affine permutation groups $G = V \rtimes H$ where $H \leq GL(V)$ is an imprimitive linear group. An ingredient of the proof is that for the distinguishing number $d(G)$ (in the sense of Albertson and Collins) of a transitive permutation group G of degree $n > 1$ we have the estimates $\sqrt[n]{|G|} < d(G) \leq 48 \sqrt[n]{|G|}$.

1. Introduction

Let G be a permutation group acting on a finite set Ω of size n. A subset Σ of Ω is called a base for G if the intersection of the stabilizers in G of the elements of Σ is trivial. Bases played a key role in the development of permutation group theoretic algorithms. For an account of such algorithms see the book of Seress [41]. Since these algorithms are generally faster and require less memory if the size of the base is small, it is fundamentally important to find a base of small size.

The minimal size of a base for G on Ω is denoted by $b(G)$. Blaha [8] showed that the problem of finding $b(G)$ for a permutation group G is NP-hard. One may approximate $b(G)$ by a greedy heuristic; always choose a point from Ω whose orbit is of largest possible size under the action of the intersection of the stabilizers in G of the previous points chosen. Blaha [8] proved that the size of such a base is $O(b(G) \log \log n)$ and that this bound is sharp. (Here and throughout the paper the base of the logarithms is 2 unless otherwise stated.) On the other hand, Pyber [36] showed that there exists a universal constant $c > 0$ such that almost all (a proportion tending to 1 as $n \to \infty$) subgroups G of $\mathrm{Sym}(n)$ satisfy $b(G) > cn$.

Date: April 4, 2018.

2010 *Mathematics Subject Classification.* 20B15, 20C99, 20B40.

Key words and phrases. minimal base size, distinguishing number, permutation group, linear group.

The second author was supported from the ERC Limits of discrete structures Grant No. 617747. The third author has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 648017) and was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The second and third authors were also supported by a Humboldt Return Fellowship and by National Research, Development and Innovation Office (NKFIH) Grant No. K115799.

The minimal base size of a primitive permutation group G of degree n not containing $\mathrm{Alt}(n)$ has been widely studied. Already in the nineteenth century Bochert [9] showed that $b(G) \leq n/2$ for such a group G. This bound was substantially improved by Babai to $b(G) < 4\sqrt{n}\log n$, for uniprimitive groups G, in [2], and to the estimate $b(G) < 2^{c\sqrt{\log n}}$ for a universal constant $c > 0$, for doubly transitive groups G, in [3]. The latter bound was improved by Pyber [35] to $b(G) < c(\log n)^2$ where c is a universal constant. These estimates are elementary in the sense that their proofs do not require the Classification of Finite Simple Groups (CFSG). Using CFSG, Liebeck [29] classified all primitive permutation groups G of degree n with $b(G) \geq 9\log n$.

Let G be an almost simple primitive permutation group. We say that G is standard if either G has alternating socle $\mathrm{Alt}(m)$ and the action is on subsets or partitions of $\{1, \ldots, m\}$, or G is a classical group acting on an orbit of subspaces (or pairs of subspaces of complementary dimension) of the natural module. Otherwise G is said to be non-standard. A well-known conjecture of Cameron and Kantor [16] asserts that there exists an absolute constant c such that $b(G) \leq c$ for all non-standard primitive permutation groups G. In case G has an alternating socle, this was established by Cameron and Kantor [16]. Later in [15, p. 122] Cameron writes that c can probably be taken to be 7, and the only extreme case is the Mathieu group M_{24} in its natural action. The Cameron-Kantor conjecture was proved by Liebeck and Shalev in [30], and Cameron's bound of 7 was established in the series of papers [32], [33], [10], [12], [13], [11]. The proofs are probabilistic and use bounds on fixed point ratios.

Let d be a fixed positive integer. Let Γ_d be the class of finite groups G such that G does not have a composition factor isomorphic to an alternating group of degree greater than d and no classical composition factor of rank greater than d. Babai, Cameron, Pálfy [4] showed that if $G \in \Gamma_d$ is a primitive permutation group of degree n, then $|G| < n^{f(d)}$ for some function $f(d)$ of d. Babai conjectured that there is a function $g(d)$ such that $b(G) < g(d)$ whenever G is a primitive permutation group in Γ_d. Seress [39] showed this for G a solvable primitive group by establishing the bound $b(G) \leq 4$. Babai's conjecture was proved by Gluck, Seress, Shalev [21] with a bound $g(d)$ which is quadratic in d. Later, Liebeck and Shalev [30] showed that in Babai's conjecture the function $g(d)$ can be taken to be linear in d.

Since any element of a permutation group G is determined by its action on a base, we clearly have $|G| \leq n^{b(G)}$ where $n = |\Omega|$ is the degree of G. From this we get the estimate $\log|G|/\log n \leq b(G)$. An important question of Pyber [36, Page 207] from 1993 asks if this latter bound is essentially sharp for primitive permutation groups G. Specifically, he asked whether there exists a universal constant $c > 0$ such that

$$b(G) < c\frac{\log|G|}{\log n}.$$

Pyber's conjecture is an essential generalization of the known upper bounds for $b(G)$, the Cameron-Kantor conjecture, and Babai's conjecture.

By the Aschbacher-O'Nan-Scott theorem, primitive permutation groups fall in several types: almost simple type, diagonal type, product type, twisted wreath product type, and affine type. Pyber's conjecture has been verified for all non-affine primitive permutation groups. For non-standard (almost simple) permutation groups Pyber's conjecture follows from the proof of the Cameron-Kantor conjecture, and for standard (almost simple) permutation groups Pyber's conjecture was settled by Benbenishty in [7]. Primitive permutation groups of diagonal type were handled by Gluck, Seress, Shalev [21, Remark 4.3] and Fawcett [18]. For primitive groups of product type and of twisted wreath product type the conjecture was established by Burness and Seress [14]. From these results one can deduce the general bound

$$b(G) < 45\frac{\log |G|}{\log n}$$

for a non-affine primitive permutation group G of degree n.

An affine primitive permutation group G acting on a set Ω is defined to be a primitive permutation group with a (unique) regular abelian normal subgroup V. The subgroup V is elementary abelian. Identifying Ω with V, denote the stabilizer in G of the zero vector by H. The group H can be viewed as a subgroup of $GL(V)$ and $G = V \rtimes H$ as a subgroup of $AGL(V)$. Since G is a primitive permutation group, H is maximal in G and acts irreducibly and faithfully on V. The action of H on V may or may not preserve a non-trivial direct sum decomposition of the vector space V. In the first case V is said to be an imprimitive H-module, and in the latter case V is called a primitive H-module. In this paper we will simply call H an imprimitive linear group or a primitive linear group if V is imprimitive or primitive, respectively.

The most general result on the base size of affine primitive permutation groups is due to Liebeck and Shalev [31], [34] who established Pyber's conjecture in the case where H is a primitive linear group (see Theorem 3.1). In this paper we use a characterization of primitive linear groups of unbounded base size given by Liebeck and Shalev [31], [34] (see Theorem 3.17). There is a similar characterization of primitive linear groups of large orders due to Jaikin-Zapirain and Pyber [27, Proposition 5.7].

In case $(|H|, |V|) = 1$ for an affine primitive permutation group $G = V \rtimes H$, Pyber's conjecture was first established by Gluck and Magaard in [20] by showing that $b(G) \leq 95$. In fact, in this case the best possible result is $b(G) \leq 3$ proved by Halasi and Podoski in [26]. Solvable or more generally, p-solvable affine primitive permutation groups also satisfy Pyber's conjecture (where p is the prime divisor of the degree). In these cases, Seress [39] and Halasi and Maróti [25] established the best possible bound $b(G) \leq 4$. Fawcett and Praeger [19] proved Pyber's conjecture for affine primitive permutation groups $G = V \rtimes H$ in case H preserves a direct sum decomposition $V = V_1 \oplus \ldots \oplus V_t$ where H is close to a full wreath product $GL(V_1) \wr L$ with L a permutation group of degree t satisfying any of four given properties.

In this paper we complete the proof of Pyber's conjecture by handling the case of affine primitive permutation groups $G = V \rtimes H$ where V is an imprimitive H-module. A stronger form of Pyber's conjecture is the following.

Theorem 1.1. *There exists a universal constant $c > 0$ such that the minimal base size $b(G)$ of a primitive permutation group G of degree n satisfies*

$$\frac{\log |G|}{\log n} \leq b(G) < 45\frac{\log |G|}{\log n} + c.$$

The minimal base size of a permutation group is related to several other invariants of the group. For example, Robinson [37] showed that if G is a primitive permutation group of degree n and rank r, then $b(G) \leq (n-1)/(r-1)$. The minimal degree m of a transitive permutation group of degree n is also related to the minimal base size b by the inequality $mb \geq n$.

There are at least two concepts termed by the name "distinguishing number". Both of these are connected to the minimal base size of a group. In 1981 Babai [2] defined the distinguishing number of a coherent configuration and used it to establish the aforementioned bound for the minimal base size. This notion was later also used in a recent paper by Sun and Wilmes [42]. In the present paper we use a different concept with the same name. This different definition was introduced for graphs in 1996 by Albertson and Collins [1] and since then many authors have used it under the name "distinguishing number". For more information, see Sections 2.2 and 3.4 of the excellent survey article by Bailey and Cameron [5].

For a permutation group G acting on a finite set Ω we write $d(G)$ for the minimal number of colors needed to color the elements of Ω in such a way that the stabilizer in G of this coloring is trivial. This invariant is called the distinguishing number of the permutation group. Seress [39] proved that $d(G) \leq 5$ for a solvable permutation group G. By results of Seress [40] and Dolfi [17], it follows that $d(G) \leq 4$ for a primitive permutation group G of degree n which does not contain $\mathrm{Alt}(n)$. Clearly, if G is a permutation group of degree $n > 1$, then $\sqrt[n]{|G|} < d(G)$. Burness and Seress [14] stated (with a different languague) that there exists a universal constant $c > 0$ such that $d(G) \leq |G|^{c/n}$ provided that G is a transitive permutation group of degree n (see also Theorem 2.2 and the discussion preceding it). The proof of this latter fact misses a case. In this paper we show the following stronger result.

Theorem 1.2. *Let G be a transitive permutation group of degree $n > 1$. Then $\sqrt[n]{|G|} < d(G) \leq 48\sqrt[n]{|G|}$.*

This result (and its proof) plays a key role in handling the "top action" of an imprimitive irreducible linear group. For a rough idea of this application, see Lemma 3.2.

This paper is organized as follows. In Section 2 we examine the distinguishing number of transitive permutation groups and we prove Theorem 1.2. One of the intermediate results, namely, Theorem 2.8, will also be used later in Section 3.3.

In Section 3 we prove Theorem 1.1 for affine permutation groups. The main difficulty arising here is that there are linear groups $G \leq GL(V)$ preserving a direct sum decomposition $V = V_1 \oplus \ldots \oplus V_t$ such that $N_G(V_1)/C_G(V_1) \leq GL(V_1)$ is a large linear group, while G still acts faithfully on $\{V_1, \ldots, V_t\}$. Therefore, in Section 3.1, we generalise the concept of an imprimitive linear group in order to be able to use a reduction argument. In Section 3.1 we also consider the case when the H-module V is induced from an H_1-module V_1 such that the base size of H_1 on V_1 is bounded. In Sections 3.2 and 3.3 we consider two special cases which we will call alternating-induced and classical-induced representations. Finally, in Section 3.4 we complete the proof of Pyber's conjecture for affine permutation groups by using a structure theorem of Liebeck and Shalev for primitive linear groups of unbounded base size and by reducing this problem to one of the previously handled cases in Sections 3.1-3.3. In the final section we indicate that Pyber's conjecture holds for all non-affine primitive permutation groups with multiplicative constant 45.

2. The distinguishing number of a transitive permutation group

Let G be a group acting (not necessarily faithfully) on a finite set Ω. A base for G is a subset Σ of Ω such that the intersection of the stabilizers in G of all points in Σ is the kernel of the action of G on Ω. We denote the minimal size of a base for G by $b(G)$ or by $b_\Omega(G)$ if Ω is to be specified. More generally, for any normal subgroup N of G we set $b_\Omega(G/N) = \min\{k \mid \exists x_1, \ldots, x_k \in \Omega,\ \cap_{i=1}^{k} G_{x_i} \leq N\}$. A trivial observation is that

$$\max\{b(N), b(G/N)\} \leq b(G) \leq b(N) + b(G/N).$$

The purpose of this section is to study yet another invariant which is closely related to the minimal base size (see Lemma 2.1).

