# Bounds of Some Invariants of Finite Permutation Groups

**Hülya Duyan**


Department of Mathematics and its Applications
Central European University
Budapest, Hungary

A dissertation presented for the degree of
Doctor of Philosophy in Mathematics

# Abstract

Let $\Omega$ be a non-empty set. A bijection of $\Omega$ onto itself is called a permutation of $\Omega$ and the set of all permutations forms a group under composition of mapping. This group is called the *symmetric group* on $\Omega$ and denoted by $\mathrm{Sym}(\Omega)$ (or $\mathrm{Sym}(n)$ or $S_n$ where $|\Omega| = n$). A *permutation group* on $\Omega$ is a subgroup of $\mathrm{Sym}(\Omega)$.

Until 1850's this was the definition of group. Although this definition and the axiomatic definition are the same, usually what we first learn is the axiomatic approach. The reason is to not to restrict the group elements to being permutations of some set $\Omega$.

Let $G$ be a permutation group. Let $\sim$ be a relation on $\Omega$ such that $\alpha \sim \beta$ if and only if there is a transformation $g \in G$ which maps $\alpha$ to $\beta$ where $\alpha, \beta \in \Omega$. $\sim$ is an equivalence relation on $\Omega$ and the equivalence classes of $\sim$ are the orbits of $G$. If there is one orbit then $G$ is called transitive.

Assume that $G$ is intransitive and $\Omega_1, \ldots, \Omega_t$ are the orbits of $G$ on $\Omega$. $G$ induces a transitive permutation group on each $\Omega_i$, say $G_i$ where $i \in \{1, \ldots, t\}$. $G_i$ are called the transitive constituents of $G$ and $G$ is a subcartesian product of its transitive constituents. So we can build any permutation group from transitive permutation groups.

A transitive permutation group $G$ acting on $\Omega$ is primitive if and only if there are no non-trivial $G$-invariant partitions of $\Omega$. So we can not break down the action into smaller ones. Hence, primitive permutation groups are the starting point for any investigation about permutation groups.

A base $\Sigma$ of $G$ is a non-empty subset of $\Omega$ with the property that only the identity element can fix every element in $\Sigma$. Bases have been studied since 1960's and have been very useful both theoretically (for an example see [3]) and computationally (see [65]). In Chapter 2 we give a detailed explanation of base, base size and Pyber's conjecture for the base size of primitive permutation groups.

In Chapter 3 we prove the conjecture for the affine type primitive groups, which was the last unfinished type.

In our proof, another invariant of permutation groups is used, namely the distinguishing number. The distinguishing number of $G$, denoted by $d(G)$ or $d_\Omega(G)$, is the minimal number of colors needed to color the elements of $\Omega$ in such a way that the stabilizer in $G$ of this coloring is trivial. Chapter 1 gives the background material about the distinguishing number and the distinguishing number of certain permutation groups, including the bound for transitive permutation groups.

The new results in Chapter 1 and Chapter 3 are from our joint work with Zoltán Halasi and Attila Maróti [24].

The last chapter is about the random bases for coprime primitive linear groups. We show that if $G \leq GL(V)$ is a coprime primitive linear group then the probability that a random 11-tuple in $V$ is a base for $G$ tends to 1 as $|V| \to \infty$. This result is from our joint paper with Zoltán Halasi and Károly Podoski [25].

# Acknowledgements

First of all, I would like to express my gratitude to my Ph.D. supervisor, Zoltán Halasi. I learned a lot from him. His vast knowledge in algebra was always at hand and he took his time to give clear explanations on complicated subjects. I had the opportunity to learn from him the process of thinking: how to attack a research question. His relentless passion for mathematics has been contagious and it helped me through the difficult periods. I am specially grateful to Attila Maróti, whose encouragement and professional support was indispensable during our collaboration.

I would also like to thank to Károly Böröczky, Head of the Department of Mathematics. Always relaxed, helpful and reassuring, ready to cope with anything that comes in the way at any time. Even being 4 months pregnant unable to work from sickness, with the deadline of the dissertation approaching quickly, with him in the background one felt safe. I am also grateful to Elvira Kadvány and Melinda Balázs, for their pro-activity, help and patience about any kind of practical or administration matters and their kindness, in general.

Finally, I would like to thank my family, who were helpful and supportive. My husband, Pali, with whom we went through the whole thing together and from whom I got plenty of encouragement, our cats, Sarıkız and Sezar who stayed always relaxed, my sister Özlem and my parents, who were always supportive and understanding.

# Contents

# Chapter 1

# The Distinguishing Number of a Transitive Permutation Group

## 1.1 Introduction

We use the term "distinguishing number" as Albertson and Collins [1] introduced for graphs in 1996. They defined the distinguishing number of a graph as the minimum number of colors needed to color the vertices of the graph in such a way that only the identity automorphism preserves the coloring.

Let $G$ be a permutation group acting on a finite set $\Omega$. The distinguishing number of $G$, denoted by $d(G)$ or $d_\Omega(G)$, is the minimal number of colors needed to color the elements of $\Omega$ in such a way that the stabilizer in $G$ of this coloring is trivial. If we collect the points with the same color in one set then we get a partition of $\Omega$ which is called a distinguishing partition.

First, I would like to give some elementary properties of the distinguishing number.

**Proposition 1.1.1.** A permutation group has distinguishing number 1 if and only if it is the trivial group.

**Proposition 1.1.2.** Let $G$ be a permutation group of degree $n$. Then $d(G) = n$ if and only if $G = \mathrm{Sym}(n)$ and $d(G) = n - 1$ if and only if $G = \mathrm{Alt}(n)$.

The action of $G$ on $\Omega$, where $n = |\Omega| > 1$, induces an action on the set of all colorings of $\Omega$ using $d(G)$ colors. This action contains a regular orbit and hence we have the following result.

**Proposition 1.1.3.** If $G$ is a permutation group of degree $n > 1$, then $\sqrt[n]{|G|} < d(G)$.

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 $\Omega$ such that the stabilizer of this coloring in $G$ is contained in $N$.

**Proposition 1.1.4.** For any $H \leq G$ and $N \lhd G$, we have $\max\{d(H), d(G/N)\} \leq d(G) \leq d(N)d(G/N)$.

**Proposition 1.1.5.** Let $G$ be a permutation group acting on a finite set $\Omega$. The following are equivalent:

(1) $G$ has distinguishing number 2;

(2) There is a subset of $\Omega$ whose setwise stabiliser in $G$ is the identity;

(3) $G$ has a regular orbit on the power set of $\Omega$.

Solvable permutation groups and primitive permutation groups which are different than the alternating and the symmetric group have small distinguishing numbers. Seress [63] proved that if $G$ is an arbitrary solvable permutation group, then there is a partition $P$ of $\Omega$ into at most five parts such that only the identity element of $G$ fixes $P$.

In [17] and [20], Cameron, Neumann and Saxl showed that if $G$ is primitive on $\Omega$ and $\mathrm{Alt}(n) \not\leq G$ then in all except finitely many cases $G$ has a regular orbit on the power set of $\Omega$ which means that $d(G) = 2$. Moreover, the probability that a uniform random subset has trivial setwise stabilizer tends to 1 as $n \to \infty$. In his paper which was published in 1997 [64], Seress gave the exact list of the 43 primitive permutation groups which are not alternating or symmetric group and have distinguishing number greater than 2. Three years later Dolfi [23] calculated the distinguishing numbers of these exceptional 43 groups. He proved that 38 of them have distinguishing number 3 and the rest have distinguishing number 4.

The distinguishing number of quasi-primitive groups different from alternating and symmetric groups is bounded by 4 (Lemma 1.2.6). Recently Devillers, Morgan and Harper [21] improved this result. They proved that the quasi-primitive groups that are not primitive have distinguishing number 2, and the semiprimitive groups that are not quasi-primitive have distinguishing number 2 except when the group is $GL(2,3)$ in its degree 8 action where $d(GL(2,3)) = 3$.

In the following section the main target is to investigate the distinguishing number of transitive permutation groups.

## 1.2 The Distinguishing Number of a Transitive Permutation Group

For a finite group $H$ acting on a set $X$ and for a subset $Y$ of $X$, the setwise and the pointwise stabilizers of $Y$ in $H$ are denoted by $N_H(Y)$ and $C_H(Y)$, respectively. If $Y = \{y_1, \ldots, y_s\}$ for $s \geq 1$ we use the notation $C_H(y_1, \ldots, y_s)$.

Let $G \leq \mathrm{Sym}(\Omega)$ and $\Gamma = \{\Delta_1, \ldots, \Delta_k\}$ be a partition of $\Omega$ permuted by $G$. Let $H_j = N_G(\Delta_j)$ for each $j$ and $N = \cap_{j=1}^{k} H_j$. Then each $H_j$ acts naturally on $\Delta_j$ with kernel $C_G(\Delta_j)$, hence $H_j/C_G(\Delta_j) \leq \mathrm{Sym}(\Delta_j)$. Furthermore, $G$ acts on $\Gamma$ with kernel $N$, so $K := G/N \leq \mathrm{Sym}(\Gamma)$.

The first goal of this section 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 $|\Delta_j|$.

In the lemma below, we do not assume the transitivity of $G$ on $\Gamma$, but we assume that $|\Delta_1| = |\Delta_2| = \ldots = |\Delta_k| = m$ for some $1 < m < |\Omega|$.