A distinguishing partition for a finite group G acting (not necessarily faithfully) on a finite set Ω is a coloring of the points of Ω in such a way that every element of G fixing this coloring is contained in the kernel of the action of G on Ω. The minimal number of parts (or colors) of a distinguishing partition is called the distinguishing number of G and is denoted by $d(G)$ or by $d_\Omega(G)$. As for the minimal base size above, for any normal subgroup N of G we define $d(G/N)$ to be the minimal number of colors needed to color the points of Ω in such a way that the stabilizer in G of this coloring is contained in N. Clearly, for every subgroup H of G and for every normal subgroup N of G we have

$$\max\{d(H), d(G/N)\} \leq d(G) \leq d(N)d(G/N).$$

The following lemma is of importance to us.

Lemma 2.1. *Let G be a finite group acting on a finite set Ω. For an integer $q \geq 2$ let $P^q(\Omega)$ denote the set of all partitions of Ω into at most q parts. Then $b_{P^q(\Omega)}(G) = \lceil \log_q(d(G)) \rceil$.*

Proof. Put $\Omega = \{1, \ldots, n\}$. We view $P^q(\Omega)$ as the direct product of n copies of the set $\{0, \ldots, q-1\}$. Moreover we think of the elements of $P^q(\Omega)$ as column vectors of length n. For a subset $P = \{v_1, \ldots, v_\ell\}$ of $P^q(\Omega)$ let X be the n-by-ℓ matrix whose ℓ columns are the vectors $v_1, \ldots, v_\ell$. Let $D = \{w_1, \ldots, w_n\}$ be the set of row vectors in X. For an arbitrary i in $\{1, \ldots, n\}$ the vector w_i can be thought of as the color of the element i in Ω.

Assume that D does not define a distinguishing partition for G on Ω. Then there exists an element $g \in G$ that does not act trivially on Ω and preserves the coloring D of Ω, that is, $w_i = w_j$ whenever i is mapped to $j(\neq i)$ by g. It follows that g fixes every vector in P and therefore P is not a base for the action of G on $P^q(\Omega)$.

Assume now that P is not a base for the action of G on $P^q(\Omega)$. Then there exists $g \in G$ fixing every element of P such that g does not act trivially on Ω. Since this element g preserves the coloring D of Ω, we conclude that D is not a distinguishing partition for G on Ω.

We have shown that the set P is a base for the action of G on $P^q(\Omega)$ if and only if D defines a distinguishing partition (with $|D|$ colors) for G on Ω. The result follows. $\square$

The main result (Theorem 1.2) of this section determines, up to an explicit constant factor, the distinguishing number of a transitive permutation group.

By combining Lemma 2.1 and Theorem 1.2, we get the following (almost) equivalent form, a slightly weaker version of which appears in [14, Theorem 3.1]. In the following result, $P(n)$ denotes the power set of $\{1, \ldots, n\}$.

Theorem 2.2. *For any transitive permutation group G of degree $n > 1$ we have*

$$\frac{\log |G|}{n} < b_{P(n)}(G) < 7 + \frac{\log |G|}{n}.$$

In the following we aim to prove Theorem 1.2.

Let Ω be a finite set of size $n > 1$ and $G \leq \mathrm{Sym}(\Omega)$ be a (not necessarily transitive) permutation group.

For the lower bound in the statement of the theorem, notice that the action of G on Ω induces an action on the set of all colorings of Ω using $d(G)$ colors and this action contains a regular orbit. Thus $|G| < d(G)^n$.

From now on we will prove the upper bound in the statement of Theorem 1.2.

Let us first introduce some notation which we will use throughout the paper. For a finite group H acting on a set X and for a subset Y of X, we denote the setwise and the pointwise stabilizer of Y in H by $N_H(Y)$ and $C_H(Y)$ respectively. In the latter case when $Y = \{y_1, \ldots, y_s\}$ has size $s \geq 1$ we write $C_H(y_1, \ldots, y_s)$. Furthermore, for any natural number k, let $[k]$ denote the set $\{1, 2, \ldots, k\}$.

For a system of blocks of imprimitivity for G, say $\Gamma = \{\Delta_1, \ldots, \Delta_k\}$ with $|\Delta_1| = |\Delta_2| = \ldots = |\Delta_k| = m$, let $H_j = N_G(\Delta_j)$ for each j, and $N = \cap_{j=1}^k H_j$. Then H_j acts naturally on Δ_j with kernel $C_G(\Delta_j)$, so $H_j/C_G(\Delta_j) \leq \mathrm{Sym}(\Delta_j)$. Furthermore, G acts on Γ with kernel N, so $K := G/N \leq \mathrm{Sym}(\Gamma)$.

Our goal is to give an upper bound for the distinguishing number $d(G) = d_\Omega(G)$ of G in terms of the distinguishing numbers $d(K) = d_\Gamma(K)$ of K and $d(H_j) = d_{\Delta_j}(H_j)$ of H_j, and the degrees k and m.

Lemma 2.3. *If H_j acts trivially on Δ_j (i.e. $H_j = C_G(\Delta_j)$) for every $1 \leq j \leq k$, then $d(G) \leq \lceil \sqrt[m]{d(K)} \rceil$.*

Proof. The assumption of the lemma means that each orbit of G on Ω has at most one common point with the block Δ_j for every $j \in [k] := \{1, \ldots, k\}$. Thus, we can define a function $f : \Omega \mapsto [m]$ such that the restriction of f to Δ_j is bijective for every j and f is constant on every orbit of G. Set $c = \lceil \sqrt[m]{d(K)} \rceil$.

We define a c-coloring λ of Ω in the following way. Let us choose a $d(K)$-coloring $\alpha : \Gamma \mapsto \{0, 1, \ldots, d(K) - 1\}$ of Γ such that only the identity of K fixes α. For every $j \in [k]$ write $\alpha(\Delta_j)$ in its base c-expansion, so

$$\alpha(\Delta_j) = a_1(j)c^0 + a_2(j)c^1 + \ldots + a_{s+1}(j)c^s,$$

where $a_1(j), \ldots, a_{s+1}(j) \in \{0, \ldots, c-1\}$. Note that $s \leq m-1$ by the definition of c. If $s < m-1$, let us define $a_{s+2}(j) = \ldots = a_m(j) = 0$. Now, for any $x \in \Delta_j$ let $\lambda(x) = a_{f(x)}(j) \in \{0, \ldots, c-1\}$. We claim that only the identity element of G preserves λ. By assumption, $N = 1$, so it is enough to show that if $g \in G$ fixes λ, then g also fixes α. Let $g \in G$ fixing λ and $g(\Delta_j) = \Delta_{j'}$ for some $j, j' \in [k]$. Then we have $a_{f(x)}(j) = \lambda(x) = \lambda(g(x)) = a_{f(g(x))}(j')$ for every $x \in \Delta_j$. Using the properties of f, this means that $a_i(j) = a_i(j')$ for every $i \in [m]$, i.e. $\alpha(\Delta_j)$ and $\alpha(\Delta_{j'})$ have the same base c-expansion. □

From now on, let us assume that the action of G is transitive (so $H_j/C_{H_j}(\Delta_j) \leq \mathrm{Sym}(\Delta_j)$ are permutation isomorphic for all $j \in [k]$), and H_1 acts on Δ_1 in a primitive way. For the remainder of this section, we say that the action of H_1 on Δ_1 is large if $m = |\Delta_1| \geq 5$ and $\mathrm{Alt}(\Delta_1) \leq H_1/C_{H_1}(\Delta_1) \leq \mathrm{Sym}(\Delta_1)$.

Lemma 2.4. *With the above notation, if H_1 is not large, then $d(G) \leq 4 \cdot \lceil \sqrt[m]{d(K)} \rceil$.*

Proof. By the results of Seress [40, Theorem 2] and Dolfi [17, Lemma 1], $d(H_1) \leq 4$. This means that each Δ_j can be colored with colors $\{0, \ldots, 3\}$ such that any element of H_j fixing this coloring acts trivially on Δ_j. Let $\chi : \Omega \mapsto \{0, \ldots, 3\}$ be the union of these colorings. Then Lemma 2.3 can be applied to the stabilizer of χ in G, so there exist a $\lceil \sqrt[m]{d(K)} \rceil$-coloring $\lambda : \Omega \mapsto \{0, \ldots, \lceil \sqrt[m]{d(K)} \rceil - 1\}$ such that only the identity of G fixes both colorings λ and χ. Finally, one can encode the pair (χ, λ) by a $4 \cdot \lceil \sqrt[m]{d(K)} \rceil$-coloring μ of Ω by choosing a suitable bijective function, e.g. let $\mu(x) = 4 \cdot \lambda(x) + \chi(x)$. □

It is possible to slightly modify the proof of Lemma 2.4 (still using Lemma 2.3) to allow the situation when the action of H_1 on Δ_1 is not primitive. The modified statement is the following.

Remark 2.5. Suppose that $d(H_1) \leq c$ for some constant c where H_1 does not necessarily act primitively on Δ_1. Then $d(G) \leq c \cdot \lceil \sqrt[m]{d(K)} \rceil$.

Now we handle the case where the action of H_1 is large and $N \neq 1$. Then the socle of N is a subdirect product of alternating groups $\mathrm{Alt}(m)$. More precisely, by [38, p. 328, Lemma], the socle of N is of the form $\prod_j D_j$ where each D_j is isomorphic to $\mathrm{Alt}(m)$ and is a diagonal subgroup of a subproduct $\prod_{\ell \in I_j} C_\ell$ where $C_\ell \cong \mathrm{Alt}(m)$ and the subsets I_j form a partition of Γ with parts of equal size. (Moreover, they form a system of blocks for the action of G on Γ.) Let us denote the size of each part I_j by t. In accordance with [14], we will refer to this number as the linking factor of N. Thus, we have

$$\text{(Eq. 1)} \qquad \mathrm{Alt}(m)^{k/t} \leq N \leq \mathrm{Sym}(m)^{k/t}.$$

Lemma 2.6. *Let us assume that H_1 is large and $N \neq 1$ with linking factor t. Then $d(G) \leq 3 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$.*

Proof. If $m = 6$, then Remark 2.5 gives the result. So from now on assume that this is not the case. In what follows we will prove a slightly stronger inequality in the remaining cases, namely $d(G) \leq 2 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$.

Applying suitable bijections $\Gamma \mapsto [k]$ and $\Delta_j \mapsto [m]$ for every $j \in [k]$ we can identify Ω with $[m] \times [k] = \{(i, j) \,|\, 1 \leq i \leq m,\ 1 \leq j \leq k\}$ such that

$$N \leq \{(\sigma_1, \ldots, \sigma_k) \,|\, \sigma_i \in \mathrm{Sym}([m]), \sigma_a = \sigma_b \text{ if } \lceil a/t \rceil = \lceil b/t \rceil\},$$
$$\mathrm{soc}(N) = \{(\sigma_1, \ldots, \sigma_k) \mid \sigma_i \in \mathrm{Alt}([m]), \sigma_a = \sigma_b \text{ if } \lceil a/t \rceil = \lceil b/t \rceil\},$$

and the action of any $n = (\sigma_1, \ldots, \sigma_k) \in N$ on $[m] \times [k]$ is given as $n(i, j) = (\sigma_j(i), j)$. Under this identification, $\Delta_j = \{(i, j) \,|\, i \in [m]\}$ for every $j \in [k]$.

Let $h \in H_j$ for some $j = ut + v \in [k]$ where $v \in [t]$. Since $\mathrm{soc}(N) \lhd G$, and the set $\{\Delta_{ut+1}, \ldots, \Delta_{ut+t}\}$ corresponds to a diagonal subgroup of $\mathrm{soc}(N)$, we get that $\{\Delta_{ut+1}, \ldots, \Delta_{ut+t}\}$ is a block of imprimitivity for the action of G on Γ. Since H_j is by definition the stabiliser of Δ_j for some $ut + 1 \leq j \leq ut + t$, it follows that $h \in H_j$ fixes the set

$$\Omega_u = \Delta_{ut+1} \cup \Delta_{ut+2} \cup \ldots \cup \Delta_{ut+t}$$

setwise. Moreover, since the restriction of $\mathrm{soc}(N)$ to Ω_u acts on each of $\Delta_{ut+1}, \ldots, \Delta_{ut+t}$ in the same way, and the action of h on Ω_u must normalize this, we get that h acts on Ω_u coordinatewise i.e. there exist $\sigma_h \in \mathrm{Sym}([m])$, $\pi_h \in \mathrm{Sym}([t])$ such that

$$h(i, ut + w) = (\sigma_h(i), ut + \pi_h(w)) \text{ for every } i \in [m],\ w \in [t].$$

First let us assume that $t \geq m$.