**Lemma 1.2.1.** *If $H_j$ acts trivially on $\Delta_j$ (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.* $H_j = C_G(\Delta_j)$ for every $1 \leq j \leq k$ means that each orbit of $G$ on $\Omega$ has at most one common point with the block $\Delta_j$ for every $j$. Thus we can define a function $f : \Omega \mapsto [m]$ where $[m] := \{1, \ldots, m\}$ such that the restriction of $f$ to $\Delta_j$ 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 $\lambda$ of $\Omega$ in the following way. Let us choose a $d(K)$-coloring $\alpha : \Gamma \mapsto \{0, 1, \ldots, d(K) - 1\}$ of $\Gamma$ such that only the identitiy of $K$ fixes $\alpha$. 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 $\lambda$. By assumption, $N = 1$, so it is enough to show that if $g \in G$ fixes $\lambda$ then it also fixes $\alpha$. Let $g \in G$ fix $\lambda$ and $\Delta_j \cdot g = \Delta_{j'}$ for some $j, j' \in [k]$. For $x \in \Delta_j$, $a_{f(x)}(j) = \lambda(x) = \lambda(x \cdot g) = a_{f(x \cdot g)}(j')$. Since $f$ is constant on every orbit of $G$, $a_{f(x)}(j) = a_{f(x)}(j')$ for every $x \in \Delta_j$. $f$ is a surjective map, hence $a_i(j) = a_i(j')$ for all $i \in [m]$. So $\alpha(\Delta_j)$ and $\alpha(\Delta_{j'})$ have the same base $c$-expansion, which means that $\Delta_j$ and $\Delta j'$ have the same color with respect to the $\alpha$-coloring. Therefore $g$ must be the identity element. □

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 $j \in [k]$).

**Lemma 1.2.2.** *Suppose that $d(H_1) \leq c$ for some constant $c$. Then $d(G) \leq c \cdot \lceil \sqrt[m]{d(K)} \rceil$.*

*Proof.* Since $d(H_1) \leq c$ for each $j$, there are colorings $\chi_j : \Delta_j \mapsto \{0, \ldots, c-1\}$, such that any element of $H_j$ fixing this coloring acts trivially on $\Delta_j$. Let $\chi : \Omega \mapsto \{0, \ldots, c-1\}$ be the union of these colorings, that is, $\chi(x) = \chi_j(x)$ for $x \in \Delta_j$. Then Lemma 1.2.1 can be applied to the stabilizer of $\chi$ in $G$, so there exist 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 of $G$ fixes both colorings $\lambda$ and $\chi$. Finally, we can encode the pair $(\chi, \lambda)$ by a $c \cdot \lceil \sqrt[m]{d(K)} \rceil$-coloring $\mu$ of $\Omega$ by choosing a suitable bijection function, e.g. let $\mu(x) = c \cdot \lambda(x) + \chi(x)$. □

Now let the action of $H_1$ on $\Delta_1$ be primitive. We say that the action of $H_1$ on $\Delta_1$ is large if $m = |\Delta_1| \geq 5$ and $\mathrm{Alt}(\Delta_1) \leq H_1/C_{H_1}(\Delta_1) \leq \mathrm{Sym}(\Delta_1)$. By the results of Seress [64, Theorem 2] and Dolfi [23, Lemma 1], if $H_1$ is not large, then $d(H_1) \leq 4$. With the lemma above we have the following result:

**Corollary 1.2.3.** *If $H_1$ is not large, then $d(G) \leq 4 \cdot \lceil \sqrt[m]{d(K)} \rceil$.*

Now assume that the action of $H_1$ is large and $N \neq 1$. We can still apply the lemma above, but with this method we get a large upper bound for $d(G)$. In the lemma following, a better bound is calculated. For that reason, we examine the structure of $N$.

Let $G_i$ be groups for $i \in I$ where $I$ is a non-empty set and $H$ be a subgroup of the direct product $\prod_{i \in I} G_i$. $H$ is called a subdirect product of $\prod_{i \in I} G_i$ if each projection $p_j : H \to G_j$ is surjective. It is called diagonal subgroup if all $p_j$'s are injective. If each $p_j$ is an isomorphism (which implies that all $G_j$ are isomorphic) then $H$ is called a full diagonal subgroup. Let $I = \{1, \ldots, k\}$ for some positive integer $k$ and $G_j \simeq G$ for all

$j \in I$. If $H$ is a full diagonal subgroup of $\prod_{i\in I} G_i$, then $H = \{(g, g^{z_2}, g^{z_3}, \dots g^{z_k}) | g \in G\}$ where $z_2, z_3, \dots, z_k \in \mathrm{Aut}(G)$ are fixed.