We define a 2-coloring χ of $\Omega = [m] \times [k]$ as

$$\chi(i, j) = \begin{cases} 1 & \text{if } \ i \leq j \,(\mathrm{mod}\ t) \leq m \\ 0 & \text{if } \ i > j \,(\mathrm{mod}\ t) \text{ or } j \,(\mathrm{mod}\ t) > m \end{cases}.$$

That is, each Ω_u is colored in the same way; only the first w elements of Δ_{ut+w} are colored with 1, unless $w > m$ when no element of Δ_{ut+w} is colored with 1. (Notice that if j is a multiple of t then here $j \,(\mathrm{mod}\ t)$ means t (not 0).)

Now, let $h \in H_j$ for some $j = ut + v,\ v = j \,(\mathrm{mod}\ t)$ preserving χ. If the action of h on Ω_u is given by $(\sigma_h, \pi_h) \in \mathrm{Sym}([m]) \times \mathrm{Sym}([t])$, then σ_h must fix each set $[w],\ w \in [m]$, i.e. $\sigma_h = \mathrm{id}_{[m]}$. It follows that $h \in H_j$ acts trivially on Δ_j. So, Lemma 2.3 can be applied to the stabilizer of χ in G to get a $\lceil \sqrt[m]{d(K)} \rceil$-coloring λ of Ω such that only the identity element of G preserves both χ and λ. Finally, as in the last paragraph of the previous lemma, the pair (χ, λ) can be encoded with the $2\lceil \sqrt[m]{d(K)} \rceil$-coloring $\mu(x) := 2 \cdot \lambda(x) + \chi(x)$.

Now, let $t < m$. First we define a 2-coloring χ of $\Omega = [m] \times [k]$ in a similar way as for the previous case:

$$\chi(i,j) = \begin{cases} 1 & \text{if } \; i \leq j \,(\text{mod } t) \\ 0 & \text{if } \; i > j \,(\text{mod } t) \end{cases}.$$

If $h \in H_j$ for some $j = ut + v,\ v \equiv j \,(\text{mod } t)$ preserving χ, then $h \in \cap_{w=1}^{t} H_{ut+w}$ must hold. Moreover, the action of h on each Δ_{ut+w} must be the same.

Second, we can define a $\lceil \sqrt[t]{m} \rceil$-coloring $\beta_u : \Omega_u \mapsto \{0, \ldots, \lceil \sqrt[t]{m} \rceil - 1\}$ for every u such that if $h \in H_{ut+v}$ fixes both χ and β_u, then it acts trivially on Ω_u. This construction is analogous to the construction of λ given in the proof of Lemma 2.3. In fact, one can use Lemma 2.3 directly by observing that $\{\Lambda_i = \{(i, ut+w) \,|\, w \in [t]\}\}_i$ is a system of blocks of imprimitivity of the stabilizer T_j of χ in H_j and the setwise stabilizer of each Λ_i in T_j acts trivially on Λ_i. Let $\beta : \Omega \mapsto \{0, \ldots, \lceil \sqrt[t]{m} \rceil - 1\}$ be the union of the β_u. Thus, we get that Lemma 2.3 can be applied for the intersections of the stabilizers of χ and β. Thus, there is a $\lceil \sqrt[m]{d(K)} \rceil$-coloring $\lambda : \Omega \mapsto \left\{0, \ldots, \lceil \sqrt[m]{d(K)} \rceil - 1\right\}$ such that only the identity element of G fixes all of the colorings χ, β, λ. Finally, we can encode the triple (χ, β, λ) with the $2 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$-coloring μ of Ω given as $\mu(x) := 2 \cdot \lceil \sqrt[t]{m} \rceil \lambda(x) + 2 \cdot \beta(x) + \chi(x)$. □

A permutation group $G \leq \text{Sym}(\Omega)$ is called quasi-primitive if every non-trivial normal subgroup of G is transitive on Ω. Clearly, every primitive permutation group is quasi-primitive.

Lemma 2.7. *If $G \leq \text{Sym}(\Omega)$ is a (finite) quasi-primitive permutation group, then $d(G) \leq 4$ or $\text{Alt}(\Omega) \leq G \leq \text{Sym}(\Omega)$.*

Proof. Let us prove the lemma by induction on $n = |\Omega|$. If G is a primitive permutation group, then the claim follows by Seress [40, Theorem 2] and Dolfi [17, Lemma 1]. Suppose that G is not primitive but quasi-primitive. Let Γ be a system of blocks for G with $k = |\Gamma| < n$ maximal. Let $K \cong G$ be the action of G on Γ. Since a distinguishing partition of Γ for K gives rise naturally to a distinguishing partition of Ω for G, we have $d_\Omega(G) \leq d_\Gamma(K)$. By induction, $d(G) \leq d(K) \leq 4$ or $\text{Alt}(\Gamma) \leq K \leq \text{Sym}(\Gamma)$. Thus we may assume that $\text{Alt}(k) \leq G \leq \text{Sym}(k)$ with $k \geq 5$. Each element of Γ is a block of size at least $k-1$. For each i with $0 \leq i \leq k-1$ color i letters in block $i+1$ with 1 and the rest 0. This way we colored the elements of Ω with 2 colors in such a way that the stabilizer in G of this coloring is trivial. Thus $d(G) \leq 2$. □

A permutation group is defined to be innately transitive if there is a minimal normal subgroup of the group which is transitive. Such groups were introduced and studied by Bamberg and Praeger [6]. A quasi-primitive permutation group is innately transitive. The next theorem is a generalization of Lemma 2.7. It considers a class of groups which contains the class of innately transitive groups.

Theorem 2.8. *Let $M \lhd G \leq \text{Sym}(\Omega)$ be transitive permutation groups where Ω is finite and M is a direct product of isomorphic simple groups. Then $d(G) \leq 12$ or $\text{Alt}(\Omega) \leq G \leq \text{Sym}(\Omega)$.*

Proof. We prove the claim using induction on $n = |\Omega|$. By Lemma 2.7 we may assume that G is not a quasi-primitive permutation group.

As before, let $\Gamma = \{\Delta_1, \ldots, \Delta_k\}$ be a system of imprimitivity consisting of minimal blocks, each of size m, for the action of G. Let the kernel of the action of G on Γ be N and set $K = G/N$, a subgroup of $\mathrm{Sym}(\Gamma)$.

We claim that we may assume that $N \neq 1$. Suppose $N = 1$. By the induction hypothesis, $d(G) = d_\Omega(G) \leq d_\Gamma(K) \leq 12$, or $G \cong \mathrm{Alt}(\Gamma)$ or $G \cong \mathrm{Sym}(\Gamma)$ with $k \geq 13$. In the latter case G is quasi-primitive, since $M = \mathrm{soc}(G)$ is transitive. The claim follows.

We claim that we may assume that the action of H_1 on Δ_1 is large. For assume that the action of H_1 on Δ_1 is not large. By the induction hypothesis, we know that $d(K) \leq 12$ or K is an alternating or symmetric group of degree at least 13 in its natural action on Γ. In the previous case the bound $d(G) \leq 12$ follows via Lemma 2.4 (for $m \geq 3$) and Remark 2.5 (for $m = 2$). Suppose that the latter case holds. If $m \geq k-1$, then Lemma 2.4 gives $d(G) \leq 8$. Suppose that $m < k - 1$. Consider the image $\overline{M}$ of M under the natural homomorphism from G to $K = G/N$. Since $M \lhd G$ acts transitively on Γ, the group $\overline{M}$ is a non-trivial normal subgroup of K. Thus $\overline{M} \cong \mathrm{Alt}(k)$ or $\overline{M} \cong \mathrm{Sym}(k)$ with $k \geq 13$. Since $\overline{M}$ is a quotient group of M and M is a direct product of isomorphic simple groups, M must be a direct product of copies of $\mathrm{Alt}(k)$. Since $m < k - 1$, the stabilizer of Δ_1 in M acts trivially on Δ_1, and this contradicts the transitivity of M.

Since the action of H_1 on Δ_1 is non-empty (that is, $N \neq 1$) and large, $R = \mathrm{soc}(N)$ is isomorphic to a direct product of, say r copies of $\mathrm{Alt}(m)$ where $m \geq 5$ (see [38, p. 328, Lemma]). Furthermore, since G acts transitively on Γ, the normal subgroup R of G is in fact a minimal normal subgroup of G.

We claim that $R \leq M$. Suppose otherwise. Then $R \cap M = 1$ implies that R is contained in the centralizer C of M in $\mathrm{Sym}(\Omega)$. Since M is transitive, C must be semiregular. However R is not semiregular. Thus $R \leq M$.

In fact, $R < M$ since M is transitive on Γ and R is not. Furthermore, since R, and thus M, is a direct product of copies of $\mathrm{Alt}(m)$, we must have $k \geq m$. By the fact that M acts transitively on Γ, it also follows that M acts transitively on the set of r direct factors of R. But every subnormal subgroup of M is also normal in M, which forces $r = 1$ and so the linking factor of N (and also of R) is k.

By Lemma 2.6, $d(G) \leq 3 \cdot \lceil \sqrt[k]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil = 6 \cdot \lceil \sqrt[m]{d(K)} \rceil$. By the induction hypothesis, $d(K) \leq 12$ (in which case $d(G) \leq 12$ by the previous inequality) or K is an alternating or a symmetric group of degree $k \geq 13$. But in the latter case $m = k$ (and $d(K) \leq m$). Thus $\lceil \sqrt[m]{d(K)} \rceil = 2$ and so $d(G) \leq 12$ by Lemma 2.6. □

Proof of Theorem 1.2. First suppose that $G \leq \mathrm{Sym}(\Omega)$ is a quasi-primitive permutation group. By Lemma 2.7, we may assume that $n = |\Omega| \geq 48$ and $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$. In this case we have $d(G) \leq n < 48 \sqrt[n]{n!/2}$ where the second inequality follows from the fact that $\frac{1}{2}(n/3)^n < n!/2$. Thus we may assume that $G \leq \mathrm{Sym}(\Omega)$ is not a quasi-primitive permutation group.

Let M be a minimal normal subgroup in G which does not act transitively on Ω. Let an orbit of M on Ω be Σ, and let Γ be the set of orbits of M on Ω. Let the size of Γ be k and let H be the stabilizer in G of Σ. As before, denote the distinguishing number of H acting on Σ by $d_\Sigma(H)$. Since $M \lhd H$, Theorem 2.8 implies that $d_\Sigma(H) \leq 12$ or $\mathrm{Alt}(\Sigma) \leq H/C_H(\Sigma) \leq \mathrm{Sym}(\Sigma)$.

Case 1. $d_\Sigma(H) \leq 12$.

By Remark 2.5, $d(G) \leq 12 \left\lceil \sqrt[m]{d(K)} \right\rceil$ where K is the action of G on Γ and $m = |\Sigma|$. Since K is a transitive group on k points, by induction we have $d(K) \leq 48 \sqrt[k]{|K|}$. If $m \geq 6$, then

$$d(G) \leq 12 \left\lceil \sqrt[m]{d(K)} \right\rceil \leq 12 \left\lceil \sqrt[m]{48 \sqrt[k]{|K|}} \right\rceil \leq 24 \sqrt[m]{48 \sqrt[k]{|K|}} \leq 48 \sqrt[n]{|K|} \leq 48 \sqrt[n]{|G|}.$$

If $m \leq 5$ then we can use the previous estimate with 12 replaced by m and 24 replaced by $2m$.

Case 2. $\mathrm{Alt}(\Sigma) \leq H/C_H(\Sigma) \leq \mathrm{Sym}(\Sigma)$ with $|\Sigma| = m \geq 13$.

In this case the action of H on Σ is large. Let the kernel of the action of G on Γ be N and let t be the linking factor of N. Since $M \leq N$, we know that $N \neq 1$. Set $\epsilon = 1$ if $t = 1$ and $\epsilon = 2$ if $t \neq 1$. Then Lemma 2.6 implies that

$$d(G) \leq 3\lceil \sqrt[t]{m} \rceil \lceil \sqrt[m]{d(K)} \rceil \leq 6\epsilon \sqrt[t]{m} \sqrt[m]{d(K)} = 6\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)}.$$

Set $c = 6 \cdot 2^{1/mt} \cdot 3^{1/t}$. By use of the inequality $\frac{1}{2}(m/3)^m < m!/2 = |\mathrm{Alt}(m)|$, we have that $d(G)$ is at most

$$6\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)} < 6\epsilon \sqrt[mk]{((m!/2) \cdot 2 \cdot 3^m)^{k/t}} \sqrt[m]{d(K)} \leq c \cdot \epsilon \sqrt[n]{(|\mathrm{Alt}(m)|)^{k/t}} \sqrt[m]{d(K)}.$$

As noted in (Eq. 1), we have that $\mathrm{Alt}(m)^{k/t} \leq N$. This gives the inequality $d(G) < c \cdot \epsilon \sqrt[n]{|N|} \sqrt[m]{d(K)}$. By the induction hypothesis, we have $d(K) \leq 48 \sqrt[k]{|K|}$. Thus

$$d(G) < c \cdot \epsilon \sqrt[m]{48} \sqrt[n]{|N|} \sqrt[n]{|K|} \leq 6 \cdot \epsilon \cdot 2^{1/13t} 3^{1/t} \sqrt[13]{48} \sqrt[n]{|G|} < 48 \sqrt[n]{|G|}.$$

□

3. The affine case

3.1. **Some reductions and notation.** We begin our study of Theorem 1.1 in the case of affine primitive permutation groups.