For the case where all $G_i$ are non-abelian simple groups, Scott [62] described the structure of $H$ as follows:

**Proposition 1.2.4.** If $H$ is a subdirect subgroup of a direct product $\prod_{i\in I} G_i$ of non-abelian simple groups, then it is the direct product of $\prod D_j$ where each $D_j$ is a full diagonal subgroup of the subproduct $\prod_{i\in I_j} G_i$ and $I_j$ form a partition of $I$.

If the action of $H_1$ is large, i.e. $\mathrm{Alt}(m) \leq H_1/C_{H_1}(\Delta_1)$ for $m \geq 5$, then the socle of $N$, denoted by $\mathrm{Soc}(N)$, is a subdirect product of alternating groups $\mathrm{Alt}(m)$. By the proposition above, 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 full diagonal subgroup of a subproduct $\prod_{\ell\in I_j} C_\ell$ where $C_\ell \cong \mathrm{Alt}(m)$. Since $G$ is transitive on $\Gamma$ and $\mathrm{Soc}(N) \lhd G$, the subsets $I_j$ form a partition of $\Gamma$ with parts of equal size. (Moreover, they form a system of blocks for the action of $G$ on $\Gamma$.) 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

$$\mathrm{Alt}(m)^{k/t} \leq N \leq \mathrm{Sym}(m)^{k/t}. \tag{1.1}$$

**Lemma 1.2.5.** *Let us assume that $H_1$ is large and $N \neq 1$ with linking factor $t$. Then $d(G) \leq 2 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$.*

*Proof.* By definition, $N$ fixes all the $\Delta_i$'s, so we can see any element $n$ of $N$ as $(\sigma_1, \dots, \sigma_k)$ where $\sigma_i \in \mathrm{Sym}(\Delta_i)$ for each $i \in [k]$. We order the blocks according to the full diagonal parts of the socle of $N$. Let $\{\Delta_{(u-1)t+1}, \dots, \Delta_{(u-1)t+t}\}$ be the set of the blocks corresponding to the $u$-th diagonal part according to our ordering. Denote the union of these blocks by $\Omega_u$. Let $D_u$ be the restriction of the $\mathrm{Soc}(N)$ to $\Omega_u$. Then

$$D_u = \mathrm{Soc}(N)|_{\Omega_u} = \{(\sigma^{z_1}, \sigma^{z_2}, \sigma^{z_3}, \dots, \sigma^{z_t}) | \sigma \in \mathrm{Alt}(m)\},$$

for some fixed $1 = z_1, z_2, \dots, z_t \in \mathrm{Aut}(\mathrm{Alt}(m))$.

If $m \neq 6$ then $\mathrm{Aut}(\mathrm{Alt}(m)) \simeq \mathrm{Sym}(m)$. However when $m = 6$, the automorphism group of $\mathrm{Alt}(6)$ is larger than $\mathrm{Sym}(6)$ where $|\mathrm{Aut}(\mathrm{Alt}(6)) : \mathrm{Sym}(6)| = 2$. Hence, if $m \neq 6$, any automorphism of $\mathrm{Alt}(m)$ is conjugation by an element of $\mathrm{Sym}(m)$. This does not change the cycle decomposition of the element.

First let us assume that $m \neq 6$. Then $z_i \in \mathrm{Sym}(m)$ for all $i \in [t]$. The action of $N$ on $\{\Delta_{(u-1)t+1}, \dots, \Delta_{(u-1)t+t}\}$ is either isomorphic to $\mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$ and moreover, the permutation actions of $N$ on $\Delta_{(u-1)t+1}, \dots, \Delta_{(u-1)t+t}$ are equivalent via the elements $z_2, \dots, z_t$. Then we can re-enumerate the elements of $\Delta_j$ for all $j \in \{(u-1)t+1, \dots, (u-1)t+t\}$ according to this equivalence. Therefore, we can apply suitable bijections $\{\Delta_{(u-1)t+1}, \dots, \Delta_{(u-1)t+t}\} \to [t]$ and $\Delta_j \to [m]$ for every $j \in \{(u-1)t+1, \dots, (u-1)t+t\}$ and identify $\Omega_u$ with $[m] \times [t] = \{(i, j) | 1 \leq i \leq m, 1 \leq j \leq t\}$ in such a way that we get

$$N|_{\Omega_u} \leq \{(\sigma, \dots, \sigma) \,|\, \sigma \in \mathrm{Sym}([m])\},$$
$$D_u = \mathrm{Soc}(N)|_{\Omega_u} = \{(\sigma, \dots, \sigma) \,|\, \sigma \in \mathrm{Alt}([m])\},$$

and the action of any $n \in N$ on $\Omega_u = [m] \times [t]$ is given as $(i,j) \cdot n = (i \cdot \sigma, j)$ for some $\sigma \in \mathrm{Sym}(m)$. Under this identification, $\Delta_j = \{(i,j) \mid i \in [m]\}$ for every $j \in \{(u-1)t+1, \ldots, (u-1)t+t\}$.

$\mathrm{Soc}(N)$ is a characteristic subgroup of $N$ and $N \lhd G$, so $\mathrm{Soc}(N) \lhd G$. $\Omega_u$ corresponds to a diagonal subgroup of $\mathrm{Soc}(N)$. Therefore, we get that $\Omega_u$ is a block of imprimitivity for the action of $G$ on $\Gamma$. Let $h \in H_j$ for some $j \in \{(u-1)t+1, \ldots, (u-1)t+t\}$. Since $H_j$ is by definition the stabiliser of $\Delta_j$, it follows that $h$ fixes $\Omega_u$ setwisely. Moreover, it permutes the $\Delta_i$'s for $(u-1)t+1 \leq i \leq (u-1)t+t$. Hence $h|_{\Omega_u} \in \mathrm{Sym}([m]) \wr \mathrm{Sym}([t])$ meaning that $h|_{\Omega_u} = (\sigma_{(h,1)}, \ldots, \sigma_{(h,t)}) \cdot \pi_h$ for some $\sigma_{(h,i)} \in \mathrm{Sym}([m])$ where $i \in [t]$ and $\pi_h \in \mathrm{Sym}([t])$. If $n \in \mathrm{Soc}(N)$ then $n|_{\Omega_u} = (\sigma, \ldots, \sigma)$ for some $\sigma \in \mathrm{Alt}([m])$. The action of $h$ on $\Omega_u$ must normalize $D_u$. So $n^h|_{\Omega_u} = (\sigma', \ldots, \sigma')$ for some $\sigma' \in \mathrm{Alt}([m])$. $(i,j) \cdot n = (i \cdot \sigma, j)$ and $(i,j) \cdot n^h = (i \cdot \sigma', j)$ for all $(i,j) \in \Omega_u$. This implies that $\sigma_{(h,1)} = \ldots = \sigma_{(h,t)}$. Hence there exists a $\sigma_h \in \mathrm{Sym}([m])$ such that $h|_{\Omega_u} = (\sigma_h, \ldots, \sigma_h) \cdot \pi_h$ and

$$(i, (u-1)t+w) \cdot h = (i \cdot \sigma_h, (u-1)t + w \cdot \pi_h)$$

for every $i \in [m]$ and $w \in [t]$.

First let us assume that $t \geq m$. We define a 2-coloring $\chi$ of $\Omega = [m] \times [k]$ as

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

| The coloring $\chi$ of $\Omega_u$ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $\Delta_{(u-1)t+1}$ | $\Delta_{(u-1)t+2}$ | $\Delta_{(u-1)t+3}$ | ..... | $\Delta_{(u-1)t+m-1}$ | $\Delta_{(u-1)t+m}$ | $\Delta_{(u-1)t+m+1}$ | ..... | $\Delta_{(u-1)t+t}$ |
| 1 | 1 | 1 | ..... | 1 | 1 | 0 | ..... | 0 |
| 0 | 1 | 1 | ..... | 1 | 1 | 0 | ..... | 0 |
| 0 | 0 | 1 | ..... | 1 | 1 | 0 | ..... | 0 |
| 0 | 0 | 0 | ..... | 1 | 1 | 0 | ..... | 0 |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| 0 | 0 | 0 | ..... | 1 | 1 | 0 | ..... | 0 |
| 0 | 0 | 0 | ..... | 0 | 1 | 0 | ..... | 0 |

That is, each $\Omega_u$ is colored in the same way; only the first $w$ elements of $\Delta_{(u-1)t+w}$ are colored with 1, if $w > m$ then no element of $\Delta_{(u-1)t+w}$ 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 $j = (u-1)t + v$, $v \equiv j \,(\mathrm{mod}\ t)$ preserving $\chi$. If the action of $h$ on $\Omega_u$ is given by $(\sigma_h, \pi_h) \in \mathrm{Sym}([m]) \times \mathrm{Sym}([t])$, then $\sigma_h$ 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 $\Delta_j$. So the elements of the stabilizer of this coloring are acting trivially on each $\Delta_i$ for $i \in [k]$ and we have a group as in the Lemma 1.2.1. We apply this lemma to the stabilizer of $\chi$ in $G$ to get a $\lceil \sqrt[m]{d(K)} \rceil$-coloring $\lambda$ of $\Omega$ such that only the identity element of $G$ preserves both $\chi$ and $\lambda$. Finally, as in the last paragraph of the Lemma 1.2.2, the pair $(\chi, \lambda)$ 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 $\chi$ of $\Omega = [m] \times [k]$ in a similar way as for the previous case:

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

| The coloring $\chi$ of $\Omega_u$ and blocks of $T_j$ | | | | | | |
|---|---|---|---|---|---|---|
| | $\Delta_{(u-1)t+1}$ | $\Delta_{(u-1)t+2}$ | $\Delta_{(u-1)t+3}$ | ..... | $\Delta_{(u-1)t+t-1}$ | $\Delta_{(u-1)t+t}$ |
| $\Lambda_1$ | 1 | 1 | 1 | ..... | 1 | 1 |
| $\Lambda_2$ | 0 | 1 | 1 | ..... | 1 | 1 |
| $\Lambda_3$ | 0 | 0 | 1 | ..... | 1 | 1 |
| $\Lambda_4$ | 0 | 0 | 0 | ..... | 1 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| $\Lambda_{t-1}$ | 0 | 0 | 0 | ..... | 1 | 1 |
| $\Lambda_t$ | 0 | 0 | 0 | ..... | 0 | 1 |
| $\Lambda_{t+1}$ | 0 | 0 | 0 | ..... | 0 | 0 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| $\Lambda_m$ | 0 | 0 | 0 | ..... | 0 | 0 |

Let $T_j = C_{H_j}(\chi)$ be the stabilizer of $\chi$ in $H_j$. Since the number of points colored with 1 is different in each $\Delta_i$, the elements of $T_j$ setwisely stabilize them. If $h \in T_j \leq H_j$ then $h$ acts on $\Omega_u$ coordinatewise and at the same time it setwisely stabilizes each $\Delta_i$. Therefore $\{\Lambda_i = \{(i, (u-1)t + w) \,|w \in [t]\}$ is a system of blocks of imprimitivity for $T_j$. If $h \in T_j$ fixes $\Lambda_i$ setwise then it must act on $\Lambda_i$ trivially. Now we define a new coloring which is analogous to the construction of $\lambda$ given in the proof of Lemma 1.2.1. We have $\Lambda_i$ instead of $\Delta_j$, the setwise stabilizer of $\Lambda_i$ instead of $H_j$ and $m$-coloring of $\{\Lambda_1, \ldots, \Lambda_m\}$ instead of the $d(K)$ coloring of $\Gamma$. So, there is a coloring $\beta_u : \Omega_u \mapsto \{0, \ldots, \lceil \sqrt[t]{m} \rceil - 1\}$ for every $u$ such that if $h \in H_{(u-1)t+v}$ fixes both $\chi$ and $\beta_u$, then it acts trivially on $\Omega_u$.

Let $\beta : \Omega \mapsto \{0, \ldots, \lceil \sqrt[t]{m} \rceil - 1\}$ be the union of the $\beta_u$'s. So, if $h \in H_j$ is fixing both $\chi$ and $\beta$ then it is pointwisely stabilizing $\Delta_j$. If $G' = C_G(\chi) \cap C_G(\beta)$ then $H'_j = N_{G'}(\Delta_j) = C_{G'}(\Delta_j)$. Thus, we get that Lemma 1.2.1 can be applied for the intersections of the stabilizers of $\chi$ and $\beta$. 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 $\chi, \beta, \lambda$. Finally, we can encode the triple $(\chi, \beta, \lambda)$ with the $2 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$-coloring $\mu$ of $\Omega$ given as $\mu(x) := 2 \cdot \lceil \sqrt[t]{m} \rceil \lambda(x) + 2 \cdot \beta(x) + \chi(x)$.

Now the only case which is missing is the $m = 6$ case. We again start with the restriction of the $\mathrm{Soc}(N)$ on $\Omega_u$:

$$D_u = \mathrm{Soc}(N)|_{\Omega_u} = \{(\sigma^{z_1}, \sigma^{z_2}, \sigma^{z_3}, \ldots, \sigma^{z_t}) | \sigma \in \mathrm{Alt}(6)\}$$

for some fixed $1 = z_1, z_2, \ldots, z_t \in \mathrm{Aut}(\mathrm{Alt}(6))$. Suppose that $z_i \notin \mathrm{Sym}(6)$ for some $i$. (Otherwise, the same argument works as for $m \neq 6$.) We claim that $|\{i \,|\, z_i \in \mathrm{Sym}(6)\}| = \frac{t}{2}$. Let $G_u$ be the restricted action of $N_G(\Omega_u)$ to $\Omega_u$. Since $\Omega_u$ is a block of imprimitivity and $\Delta_i$'s are blocks as well, $G_u$ acts on $\{\Delta_{(u-1)t+1}, \ldots, \Delta_{(u-1)t+t}\}$ transitively. Let $\sim$ be a relation on $\{\Delta_{(u-1)t+1}, \ldots, \Delta_{(u-1)t+t}\}$ such that $\Delta_i \sim \Delta_j$ if and only if $z_i z_j^{-1} \in \mathrm{Sym}(6)$. It is obvious that $\sim$ is an equivalence relation. Since we assumed that there is a $z_i \notin \mathrm{Sym}(6)$, there are two equivalence classes. The equivalence classes of $\sim$ gives us a new system of blocks of imprimitivity. Therefore $t$ must be even and $|\{i \,|\, z_i \in \mathrm{Sym}(6)\}| = \frac{t}{2}$.