Let G be an affine primitive permutation group acting on a finite set Ω. Then G contains a unique minimal normal subgroup V acting regularly on Ω, so $|\Omega| = p^d$ for some prime p and it can be identified with the finite vector space V over $\mathbb{F}_p$ of dimension d. Furthermore, $G = V \rtimes H$ for some $H \leq GL(V)$ and H acts faithfully and irreducibly on the vector space V. Clearly, $b(G) = b_V(G) = b_V(H) + 1$.

In this section we will show that there exists a universal constant $c > 0$ such that for the affine primitive permutation group $G = V \rtimes H$, we have

$$b_V(H) \leq 45(\log |H|/\log |V|) + c.$$

The following theorem shows that we may assume that H acts imprimitively (and irreducibly) on V.

Theorem 3.1 (Liebeck, Shalev [31], [34]). *There exists a universal constant $c > 0$ such that if H acts primitively on V, then $b_V(H) \leq \max\{18(\log |H|/\log |V|) + 30\ ,\ c\}$.*

Thus we may assume that V is an imprimitive irreducible $\mathbb{F}_pH$-module. Let $V = \oplus_{i=1}^t V_i$ be a decomposition of V into a sum of subspaces V_i of V that is preserved by the action of H. For every i with $1 \leq i \leq t$, let $H_i = N_H(V_i)$ and let $K_i = H_i/C_{H_i}(V_i) \leq GL(V_i)$ be the image of the restriction of H_i to V_i. The group H acts transitively on the set $\Pi = \{V_1, \ldots, V_t\}$. Let N be the kernel of this action and let P be the image of H in $\mathrm{Sym}(\Pi)$. So $N = \cap_{i=1}^t H_i$ and $P = H/N$.

As an easy application of the results of Section 2, we first prove Theorem 1.1 in the case when each $b_{V_i}(K_i)$ is bounded (see Theorem 3.4). Note that because the action of P on Π is transitive, it is enough to assume this only for K_1. First we handle the even more special case when K_1 is trivial.

Lemma 3.2. *If $K_1 = 1$, then $b_V(H) = \lceil \log_{|V_1|} d_\Pi(P) \rceil$.*

Proof. First note that the condition $K_1 = 1$ implies that every orbit of H in $\cup_{i=1}^t V_i$ contains exactly one element from every subspace V_i, which defines a one-to-one correspondence $\alpha_{ij} : V_i \mapsto V_j$ between any pair of subspaces V_i and V_j.

Let b be a positive integer. Let $w_s = v_s^{(1)} + v_s^{(2)} + \ldots + v_s^{(t)}$ be vectors in V for $1 \leq s \leq b$ decomposed with respect to the direct sum decomposition $V = \oplus_i V_i$. We define an equivalence relation on Π by $V_i \sim V_j$ if and only if $(v_1^{(i)}, \ldots, v_b^{(i)})$ corresponds to $(v_1^{(j)}, \ldots, v_b^{(j)})$, i.e. $\alpha_{ij}(v_s^{(i)}) = v_s^{(j)}$ for every $1 \leq s \leq b$. Then the set $\{w_1, \ldots, w_b\}$ is a base for H on V if and only if $\sim$ defines a distinguishing partition for P on Π. The number of different vectors of the form $(v_1^{(i)}, \ldots, v_b^{(i)})$ with entries from V_i (for any i) is $|V_1|^b$. It follows that $b_V(H)$ is the smallest integer such that $|V_1|^{b_V(H)}$ is at least $d_\Pi(P)$. $\square$

Remark 3.3. Note that this proof also works if P is not transitive on Π but $K_i = 1$ for every i with $1 \leq i \leq t$.

Theorem 3.4. *Let us assume that $b_{V_1}(K_1) \leq b$ for some constant b. Then we have*

$$b_V(H) \leq b + 1 + \log 48 + \frac{\log |P|}{\log |V|}.$$

Proof. By our assumption, for each $1 \leq i \leq t$ we can choose a base $\{v_1^{(i)}, v_2^{(i)}, \ldots, v_b^{(i)}\} \subset V_i$ for $K_i \simeq H_i/C_{H_i}(V_i)$. Put $w_s = \sum_{i=1}^t v_s^{(i)}$ for every $1 \leq s \leq b$ and let $L = \cap_s C_H(w_s)$. Then

$L \cap H_i = C_L(V_i)$ for every i so we can apply Lemma 3.2 for L (see also Remark 3.3). Hence $b_V(H) \leq b + \lceil \log_{|V_1|} d_\Pi(P) \rceil$. Since $d_\Pi(P) \leq 48\sqrt[t]{|P|}$ by Theorem 1.2, we get

$$b_V(H) \leq b + 1 + \log_{|V_1|}(48\sqrt[t]{|P|}) \leq b + 1 + \log 48 + \frac{\log |P|}{t \log |V_1|} = b + 1 + \log 48 + \frac{\log |P|}{\log |V|},$$

as claimed. □

Note that Theorem 3.4 proves Theorem 1.1 in case $b + 1 + \log 48$ is bounded. In other words, we must now look at situations when $b_{V_1}(K_1)$ is not bounded by any fixed constant.

For the remainder of this section, it will be more convenient for us to use the language of group representations. So, instead of choosing H as a fixed linear subgroup of $GL(V)$, let H be a fixed abstract group and $X : H \to GL(V)$ a representation of H. Then we would like to give an upper bound for $b_V(X(H))$. (The reason for this is that in the proof, we will reduce this problem to some other representations of H with simpler image structure.) Moreover, in order to use a theorem of Liebeck and Shalev [34, Theorem 1], we may also need to extend the base field to consider vector spaces over $\mathbb{F}_q$ for some p-power q. (Of course, the base size $b_V(X(H))$ is independent on whether we view V as an $\mathbb{F}_p$-space or as an $\mathbb{F}_q$-space.) Occasionally, we want to view the vector space V over $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$, which we will emphasize by the notation $V(p)$.

By using our previous notation, we assume that $V = \oplus_{i=1}^t V_i$ is a direct sum of $\mathbb{F}_q$-spaces and $X : H \to GL(V)$ is a representation such that $X(H)$ permutes the set $\Pi = \{V_1, \ldots, V_t\}$ in a transitive way. Thus, the representation X is equivalent to the induced representation $\mathrm{Ind}_{H_1}^H(X_1)$, where $X_1 : H_1 \to GL(V_1)$ is a linear representation of H_1.

In Sections 3.2 and 3.3 we first consider two special cases, which we will respectively call alternating-induced and classical-induced classes. Here alternating-induced means that K_1 is isomorphic to an alternating or symmetric group, and V_1 as an $\mathbb{F}_q K_1$-module is the deleted permutation module for K_1. Similarly, classical-induced means that K_1 is a classical group (maybe over some subfield $\mathbb{F}_{q_0} \leq \mathbb{F}_q$) with its natural action on V_1. Then we show in Section 3.4 how the general case can be reduced to one of these modules.

In fact, in order to be able to use a reduction argument in Section 3.4, we need to work with the following natural generalization of projective representations.

Definition 3.5. Let V be a finite vector space over $\mathbb{F}_q$ and $T \leq GL(V)$ any subgroup. We say that a map $X : H \to GL(V)$ is a $\pmod T$-representation of H if the following two properties hold:

(1) $X(g)$ normalizes T for every $g \in H$;
(2) $X(gh)T = X(g)X(h)T$ for every $g, h \in H$.

Definition 3.6. Let $T \leq GL(V)$ and $X_1, X_2 : H \to GL(V)$ be two $\pmod T$-representations of H. We say that X_1 and X_2 are $\pmod T$-equivalent if there is an $f \in N_{GL(V)}(T)$ such that $X_1(g)T = fX_2(g)f^{-1}T$ for all $g \in G$.

For a $\pmod T$-representation $X : H \to GL(V)$, we define the corresponding base size of H as

$$b_X(H) := b_V(X(H)T) \qquad \text{(Eq. 2)}$$

(note that $X(H)T$ is a subgroup of $GL(V)$). It is easy to see that equivalent $\pmod T$-representations have the same base size. Note that $b_V(H) \leq b_X(H)$ in case $H \leq GL(V)$ and $X = \mathrm{id}$.

For $T = 1$ a $\pmod T$-representation is the same as a linear representation.

In this paragraph let $T = Z(GL(V)) \simeq \mathbb{F}_q^\times$ be the group of all scalar transformations on V. Then a $\pmod T$-representation of H is the same as a projective representation of H. Furthermore, in this case T-equivalence of two T-representations of H means exactly that they are projectively equivalent. Slightly more generally, if $X : H \to GL(V(p))$ is any map satisfying (1) of Definition 3.5 (still with the assumption that V is an $\mathbb{F}_q$-space and $T \simeq \mathbb{F}_q^\times$), then $X(h)$ acts on T by a field automorphism $\sigma(h) \in \mathrm{Aut}(\mathbb{F}_q)$ for any $h \in H$, so $X(H)$ is contained in the semilinear group $\Gamma L(V) = GL(V) \rtimes \mathrm{Aut}(\mathbb{F}_q)$. In the following, we will also call such a $\pmod T$-representation $X : H \to \Gamma L(V(p))$ a projective representation. Furthermore, for any projective representation $X : H \to \Gamma L(V)$, we will denote by $\mathfrak{X}$ the associated homomorphism $H \to P\Gamma L(V)$ (which we again call a projective representation).

For the remainder, we consider the special case where $V = \oplus_{i=1}^t V_i$ is a direct sum of $\mathbb{F}_q$-spaces, and

$$T_V = \{g \in GL(V) \,|\, g(V_i) = V_i \text{ and } g|_{V_i} \in Z(GL(V_i)) \ \ \forall 1 \leq i \leq t\} \simeq (\mathbb{F}_q^\times)^t. \qquad \text{(Eq. 3)}$$

If a direct sum decomposition of a vector space U is given, then T_U will always denote the appropriate subgroup defined by the above displayed formula.

If $q > 2$ and $X : H \to GL(V)$ is an arbitrary map, then X satisfies (1) of Definition 3.5 (with $T = T_V$) if and only if the direct sum decomposition $V = \oplus_{i=1}^t V_i$ is preserved by $X(H)$. In particular, if X happens to be a linear representation of H preserving the direct sum decomposition $V = \oplus_{i=1}^t V_i$, then X is also a $\pmod{T_V}$-representation of H.

A further observation is that if $X : H \to GL(V(p))$ is a $\pmod{T_V}$-representation, then the restricted map $X_i : H_i \to GL(V_i)$ is a projective representation of H_i. (Here X_i is defined so that first we take the restriction of X to H_i, then we restrict the action of $X(H_i)$ to V_i.) Conversely, if $X_1 : H_1 \to \Gamma L(V_1)$ is any projective representation, then the induced representation $X = \mathrm{Ind}_{H_1}^H(X_1) : H \to GL(V(p))$ will be a $\pmod{T_V}$-representation of H transitively permuting the V_i, and it is easy to see that every $\pmod{T_V}$-representation of H transitively permuting the V_i can be obtained in this way. Here the induced representation $X = \mathrm{Ind}_{H_1}^H(X_1)$ can be defined with the help of a transversal in H to H_1, so it is not uniquely defined. However, it is uniquely defined up to $\pmod{T_V}$-equivalence, so this will not be a problem for us.

So, for the remainder, we assume that the groups $H_1 \leq H$ are fixed, and we consider representations of the form $X = \mathrm{Ind}_{H_1}^H(X_1)$, where $X_1 : H_1 \to \Gamma L(V_1)$ is a projective representation of H_1.

3.2. **Alternating-induced representations.** In this subsection we will only consider linear representations $X : H \to GL(V)$ and $X_i : H_i \to GL(V_i)$ such that $X = \mathrm{Ind}_{H_i}^{H}(X_i)$ for all i. We also assume that for all i with $1 \leq i \leq t$, the groups $K_i = X_i(H_i) \leq GL(V_i)$ are isomorphic to some alternating or symmetric group of degree k at least 7, and K_i acts on V_i such that V_i as an $\mathbb{F}_q K_i$-module (q is a power of p) is isomorphic to the non-trivial irreducible component of the permutation module obtained from the natural permutation action of K_i on a fixed basis of a vector space of dimension k over $\mathbb{F}_q$. In this situation we say that $V \simeq \mathrm{Ind}_{H_1}^{H}(V_1)$ is an alternating-induced $\mathbb{F}_q H$-module, and $X : H \to GL(V)$ is an alternating-induced representation.

In the following proposition we describe the construction of the module V_i.

Proposition 3.7. *Let $K \simeq \mathrm{Alt}(k)$ or $\mathrm{Sym}(k)$ and consider its action on an $\mathbb{F}_q$ vector space U of dimension $k \geq 5$, defined by permuting the elements of a fixed basis $\{e_1, \ldots, e_k\}$ of U. Let us define the subspaces*

$$U_0 = \Big\{ \sum_i \alpha_i e_i \,|\, \alpha_i \in \mathbb{F}_q,\ \sum_i \alpha_i = 0 \Big\} \qquad \textit{and} \qquad W = \Big\{ \alpha(\sum_i e_i) \,|\, \alpha \in \mathbb{F}_q \Big\}.$$

1. *If $p \nmid k$, then $U = U_0 \oplus W$, W is isomorphic to the trivial $\mathbb{F}_q K$-module and U_0 is the unique non-trivial irreducible component of the $\mathbb{F}_q K$-module U.*
2. *If $p \mid k$, then $U \geq U_0 \geq W$, both U/U_0 and W are isomorphic to the trivial $\mathbb{F}_q K$-module and U_0/W is the unique non-trivial irreducible component of the $\mathbb{F}_q K$-module U.*

Proof. This is well known (see [28, Page 185], for example). □

We can apply Proposition 3.7 to each pair K_i, V_i to define $\mathbb{F}_q K_i$-modules U_i and their submodules $U_{i,0}$, $W_i \leq U_i$ such that either $V_i \simeq U_{i,0}$ (for $p \nmid k$) or $V_i \simeq U_{i,0}/W_i$ (for $p \mid k$). Then the original action of H on V may be defined using the action of H on $U := \oplus_i U_i$. Moreover, if we choose a basis $\{e_1^{(i)}, \ldots, e_k^{(i)}\} \subset U_i$ for every i as in Proposition 3.7 in a suitable way, then $\{e_j^{(i)} \,|\, 1 \leq i \leq t,\ 1 \leq j \leq k\}$ will be a basis of U such that H acts on U by permuting the elements of this basis.

The next lemma says that $b_V(H)$ is bounded by a linear function of $b_U(H)$.

Lemma 3.8. *With the above notation $b_V(H) \leq 2b_U(H) + 3$ for $k \geq 7$.*

Proof. First, we define three vectors $w_1, w_2, w_3 \in U_{1,0} \oplus U_{2,0} \oplus \ldots \oplus U_{t,0}$ as linear combinations of the basis vectors $\{e_j^{(i)} \,|\, 1 \leq i \leq t,\ 1 \leq j \leq k\}$ as follows.

$$w_1 = \sum_{i=1}^{t} (e_1^{(i)} - e_2^{(i)}),\ w_2 = \sum_{i=1}^{t} (e_2^{(i)} - e_3^{(i)}),\ w_3 = \sum_{i=1}^{t} (e_3^{(i)} - e_4^{(i)}).$$

Let $L = C_H(w_1, w_2, w_3)$, so $\{e_j^{(i)} \,|\, 1 \leq i \leq t\}$ are L-invariant subsets for $1 \leq j \leq 4$.

Let $\{u_1, \ldots, u_b\} \subset U$ be a base for H of size $b = b_U(H)$. Now, for any $u \in \{u_1, \ldots, u_b\}$ we define two further vectors $u^e, u^f \in U_{1,0} \oplus U_{2,0} \oplus \ldots \oplus U_{t,0}$ as follows. Write $u = \sum_{i,j} a_{ij} e_j^{(i)}$ and define

$$u^e = \sum_i \sum_{j>2} a_{ij} e_j^{(i)} + \sum_i \beta_i e_1^{(i)}, \text{ for } \beta_i = -\sum_{j>2} a_{ij},$$
$$u^f = \sum_i \sum_{j\le 2} a_{ij} e_j^{(i)} + \sum_i \gamma_i e_3^{(i)}, \text{ for } \gamma_i = -(a_{i1} + a_{i2}).$$

The above definition of the β_i and γ_i ensures that the projection of u^e and u^f to any U_i is really in $U_{i,0}$. Furthermore, if $l \in L$ fixes u^e, then because of the above mentioned L-invariant subsets of basis vectors we get that l must fix both $\sum_i \beta_i e_1^{(i)}$ and $\sum_i \sum_{j>2} a_{ij} e_j^{(i)}$. Similarly, if $l \in L$ fixes u^f then it must fix both $\sum_i \gamma_i e_3^{(i)}$ and $\sum_i \sum_{j\le 2} a_{ij} e_j^{(i)}$. As a consequence every element of $C_L(u^e, u^f)$ must also fix $\sum_i \sum_{j>2} a_{ij} e_j^{(i)} + \sum_i \sum_{j\le 2} a_{ij} e_j^{(i)} = u$. Applying this construction to $u_1, \ldots, u_b$ we get that

$$\{w_1, w_2, w_3, u_1^e, u_1^f, u_2^e, u_2^f, \ldots, u_b^e, u_b^f\}$$

is a base of size $2b + 3$ for H acting on $U_{1,0} \oplus \ldots \oplus U_{t,0}$.

If $p \nmid k$, then there is nothing more to do, since in this case $V \simeq U_{1,0} \oplus \ldots \oplus U_{t,0}$ as $\mathbb{F}_q H$-modules.

For the remainder, let $p \mid k$ and $W = W_1 \oplus \ldots \oplus W_t$ where W_i is the 1-dimensional submodule of $U_{i,0}$ for all i with $1 \le i \le t$. For any $x \in U$, let $\bar{x} = x + W \in U/W$ be the associated element in the factor space. Now, we claim that

$$\{\bar{w}_1, \bar{w}_2, \bar{w}_3, \bar{u}_1^e, \bar{u}_1^f, \bar{u}_2^e, \bar{u}_2^f, \ldots, \bar{u}_b^e, \bar{u}_b^f\}$$

is a base for H acting on $(\oplus_i U_{i,0})/W \simeq V$.

Let $z_i = \sum_j e_j^{(i)}$ for every $1 \le i \le t$, so $\{z_1, \ldots, z_t\}$ is a basis for W. An element $g \in H$ fixes $\bar{w}_s$ (where $s \in \{1, 2, 3\}$) if and only if there are field elements $\lambda_1, \ldots, \lambda_t$ such that $g(w_s) = w_s + \sum_i \lambda_i z_i$. But g permutes the basis vectors in $\{e_j^{(i)} \mid 1 \le i \le t,\ 1 \le j \le k\}$ and also the subspaces $\{U_{i,0} \mid 1 \le i \le t\}$. A consequence of this is that the projection of $g(w_s)$ to any $U_{i,0}$ must be a non-zero linear combination of exactly two basis vectors from $\{e_j^{(i)} \mid 1 \le j \le k\}$. Since $k \ge 7$, this can happen only if $\lambda_i = 0$ for every $1 \le i \le t$, i.e. when g fixes w_s. So $C_H(\bar{w}_s) = C_H(w_s)$ for every s with $1 \le s \le 3$. The same argument can be applied to prove that $C_H(\bar{u}_s^f) = C_H(u_s^f)$ for every $1 \le s \le b$.

Finally, let us assume that $g \in C_H(\bar{w}_1, \bar{w}_2, \bar{w}_3) = L$ and $g(\bar{u}_s^e) = \bar{u}_s^e$ for some $1 \le s \le b$. Again this means that $g(u_s^e) = u_s^e + \sum_i \lambda_i z_i$ for some field elements $\lambda_1, \ldots, \lambda_t$. But the linear combination we used to define u_s^e contains no $e_2^{(i)}$ with non-zero coefficient. In other words u_s^e is contained in the L-invariant subspace generated by $\{e_j^{(i)} \mid j \ne 2,\ 1 \le i \le t\}$, so this must also hold for $g(u_s^e) = u_s^e + \sum_i \lambda_i z_i$, which implies that $\lambda_i = 0$ for every i, i.e.

$C_L(\bar{u}_s^e) = C_L(u_s^e)$ holds. We proved that

$$C_H(\bar{w}_1, \bar{w}_2, \bar{w}_3, \bar{u}_1^e, \bar{u}_1^f, \ldots, \bar{u}_b^e, \bar{u}_b^f) = C_H(w_1, w_2, w_3, u_1^e, u_1^f, \ldots, u_b^e, u_b^f) = 1,$$

as claimed. □

We can now establish Theorem 1.1 for alternating-induced groups.

Theorem 3.9. *If $H \leq GL(V)$ is an alternating-induced linear group, then*

$$b_V(H) \leq 17 + 2\frac{\log |H|}{\log |V|}.$$

Proof. By definition, $k \geq 7$. By using the same notation as above let H act on U by permuting the basis $B = \{e_j^{(i)} \,|\, 1 \leq i \leq t,\ 1 \leq j \leq k\}$. This action is clearly transitive, so we can use Theorem 1.2 to conclude that we can color the basis vectors by using at most $48\sqrt[kt]{|H|}$ colors such that only the identity of H fixes this coloring, i.e. $d_B(H) \leq 48\sqrt[kt]{|H|}$. Now any vector $u \in U$ can be seen as a coloring of this basis by using at most $|\mathbb{F}_q| = q$ colors. By Lemma 2.1, it follows that

$$b_U(H) \leq \lceil \log_q(d_B(H)) \rceil \leq \lceil \log_q(48\sqrt[kt]{|H|}) \rceil < 7 + \frac{\log |H|}{kt \log q} = 7 + \frac{\log |H|}{\log |U|}.$$

By Lemma 3.8, $b_V(H) \leq 2b_U(H) + 3 \leq 17 + 2(\log |H| / \log |V|)$, as claimed. □

3.3. **Classical-induced representations without multiplicities.** In this subsection let q be a power of the prime p, $V = \oplus_{i=1}^t V_i$ be a direct sum of $\mathbb{F}_q$ vector spaces, and define T_V as in (Eq. 3). Let k denote the $\mathbb{F}_q$-dimension of each V_i. Throughout this subsection we will assume that $k \geq 9$ holds. We also use the notation H_i, Π, N defined in Section 3.1.

Let $X : H \to GL(V(p))$ be a $\pmod{T_V}$-representation of H such that $X(H)T_V$ acts on $\Pi = \{V_1, \ldots, V_t\}$ in a transitive way. By our discussion at the end of Section 3.1, this means that $X = \mathrm{Ind}_{H_i}^H(X_i)$, where $X_i : H_i \to \Gamma L(V_i)$ is a projective representation of H_i for every $1 \leq i \leq t$. Then there is an associated homomorphism $\mathfrak{X} : H \to N_{GL(V(p))}(T_V)/T_V$ defined by $\mathfrak{X}(h) := X(h)T_V/T_V$. For the remainder of this subsection let $L = \mathfrak{X}(H)$ be the image of this homomorphism. Note that the action of H on Π induces an action of L on Π.

In this subsection we additionally assume that X is classical-induced, i.e. for each i, the image K_i of the homomorphism $\mathfrak{X}_i : H_i \to P\Gamma L(V_i)$ is some classical group i.e. $S_i = \mathrm{soc}(K_i) \leq P\Gamma L(V_i)$ is isomorphic to some simple classical group S over some subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. Because of our assumption $k \geq 9$, the group generated by all inner, diagonal and field automorphisms of S (for the remainder, we denote this group by $\mathrm{IDF}(S)$) has index at most 2 in $\mathrm{Aut}(S)$.

We introduce some further notation. For an H-block $\Delta \subseteq \Pi$ let $V_\Delta := \oplus_{V_i \in \Delta} V_i$, and $X_\Delta : N_H(\Delta) \to GL(V_\Delta(p))$ be the $\pmod{T_{V_\Delta}}$-representation of $N_H(\Delta)$ defined by taking the restriction of $X(h)$ to V_Δ for all $h \in N_H(\Delta)$. In particular, $X_\Pi = X$ and $X_{\{V_i\}} = X_i$ holds for each $V_i \in \Pi$. Furthermore, let the associated homomorphism $\mathfrak{X}_\Delta$ be $\mathfrak{X}_\Delta(h) := X_\Delta(h)T_{V_\Delta}/T_{V_\Delta}$. Define $L_\Delta = \mathfrak{X}_\Delta(N_H(\Delta))$ and $S_\Delta := \mathrm{soc}(\mathfrak{X}_\Delta(C_H(\Delta))) \lhd L_\Delta$.