As in the previous case, we can re-enumerate the the elements of each $\Omega_u$ in such a way that $D_u = \{(\sigma_1, \ldots, \sigma_t) | \sigma_i \in \mathrm{Alt}(6) \text{ for all } i \in [t]\}$ where $\sigma_i = \sigma$ for $i \in \{1, \ldots, \frac{t}{2}\}$ and $\sigma_i = \sigma^z$ for $i \in \{\frac{t}{2} + 1, \ldots t\}$ where $\sigma \in \mathrm{Alt}(6)$ and $z \in \mathrm{Aut}(\mathrm{Alt}(6)) \setminus \mathrm{Sym}(6)$. Let $\Omega_u^{(1)} = \cup_{i=(u-1)t+1}^{(u-1)t+\frac{t}{2}} \Delta_i$ and $\Omega_u^{(2)} = \cup_{i=(u-1)t+\frac{t}{2}+1}^{(u-1)t+t} \Delta_i$. Then $\{\Omega_u^{(1)}, \Omega_u^{(2)}\}$ is a system of blocks

for $G_u$.

If $t = 2$, $2 \cdot \lceil \sqrt[t]{m} \rceil = 2 \cdot \lceil \sqrt{6} \rceil = 6$. By Lemma 1.2.2, $d(G) \leq 6 \cdot \lceil \sqrt[6]{d(K)} \rceil$ since $m = 6$. Hence, when $t = 2$ the lemma is satisfied.

Now assume that $t \geq 4$. Then $2 \cdot \lceil \sqrt[t]{m} \rceil = 2 \cdot \lceil \sqrt[t]{6} \rceil = 4$. We define a 4 coloring $\chi_u$ of $\Omega_u$ as the following:

| The coloring $\chi_u$ of $\Omega_u$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\Omega_u^{(1)}$ | | | | | $\Omega_u^{(2)}$ | | | | |
| $\Delta_{(u-1)t+1}$ | $\Delta_{(u-1)t+2}$ | $\Delta_{(u-1)t+3}$ | $\cdots$ | $\Delta_{(u-1)t+\frac{t}{2}}$ | $\Delta_{(u-1)t+\frac{t}{2}+1}$ | $\Delta_{(u-1)t+\frac{t}{2}+2}$ | $\Delta_{(u-1)t+\frac{t}{2}+3}$ | $\cdots$ | $\Delta_{(u-1)t+t}$ |
| 0 | 0 | 0 | ... | 0 | 3 | 3 | 0 | ... | 0 |
| 1 | 0 | 0 | ... | 0 | 2 | 3 | 0 | ... | 0 |
| 1 | 1 | 0 | ... | 0 | 2 | 2 | 0 | ... | 0 |
| 2 | 1 | 0 | ... | 0 | 1 | 2 | 0 | ... | 0 |
| 2 | 2 | 0 | ... | 0 | 1 | 1 | 0 | ... | 0 |
| 3 | 2 | 0 | ... | 0 | 0 | 1 | 0 | ... | 0 |

Suppose that $g \in G_u$ is fixing $\chi_u$. Then it must fix the blocks $\Omega_u^{(1)}$ and $\Omega_u^{(2)}$. Furthermore, the restriction of $g$ on each of $\Omega_u^{(1)}$ and $\Omega_u^{(2)}$ has the form $(\sigma_g, \pi_g)$ where $\sigma_g$ is permuting the rows and $\pi_g$ is permuting the columns. Obviously, $\sigma_g$ must be trivial. Let $\chi$ be the union of $\chi_u$ colorings. We apply Lemma 1.2.1 to the stabilizer of $\chi$ to get a $\lceil \sqrt[m]{d(K)} \rceil$-coloring $\lambda$. If $\mu(x) := 4 \cdot \lambda(x) + \chi(x)$ then only the identity element of $G$ preserves $\mu$. Therefore, $d(G) \leq 4 \cdot \lceil \sqrt[m]{d(K)} \rceil = 2 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$.