If $\mathfrak{X}_\Delta(C_H(\Delta)) = 1$, then we set $S_\Delta = 1$. Finally, let $\widetilde{S_\Delta} \le N_H(\Delta)$ be the inverse image of S_Δ under the function $\mathfrak{X}_\Delta$. Then $\mathfrak{X}_i$ is defined on $\widetilde{S_\Delta}$ for each $V_i \in \Delta$ and it induces a homomorphism on S_Δ, which we also denote by $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$.

We next introduce a condition which we will additionally assume in this subsection.

Definition 3.10 (Multiplicity-free condition)**.** If $\Delta \subseteq \Pi$ is an H-block such that $S_\Delta \simeq S$ and all $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$ for $V_i \in \Delta$ are projectively equivalent, then $|\Delta| = 1$.

A consequence of this assumption is the following.

Proposition 3.11. *Suppose X is classically-induced and let $\Delta \subseteq \Pi$ be an H-block such that $S_\Delta \simeq S$. If the multiplicity-free condition holds, then $|\Delta| \le 2$.*

Proof. First note that if $\Delta' \subset \Delta$ is any H-block, then the assumption $S_\Delta \simeq S$ implies that $S_{\Delta'} \simeq S$. For simpler notation, we can assume that $\Delta = \{V_1, \dots, V_d\}$ for $d = |\Delta|$. By assumption, S_Δ is a diagonal subgroup of $S_1 \times \dots \times S_d \simeq S^d$. So, S_Δ can be identified with $\{(s, s^{z_2}, \dots, s^{z_d}) \,|\, s \in S\}$, where $z_2, \dots, z_d \in \mathrm{Aut}(S)$ are fixed elements. Now, if $z_i^{-1} z_j \in \mathrm{IDF}(S)$, then $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$ and $\mathfrak{X}_j : S_\Delta \to P\Gamma L(V_j)$ are projectively equivalent. The relation $V_i \sim V_j \iff z_i^{-1} z_j \in \mathrm{IDF}(S)$ defines an $N_H(\Delta)$-congruence on Δ. Using that $|\mathrm{Aut}(S) : \mathrm{IDF}(S)| \le 2$ and the first sentence of the proof, we get that there is an H-block $\Delta' \subset \Delta$ such that $|\Delta'| \ge |\Delta|/2$, $S_{\Delta'} \simeq S$ and all $\mathfrak{X}_i : S_{\Delta'} \to P\Gamma L(V_i)$ for $V_i \in \Delta'$ are projectively equivalent. Thus, the result follows from the multiplicity-free condition. □

For the rest of this subsection let $\Delta \subseteq \Pi$ be an H-block. The group S_Δ is either trivial or is a subdirect product of isomorphic simple classical groups. As for subdirect products of alternating groups in Section 2, this means that S_Δ is a direct product of diagonal subgroups corresponding to a partition $\Delta = \cup_i \Delta_i$ of Δ into equal-size parts. Again, we call the size of the parts of this partition the linking factor of S_Δ. Note that the Δ_i themselves are H-blocks and $S_{\Delta_i} \simeq S$ for each i. Hence, by Proposition 3.11, the linking factor of S_Δ is at most 2. As before, let $N = C_H(\Pi)$ be the kernel of the action of H on Π.

Recall the definitions of X_1 and K_1 from the second and third paragraphs of Section 3.3. The base size $b_{X_1}(K_1)$ is defined as in (Eq. 2). With this notation the following result is a consequence of Theorem 3.1.

Theorem 3.12. *With the above assumptions, there exists a universal constant $c > 0$ such that $b_{X_1}(K_1) \le 18(\log |K_1|)/(\log |V_1|) + c$.*

We can now prove Theorem 1.1 for such classical-induced representations which have the multiplicity-free condition.

Theorem 3.13. *There exists a universal constant $c > 0$ such that if $X : H \to GL(V)$ is a $(\mathrm{mod}\ T_V)$-representation of H (with respect to some direct sum decomposition $V = \oplus_{i=1}^t V_i$), which is a classical-induced representation possessing the multiplicity-free condition, then $b_X(H) \le 45(\log |H|)/(\log |V|) + c$.*

Proof. Assume that $\mathfrak{X}(N) \neq 1$. Then $\mathrm{soc}(\mathfrak{X}(N)) = S_\Pi$ for the H-block Π, so $\mathrm{soc}(\mathfrak{X}(N))$ is a subdirect product of the simple classical groups S_i with linking factor at most 2. Thus $|N| \geq |S_1|^{t/2} \geq |K_1|^{2t/5}$ (see [23, Page 18]). Therefore, by applying Theorem 3.12, we deduce that

$$b_{X_1}(H_1) = b_{X_1}(K_1) \leq 45(\log|N|)/(\log|V|) + c.$$

A slightly modified version of Theorem 3.4 gives $b_X(H) \leq 45(\log|H|)/(\log|V|) + c$ for another universal constant $c > 0$.

From now on assume that $\mathfrak{X}(N) = 1$. This means that $L = \mathfrak{X}(H)$ acts faithfully on Π. Let M be a normal subgroup of H strictly containing $\ker(\mathfrak{X})$ such that $\mathfrak{X}(M)$ is a minimal normal subgroup of L and let Δ be an orbit of M on Π. Furthermore, let $M_\Delta := \mathfrak{X}_\Delta(M) \lhd L_\Delta$. Notice that $\Delta \subseteq \Pi$ is an H-block of size at least 2 and M_Δ is a direct product of isomorphic simple groups.

Assume first that $S_\Delta \neq 1$. Then S_Δ is a subdirect product of the isomorphic (non-abelian) simple classical groups from the set $\{S_i \mid V_i \in \Delta\}$.

If M_Δ centralizes S_Δ, then all $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$ for $i \in \Delta$ are projectively equivalent since M is transitive on Δ. This contradicts our multiplicity-free assumption. So we assume that M_Δ does not centralize S_Δ. Since both M_Δ and S_Δ are normal subgroups in L_Δ, this implies that $M_\Delta \cap S_\Delta \neq 1$. In particular M_Δ and $M_\Delta \cap S_\Delta$ are isomorphic to some powers of the (non-abelian) simple classical group S. Since M_Δ is transitive on Δ, we have that $|\Delta| \geq 5$ and S_Δ cannot contain a nontrivial, proper M_Δ-invariant normal subgroup. But $M_\Delta \cap S_\Delta \neq 1$ is normal in both M_Δ and S_Δ, so $S_\Delta \leq M_\Delta$. Since any subnormal subgroup of M_Δ is normal in M_Δ, we get that S_Δ is simple, so $S_\Delta \simeq S$ has linking factor $|\Delta| \geq 5$, which is in contradiction with the discussion following the proof of Proposition 3.11.

It remains to handle the case where $S_\Delta = 1$. Then L_Δ and M_Δ act faithfully and transitively on Δ and M_Δ is a normal subgroup of L_Δ isomorphic to a direct product of isomorphic simple groups. By Theorem 2.8, $d_\Delta(L_\Delta) \leq 12$ or $\mathrm{Alt}(\Delta) \leq L_\Delta \leq \mathrm{Sym}(\Delta)$.

If $d_\Delta(L_\Delta) \leq 12$, then $b_{P(\Delta)}(L_\Delta) \leq 4$, by Lemma 2.1, and so $b_{V_\Delta}(L_\Delta) \leq 4$ (any subset of Δ can be represented by a vector in V_Δ whose projection to $V_i \in \Delta$ is non-zero if and only if V_i is an element of the subset). Thus, $b_{X_\Delta}(N_H(\Delta)) \leq b_{V_\Delta}(L_\Delta) + b_{V_\Delta}(T_{V_\Delta}) \leq 5$. Applying Theorem 3.4 for V_Δ instead of V_1 we get

$$b_X(H) \leq b_{X_\Delta}(N_H(\Delta)) + 1 + \log 48 + \frac{\log|P|}{\log|V|} \leq \frac{\log|H|}{\log|V|} + 12.$$

Finally, if $d_\Delta(L_\Delta) > 12$, then $m := |\Delta| \geq 13$ and $\mathrm{Alt}(\Delta) \leq L_\Delta \leq \mathrm{Sym}(\Delta)$. In this case for any $V_i \in \Delta$, we have that $\mathfrak{X}_\Delta(H_i) \cong \mathrm{Alt}([m-1])$ or $\mathfrak{X}_\Delta(H_i) \cong \mathrm{Sym}([m-1])$ must hold. But S_i is a composition factor of $\mathfrak{X}_\Delta(H_i)$ and it is a simple classical group. A contradiction. □

3.4. **Eliminating small tensor product factors from the K_i.** Let us continue to use the notation of this section.

The purpose of this subsection is to reduce the affine case of Theorem 1.1 to the case when each K_i acts on V_i either as a "big" classical group (possibly over a field extension $\mathbb{F}_q$ of $\mathbb{F}_p$) or as an alternating or symmetric group on the non-trivial irreducible component of its natural permutation module. More precisely, we will reduce the affine case of Theorem 1.1 to the case where the action of H is alternating-induced or multiplicity-free classical-induced. Since these types were dealt with in the previous two subsections, this reduction will complete the proof of Theorem 1.1 in the affine case.

Lemma 3.14. *Let L be a finite group and W be a faithful, finite-dimensional L-module. For a positive integer l let V be the direct sum of l copies of the L-module W. Then $b_V(L) = \lceil b_W(L)/l \rceil$.*

Proof. Let $b' := b_W(L)$ and $\{x_1, x_2, \ldots, x_{b'}\} \subset W$ be a minimal base for L with respect to its action on Λ. Set $b := \lceil b'/l \rceil$. Let us define the vectors

$$y_1 = (x_1, x_2, \ldots, x_l),\ y_2 = (x_{l+1}, x_{l+2}, \ldots, x_{2l}), \ldots, y_b = (x_{(b-1)l+1}, \ldots, x_{b'}, 0, \ldots, 0) \in V.$$

It is easy to see that $\{y_1, \ldots, y_b\} \subset V$ is a minimal base for L on V. □

We now consider the case where the projective representation $X_1 : H_1 \to \Gamma L(V_1)$ preserves a proper tensor product decomposition $V_1 = U_1 \otimes W_1$ over $\mathbb{F}_q$ where U_1 and W_1 are $\mathbb{F}_q$ vector spaces and $2 \leq l := \dim_{\mathbb{F}_q}(U_1) \leq \dim_{\mathbb{F}_q}(W_1)$. Using that H transitively permutes the subspaces $V_1, \ldots, V_t$, it follows that each $X_i : H_i \to \Gamma L(V_i)$ preserves a corresponding tensor product decomposition $V_i = U_i \otimes W_i$.

By taking the composition of X_i with the projection map to W_i, one can define new projective representations $Y_i : H_i \to \Gamma L(W_i)$. Let $Y : H \to GL(W(p))$ be the induced representation $Y = \mathrm{Ind}_{H_1}^H(Y_1)$, where W can be identified with $W_1 \oplus \ldots \oplus W_t$. The key to our reduction argument is the following lemma, which gives an upper bound for $b_X(H)$ in terms of $b_Y(H)$.

Lemma 3.15. *With the above notation we have $b_X(H) \leq \lceil b_Y(H)/l \rceil + 4$.*

Proof. By using a construction of Liebeck and Shalev (see the proof of [31, Lemma 3.3]), for each $1 \leq i \leq t$ there exist three vectors $v_1^{(i)}, v_2^{(i)}, v_3^{(i)} \in V_i$ such that

$$C_{GL(U_i)\otimes GL(W_i)}(v_1^{(i)}, v_2^{(i)}, v_3^{(i)}) \leq \mathrm{id}_{U_i} \otimes GL(W_i).$$

Additionally, let $v_4^{(i)} = \alpha v_1^{(i)}$ for each $1 \leq i \leq t$, where α is some generator of $\mathbb{F}_q^\times$. Define $v_j = \sum_{i=1}^t v_j^{(i)}$ for $j = 1, 2, 3$ and let $L := C_H(v_1, v_2, v_3)$. The choice of $v_1^{(i)}$ and $v_4^{(i)}$ guarantees that $X_i(L) \subset GL(U_i) \otimes GL(W_i)$ for each i, so $X_i(L) \subset \mathrm{id}_{U_i} \otimes GL(W_i)$ by the displayed formula above. It follows that the restriction map $X_i : L \cap H_i \to \Gamma L(V_i)$ is projectively equivalent to an $l = \dim_{\mathbb{F}_q} U_i$ multiple of $Y_i : L \cap H_i \to \Gamma L(W_i)$.

Let $\Delta_1, \ldots, \Delta_s \subset \Pi$ be the orbits of L on Π, $V_{\Delta_j} = \oplus_{V_i \in \Delta_j} V_i$ and $W_{\Delta_j} = \oplus_{V_i \in \Delta_j} W_i$ for every $1 \leq j \leq s$. Then each V_{Δ_j} is $X(L)$-invariant which means that $X = \oplus_{j=1}^s X_{\Delta_j}$ on L, where the $\pmod{T_{V_{\Delta_j}}}$-representation $X_{\Delta_j} : L \to GL(V_{\Delta_j}(p))$ is defined by taking the restriction of $X(L)$ to V_{Δ_j}. One can similarly define the $\pmod{T_{W_{\Delta_j}}}$-representations $Y_{\Delta_j} : L \to GL(W_{\Delta_j}(p))$ and establish the decomposition $Y = \oplus_{j=1}^{s} Y_{\Delta_j}$ on L. This means that if $V_a \in \Delta_j$ is arbitrary, then $X_{\Delta_j} = \mathrm{Ind}_{L\cap H_a}^{L}(X_a)$ and $Y_{\Delta_j} = \mathrm{Ind}_{L\cap H_a}^{L}(Y_a)$. Since X_a on L is projectively equivalent to the l multiple of Y_a on L, and induction of representations preserves multiplicity, we get that X_{Δ_j} is $\pmod{T_{V_{\Delta_j}}}$-equivalent to the l multiple of Y_{Δ_j} on L for every $1 \le j \le s$. So, $X = \oplus_{j=1}^{s} X_{\Delta_j}$ is $\pmod{T_V}$-equivalent to the l multiple of Y on L. By using Lemma 3.14, we get that $b_X(L) = \lceil b_Y(L)/l \rceil$. Since $b_X(H) \le b_X(L) + 4$ and $b_Y(L) \le b_Y(H)$ hold trivially, the result follows. □

Corollary 3.16. *With the above notation, if* $b_Y(H) \le c_1 \cdot \frac{\log|H|}{\log|W|} + c_2$ *for some constants* c_1 *and* $c_2 \ge 10$*, then* $b_X(H) \le c_1 \cdot \frac{\log|H|}{\log|V|} + c_2$.

Proof. By Lemma 3.15 and by assumption,

$$b_X(H) \le \left\lceil \frac{b_Y(H)}{l} \right\rceil + 4 \le c_1 \frac{\log|H|}{l \log|W|} + \frac{c_2}{l} + 5 \le c_1 \frac{\log|H|}{\log|V|} + c_2.$$

□

From now on we will assume that $K_1 \le GL(V_1) \simeq GL(k,p)$ is a primitive irreducible linear group with unbounded base size. We may make this assumption by Theorem 3.4.

Primitive groups of unbounded base size were characterized in [31, Theorem 2] and in [34, Theorem 1, Proposition 2]. In the following we collect some of their properties in a form which will be most convenient for us. Note that in [31, 34] the authors state their theorem in terms of a tensor product of several linear groups, but for our purpose it is better to "pack" together all but the one with the largest dimension.

First we fix some further notation, mostly borrowed from [22]. Let $U = U_k(p)$ be a vector space of dimension k over $\mathbb{F}_p$. Let $H \le GL(U_k(p))$ be a primitive linear group. Let $q = p^f$ be the largest power of p such that one can extend scalar multiplication on U to be an $\mathbb{F}_q$-vector space $U = U_{k/f}(q)$ such that $H \le \Gamma L(U_{k/f}(q)) \le GL(U_k(p))$.

If $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$, then $\mathrm{Cl}(r, q_0) \le GL(r,q)$ denotes a classical linear group over $\mathbb{F}_{q_0}$ for some subfield $\mathbb{F}_{q_0} \le \mathbb{F}_q$ and for some $r \ge 9$. (This lower bound on r is assumed because we want to apply the result of Section 3.3.)

Theorem 3.17 (Liebeck, Shalev [31], [34])**.** *Let* $H \le GL(U_k(p))$ *be a primitive linear group of unbounded base size and* $q = p^f$ *be maximal such that* $H \le \Gamma L(U_{k/f}(q))$*. Then there is a tensor product decomposition* $U = U_1 \otimes U_2$ *over* $\mathbb{F}_q$ *such that* $1 \le \dim(U_1) < \dim(U_2)$ *and* H *preserves this tensor product decomposition, that is,* $H \le N_{\Gamma L(U_{k/f}(q))}(GL(U_1) \otimes GL(U_2))$*. Let* $H^0 = GL(U_{k/f}(q)) \cap H$ *and let* H_2^0 *be the image of the projection of* H^0 *to* $GL(U_2)$*, that is,* $H_2^0 := \{b \in GL(U_2) \,|\, \exists a \in GL(U_1) : \ a \otimes b \in H^0\}$*. Then one of the following holds.*

(1) $H_2^0 \simeq \mathrm{Sym}(m) \times \mathbb{F}_q^\times$ *or* $\mathrm{Alt}(m) \times \mathbb{F}_q^\times$ *for some* m *such that* U_2 *is the unique non-trivial irreducible component of the natural* m*-dimensional permutation representation of* $\mathrm{Sym}(m)$*. In that case* $\dim_{\mathbb{F}_q}(U_2) = m - 1$ *unless* $p \mid m$*, when* $\dim_{\mathbb{F}_q}(U_2) = m - 2$.

(2) *H_2^0 is a classical group* $\mathrm{Cl}(r, q_0) \leq GL(r, q)$ *over some subfield* $\mathbb{F}_{q_0} \leq \mathbb{F}_q$*, where* $r = \dim_{\mathbb{F}_q}(U_2)$.

Proof. This follows by combining parts of [34, Theorem 1] and [34, Proposition 2]. □

Note that there is a similar characterization of primitive linear groups of large orders due to Jaikin-Zapirain and Pyber [27, Proposition 5.7].

In the following we will apply Theorem 3.17 to $K_i \leq GL(V_i)$ where $1 \leq i \leq t$. We can extend scalar multiplication on each V_i to become an $\mathbb{F}_q$-vector space for some $q = p^f$ to get a tensor product decomposition $V_i = V_{i,1} \otimes V_{i,2}$ satisfying the statements of Theorem 3.17. In this way, $V = V_s(q)$ becomes a vector space over $\mathbb{F}_q$ (where $sf = \dim_{\mathbb{F}_p}(V)$) and $X : H \to GL(V(p))$ is a $\pmod{T_V}$-representation of H with $T_V \simeq \mathbb{F}_q^\times$.

We are now in a position to complete the proof of Theorem 1.1 for affine groups. In fact, we prove the following more general statement for $\pmod{T_V}$-representations. To recover the original statement, take an irreducible imprimitive linear group $H \leq GL(V)$ with the identity.

Theorem 3.18. *There exists an absolute constant $c \geq 10$ such that if $X : H \to GL(V(p))$ is a $\pmod{T_V}$-representation of H (with respect to some direct sum decomposition $V = \oplus_{i=1}^t V_i$) induced from a primitive projective representation $X_1 : H_1 \to \Gamma L(V_1)$, then*

$$b_X(H) \leq 45 \frac{\log |H|}{\log |V|} + c.$$

Proof. By Theorem 3.1, we may assume that V is an imprimitive $X(H)T_V$-module, i.e. $t > 1$.

We proceed by induction on the dimension of V_1. Note that if $\dim V_1$ is bounded (or, more generally, if $b_{X_1}(H_1)$ is bounded), the theorem follows from Theorem 3.4.

By our assumption, $X_1(H_1)Z(GL(V_1)) \leq \Gamma L(V_1)$ is a primitive semilinear group, so Theorem 3.17 can be applied. Thus, an $\mathbb{F}_q$ vector space structure can be defined on each V_i (where $\mathbb{F}_q$ is a (maybe non-proper) field extension of the base field of V_i) such that there is a tensor product decomposition $V_i = U_i \otimes W_i$ over $\mathbb{F}_q$ preserved by $X_i(H_i)$. Furthermore, $l := \dim_{\mathbb{F}_q}(U_i) < \dim_{\mathbb{F}_q}(W_i)$.

First, let us assume that the tensor product decomposition $V_i = U_i \otimes W_i$ is proper, i.e. $l \geq 2$. Let $Y_i : H_i \to \Gamma L(W_i)$ be the projective representation and $Y : H \to GL(W(p))$ be the $\pmod{T_W}$-representation for $W = \oplus_{i=1}^t W_i$ defined in the paragraph before Lemma 3.15, so $Y = \mathrm{Ind}_{H_1}^H(Y_1)$. By induction, $b_Y(H) \leq 45 \frac{\log |H|}{\log |W|} + c$ for some constant $c \geq 10$, so the result follows by Corollary 3.16.

So we can assume that $l = 1$. We can also assume that $\dim_{\mathbb{F}_q} V_i \geq 9$ by the second paragraph of this proof.

If $X_1(H_1)Z(GL(V_1))$ satisfies part (1) of Theorem 3.17, then there is a (trivial) tensor product decomposition $V_1 = U_1 \otimes W_1$ with $\dim_{\mathbb{F}_q} U_1 = 1$ fixed by $X_1(H_1)$ and maps

$\lambda_1 : H_1 \to GL(U_1) \simeq \mathbb{F}_q^\times$ and $X_1' : H_1 \to GL(W_1)$ such that X_1' is a linear representation of H_1 and $X_1'(H_1) \simeq \mathrm{Sym}(m)$ or $\mathrm{Alt}(m)$. This means $X' = \mathrm{Ind}_{H_1}^H(X_1') : H \to GL(W)$ is an alternating-induced representation (where $W = \oplus_{i=1}^t W_i$), so $b_{X'}(H) \leq 2(\log|H|/\log|W|)+17$ by Theorem 3.9. Finally, $b_X(H) \leq b_{X'}(H) + 4$ by Lemma 3.15 and $|W| = |V|$, so $b_X(H) \leq 2(\log|H|/\log|V|) + 21$ and we are done.

For the remainder, we may assume that $X_1(H_1)Z(GL(V_1))$ satisfies part (2) of Theorem 3.17, in which case X is classical-induced. In order to use Theorem 3.13 in this case, we need to further reduce it to satisfy the multiplicity-free condition. (For a reminder of this condition and the notation used in the rest of the proof, see Definition 3.10 and the preceding discussion at the start of Section 3.3.) For this purpose let $\Delta \subseteq \Pi$ be a maximal H-block violating the multiplicity-free condition, i.e. $|\Delta| \geq 2$, $S_\Delta \simeq S$ and the representations $X_i : \widetilde{S_\Delta} \to \Gamma L(V_i)$ for $V_i \in \Delta$ are all projectively equivalent. To simplify the notation, we may assume that $\Delta = \{V_1, V_2, \dots, V_s\}$ with $s = |\Delta| > 1$ and $k = \dim V_1$. Let $X_\Delta : N_H(\Delta) \to GL(V_\Delta(p))$ be the (mod T_{V_Δ})-representation defined by the restriction of X (where T_{V_Δ} is defined by the decomposition $V_\Delta = \oplus_{V_i\in\Delta} V_i$). Then $X = \mathrm{Ind}_{N_H(\Delta)}^H(X_\Delta)$.

Let U_Δ be an s-dimensional vector space over $\mathbb{F}_q$ with fixed basis $f_1, \dots, f_s$ and let W_Δ be a k-dimensional vector space over $\mathbb{F}_q$ with fixed basis $e_1, \dots, e_k$. Furthermore, let $\{b_1, \dots, b_k\}$ be a basis of V_1. By assumption, for each $2 \leq i \leq s$ there are isomorphisms $\varphi_i : V_1 \to V_i$ and scalar maps $\lambda_i : \widetilde{S_\Delta} \to \mathbb{F}_q^\times$ such that $X_i(h) = \lambda_i(h)\varphi_i X_1(h)\varphi_i^{-1}$ for every $h \in \widetilde{S_\Delta}$. We also define $\varphi_1 := \mathrm{id}_{V_1}$ and $\lambda_1 : \widetilde{S_\Delta} \to \{1\}$. Now, $\{\varphi_i(b_j) \mid 1 \leq i \leq s,\ 1 \leq j \leq k\}$ is a basis of V_Δ. Let $\Phi : V_\Delta \to U_\Delta \otimes W_\Delta$ be the isomorphism defined by $\Phi(\varphi_i(b_j)) := f_i \otimes e_j$. By identifying V_Δ and $U_\Delta \otimes W_\Delta$ via Φ, we get that for any $h \in \widetilde{S_\Delta}$, the matrix form of $X_\Delta(h)$ with respect to the basis $\{f_1 \otimes e_1, f_1 \otimes e_2, \dots, f_s \otimes e_k\}$ is the Kronecker product of matrices $D(h) \otimes A(h)$ where $A(h)$ is the matrix form of $X_1(h)$ with respect to the basis $\{b_1, \dots, b_k\}$ while $D(h)$ is the diagonal matrix with entries $\lambda_1(h), \dots, \lambda_s(h)$ in its main diagonal. Since $X_\Delta(\widetilde{S_\Delta})$ is normalised by $X_\Delta(N_H(\Delta))$, we can apply [28, Lemma 4.4.3(ii)] to see that $X_\Delta(N_H(\Delta))$ is contained in the Kronecker product of a group of monomial matrices and a group of matrices isomorphic to some classical group.

This means that we have a tensor product decomposition $V_\Delta = U_\Delta \otimes W_\Delta$ preserved by $X_\Delta(N_H(\Delta))$. Taking the composition of X_Δ with the projections to the factors of this tensor product decomposition, we can define the maps $Y_\Delta : N_H(\Delta) \to GL(U_\Delta)$ and $Z_\Delta : N_H(\Delta) \to \Gamma L(W_\Delta)$ such that $Y_\Delta(N_H(\Delta))$ consists of monomial matrices, while $Z_\Delta(N_H(\Delta))$ is some classical group (modulo the group of scalar transformations). Then we can induce these representations to H to get the monomial representation (with transitive permutation part) $Y = \mathrm{Ind}_{N_H(\Delta)}^H(Y_\Delta)$ and classical-induced representation $Z = \mathrm{Ind}_{N_H(\Delta)}^H(Z_\Delta)$. Note that Z satisfies the multiplicity-free condition by the maximality of Δ. Furthermore, let $U := \oplus_i U_{\Delta_i}$, $W := \oplus_i W_{\Delta_i}$, where $\{\Delta = \Delta_1, \dots, \Delta_{t/|\Delta|}\}$ is the orbit of Δ under the action of H on the power set of Π. Thus, $Y : H \to GL(U(p))$ and $Z : H \to GL(W(p))$.

If $\dim U_{\Delta_1} \geq \dim W_{\Delta_1}$, then $b_Y(H) \leq \frac{\log|H|}{\log|U|} + 10$ by use of Theorem 3.4 with $b = 1$, so we get $b_X(H) \leq \frac{\log|H|}{\log|V|} + 10$ by Corollary 3.16.

Similarly, if $\dim U_{\Delta_1} \leq \dim W_{\Delta_1}$ then $Z : H \to GL(W(p))$ is multiplicity-free classical induced representation, so Theorem 3.13 can be applied to conclude that $b_Z(H) \leq 45\frac{\log|H|}{\log|W|}+c$ for a suitable constant $c \geq 10$. Using Corollary 3.16 again, we get that $b_X(H) \leq 45\frac{\log|H|}{\log|V|}+c$ holds, which completes our argument. □

4. Non-affine primitive permutation groups

Pyber's conjecture is known to be true for all non-affine primitive permutation groups. Since the explicit constants have not always been specified, we collect here the information needed to complete the proof of Pyber's conjecture with multiplicative constant 45.

Let G be a non-affine primitive permutation group acting on a finite set Ω of size n. The first result deals with almost simple groups.

Theorem 4.1 (Liebeck, Shalev [30]; Burness et al [10], [11], [12], [13]; Benbenishty [7]). *If G is an almost simple primitive permutation group of degree n, then $b(G) < 15(\log|G|/\log n)$.*

When G is a primitive group of diagonal type, an almost exact formula for $b(G)$ is determined by Fawcett [18] (her upper bound differs from $b(G)$ by at most 1 in every such case). Here we only need an upper bound.

Theorem 4.2 (Gluck, Seress, Shalev [21]; Fawcett [18]). *If G is a primitive permutation group of diagonal type and of degree n, then $b(G) < (\log|G|/\log n) + 3 < 4(\log|G|/\log n)$.*

It remains to establish Theorem 1.1 when G is a primitive permutation group of product type or of twisted wreath product type. For these types Pyber's conjecture has been proved by Burness and Seress [14].

By the proof of [14, Theorem 4.1] it is sufficient to prove that if G is of product type, then $b(G) < (45/2)(\log|G|/\log n)$.

Let Γ be a finite set and let $H \leq \mathrm{Sym}(\Gamma)$ be a primitive permutation group of almost simple type or of diagonal type. Let Ω be the direct product of k copies of Γ for some integer $k \geq 2$. For a transitive permutation group P of degree k, the group $H \wr P$ acts in product action on Ω in a natural way. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive permutation group contained in $H \wr P$. Assume that $\mathrm{soc}(G) = T^k$ where $T = \mathrm{soc}(H)$ and that the action of G on the set of the k direct factors of $\mathrm{soc}(G)$ is P. It remains to establish Pyber's conjecture with multiplicative constant 45 for such groups G.

If H is of almost simple type, then [14, Proposition 3.9] and its proof yield $b(G) < (45/2)(\log|G|/\log n)$. Thus we may assume that H is of diagonal type. In this case, by an argument different from the one in [14, Proposition 3.10], it is possible to obtain a bound with multiplicative constant less than 22. For the details, see [24, Section 4.3.2] by Liebeck and the second and third authors.

Acknowledgement

We thank Laci Pyber for drawing our attention to some of the references in this paper. We also thank the referee for the very thorough reading of our paper and the large number of comments.

References

[1] Albertson, M. O.; Collins, K. L. Symmetry breaking in graphs. *Electron. J. Combin.* **3** (1996), no. 1, RP #18.
[2] Babai, L. On the order of uniprimitive permutation groups. *Ann. of Math.* (2) **113** (1981), no. 3, 553–568.
[3] Babai, L. On the order of doubly transitive permutation groups. *Invent. Math.* **65** (1981/82), no. 3, 473–484.
[4] Babai, L.; Cameron, P. J.; Pálfy, P. P. On the orders of primitive groups with restricted nonabelian composition factors. *J. Algebra* **79** (1982), no. 1, 161–168.
[5] Bailey, R. F.; Cameron, P. J. Base size, metric dimension and other invariants of groups and graphs. *Bull. Lond. Math. Soc.* **43** (2011), no. 2, 209–242.
[6] Bamberg, J.; Praeger, C. E. Finite permutation groups with a transitive minimal normal subgroup. *Proc. London Math. Soc.* (3) **89** (2004), no. 1, 71–103.
[7] Benbenishty, C. On actions of primitive groups. Ph.D. thesis, Hebrew University, Jerusalem, 2005.
[8] Blaha, K. D. Minimum bases for permutation groups: the greedy approximation. *J. Algorithms* **13** (1992), no. 2, 297–306.
[9] Bochert, A. Über die Transitivitätsgrenze der Substitutionengruppen, welche die alternirende ihres Grades nicht enthalten. *Math. Ann.* **33** (1889), no. 4, 572–583.
[10] Burness, T. C. On base sizes for actions of finite classical groups. *J. Lond. Math. Soc.* (2) **75** (2007), no. 3, 545–562.
[11] Burness, T. C.; Guralnick, R. M.; Saxl, J. On base sizes for symmetric groups. *Bull. Lond. Math. Soc.* **43** (2011), no. 2, 386–391.
[12] Burness, T. C.; Liebeck, M. W.; Shalev, A. Base sizes for simple groups and a conjecture of Cameron. *Proc. Lond. Math. Soc.* (3) **98** (2009), no. 1, 116–162.
[13] Burness, T. C.; O'Brien, E. A.; Wilson, R. A. Base sizes for sporadic simple groups. *Israel J. Math.* **177** (2010), 307–333.
[14] Burness, T. C.; Seress, Á. On Pyber's base size conjecture. *Trans. Amer. Math. Soc.* **367** (2015), no. 8, 5633–5651.
[15] Cameron, P. J. Permutation groups. London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999.
[16] Cameron, P. J.; Kantor, W. M. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.* **2** (1993), no. 3, 257–262.
[17] Dolfi, S. Orbits of permutation groups on the power set. *Arch. Math.* **75** (2000), 321–327.
[18] Fawcett, J. B. The base size of a primitive diagonal group. *J. Algebra* **375** (2013), 302–321.
[19] Fawcett, J. B.; Praeger, C. E. Base sizes of imprimitive linear groups and orbits of general linear groups on spanning tuples. *Arch. Math. (Basel)* **106** (2016), no. 4, 305–314.
[20] Gluck, D.; Magaard, K. Base sizes and regular orbits for coprime affine permutation groups. *J. London Math. Soc.* (2) **58** (1998), 603–618.
[21] Gluck, D.; Seress, Á.; Shalev, A. Bases for primitive permutation groups and a conjecture of Babai. *J. Algebra* **199** (1998), no. 2, 367–378.
[22] Guidici, M.; Liebeck, M. W.; Praeger, C. E.; Saxl, J; Tiep, P. H. Arithmetic results on orbits of linear groups. *Trans. Amer. Math. Soc.* **368** (2016), 2415–2467.
[23] Guralnick, R. M.; Maróti, A.; Pyber, L. Normalizers of primitive permutation groups. *Adv. Math.* **310** (2017), 1017–1063.

[24] Halasi, Z.; Liebeck, M. W.; Maróti, A. Base sizes of primitive groups: bounds with explicit constants. arXiv:1802.06972.
[25] Halasi, Z.; Maróti, A. The minimal base size for a p-solvable linear group. *Proc. Amer. Math. Soc.* **144** (2016), 3231–3242.
[26] Halasi, Z.; Podoski, K. Every coprime linear group admits a base of size two. *Trans. Amer. Math. Soc.* **368** (2016), 5857–5887.
[27] Jaikin-Zapirain, A.; Pyber, L. Random generation of finite and profinite groups and group enumeration. *Ann. of Math.* (2) **173** (2011), no. 2, 769–814.
[28] Kleidman, P.; Liebeck, M. W. The subgroup structure of the finite classical groups, LMS Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.
[29] Liebeck, M. W. On minimal degrees and base sizes of primitive permutation groups. *Arch. Math. (Basel)* **43** (1984), no. 1, 11–15.
[30] Liebeck, M. W.; Shalev, A. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.* **12** (1999), no. 2, 497–520.
[31] Liebeck, M. W.; Shalev, A. Bases of primitive linear groups. *J. Algebra* **252** (2002), 95–113.
[32] Liebeck, M. W.; Shalev, A. Bases of primitive permutation groups. *Groups, combinatorics & geometry* (Durham, 2001), 147–154, World Sci. Publ., River Edge, NJ, 2003.
[33] Liebeck, M. W.; Shalev, A. Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc.* (3) **90** (2005), no. 1, 61–86.
[34] Liebeck, M. W.; Shalev, A. Bases of primitive linear groups II. *J. Algebra* **403** (2014), 223–228.
[35] Pyber, L. On the orders of doubly transitive permutation groups, elementary estimates. *J. Combin. Theory Ser. A* **62** (1993), no. 2, 361–366.
[36] Pyber, L. Asymptotic results for permutation groups, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 11 (ed. L. Finkelstein and W. M. Kantor) Amer. Math. Soc. Providence RI 1993, pp. 197–219.
[37] Robinson, G. R. On the base size and rank of a primitive permutation group. *J. Algebra* **187** (1997), no. 1, 320–321.
[38] Scott, L. L. Representations in characteristic p. The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), pp. 319–331, Proc. Sympos. Pure Math., 37, Amer. Math. Soc., Providence, R.I., 1980.
[39] Seress, Á. The minimal base size of primitive solvable permutation groups. *J. Lond. Math. Soc.* (2) **53** (1996), no. 2, 243–255.
[40] Seress, Á. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc.* **29** (1997), 697–704.
[41] Seress, Á. Permutation group algorithms. Cambridge Tracts in Mathematics, 152. Cambridge University Press, Cambridge, 2003.
[42] Sun, X.; Wilmes, J. Structure and automorphisms of primitive coherent configurations. arXiv:1510.02195.

Department of Mathematics, Central European University, Nádor utca 9., H-1051, Budapest, Hungary

E-mail address: duyan_hulya@phd.ceu.edu

Department of Algebra and Number Theory, Eötvös University, Pázmány Péter sétány 1/c, H-1117, Budapest, Hungary and Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: zhalasi@cs.elte.hu and halasi.zoltan@renyi.mta.hu

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

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