□

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

**Lemma 1.2.6.** *If $G \leq \mathrm{Sym}(\Omega)$ is a (finite) quasi-primitive permutation group, then $d(G) \leq 4$ or $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$.*

*Proof.* We prove this lemma by induction on $n$ where $n = |\Omega|$. If $G$ is a primitive permutation group, then by Seress [64, Theorem 2] and Dolfi [23, Lemma 1], $d(G) \leq 4$ or $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$. Now assume that $G$ is not primitive but quasi-primitive. Let $\Gamma$ be a system of blocks for $G$ with $k = |\Gamma| < n$ maximal. Let $K$ be the action of $G$ on $\Gamma$, i.e. if $\varphi : G \mapsto \mathrm{Sym}(\Gamma)$ is the homomorphism associated with the action of $G$ on $\Gamma$ then $K \cong G/\ker(\varphi)$. Then $\ker(\varphi) \lhd G$ but it is not transitive, hence $\ker(\varphi) = 1$ and so $K \cong G$. Since a distinguishing partition of $\Gamma$ for $K$ naturally gives rise to a distinguishing partition of $\Omega$ for $G$, we have $d_\Omega(G) \leq d_\Gamma(K)$. By induction, $d(G) \leq d(K) \leq 4$ or $\mathrm{Alt}(\Gamma) \leq K \leq \mathrm{Sym}(\Gamma)$. Thus we may assume that $\mathrm{Alt}(\Gamma) \leq K \leq \mathrm{Sym}(\Gamma)$ with $k \geq 5$. We claim that the size of each block should be at least $k - 1$. Assume that $H_1 = N_G(\Delta_1)$ acts on $\Delta_1$ non-trivially. $H_1$ also acts on $\{\Delta_2, \ldots, \Delta_k\}$. Since $G$ acts on $\Gamma$ faithfully and $\mathrm{Alt}(\Gamma) \leq G$, we have $H_1 \simeq \mathrm{Alt}(k-1)$ or $H_1 \simeq \mathrm{Sym}(k-1)$. Thus $|\Delta_1| \geq k - 1$ unless $H_1 \simeq \mathrm{Sym}(k-1)$ and $C_{H_1}(\Delta_1) \simeq \mathrm{Alt}(k-1)$ or $k = 5$, $H_1 \simeq \mathrm{Alt}(4)$ and $C_{H_1}(\Delta_1) \simeq (\mathrm{Alt}(4))'$. In the first case, $G \simeq \mathrm{Sym}(\Gamma)$, $G' \simeq \mathrm{Alt}(\Gamma)$ and $G_\alpha < G' < G$ for any $\alpha \in \Omega$. $G'$ is a non-trivial normal subgroup of $G$ which is not transitive on $\Omega$, which contradicts with the assumption that $G$ is quasi-primitive. In the second case we have $K = \mathrm{Alt}(\Gamma)$, so $d_\Omega(G) \leq d_\Gamma(K) \leq 4$ holds.

Now, for each $i$ with $0 \leq i \leq k - 1$, we color $i$ letters in block $i + 1$ with 1 and the rest with 0.

| Coloring of $\Omega$ | | | | | |
|---|---|---|---|---|---|
| $\Delta_1$ | $\Delta_2$ | $\Delta_3$ | ..... | $\Delta_{k-1}$ | $\Delta_k$ |
| 0 | 1 | 1 | ..... | 1 | 1 |
| 0 | 0 | 1 | ..... | 1 | 1 |
| 0 | 0 | 0 | ..... | 1 | 1 |
| 0 | 0 | 0 | ..... | 1 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| 0 | 0 | 0 | ..... | 1 | 1 |
| 0 | 0 | 0 | ..... | 0 | 1 |
| 0 | 0 | 0 | ..... | 0 | 0 |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| 0 | 0 | 0 | ..... | 0 | 0 |

If $g \in G$ is fixing this coloring then it fixes all the blocks setwisely, i.e. $g \in \ker(\varphi)$. This way we colored the elements of $\Omega$ 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]. Every quasi-primitive permutation group is innately transitive. The next theorem is a partial generalization of Lemma 1.2.6. It considers a class of groups which contains the class of innately transitive groups.

**Theorem 1.2.7.** *Let $M \lhd G \leq \mathrm{Sym}(\Omega)$ be transitive permutation groups where $\Omega$ is finite and $M$ is a direct product of isomorphic simple groups. Then $d(G) \leq 8$ or $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$.*

*Proof.* We prove the claim using induction on $n = |\Omega|$. By Lemma 1.2.6 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 blocks of imprimitivity for the action of $G$. Let $\Gamma$ consists of minimal blocks, each of size $m$ and let $N$ be the kernel of the action of $G$ on $\Gamma$. Set $K = G/N$, a subgroup of $\mathrm{Sym}(\Gamma)$.

First let us assume that $N = 1$. By the induction hypothesis, $d(G) = d_\Omega(G) \leq d_\Gamma(K) \leq 8$, or $G \cong \mathrm{Alt}(\Gamma)$ or $G \cong \mathrm{Sym}(\Gamma)$ with $k \geq 9$. In the latter case $G$ is quasi-primitive, since $M = \mathrm{Soc}(G)$ is the only minimal normal subgroup of $G$ and it is transitive. The claim follows. So from now on $N$ is non-trivial.

Now assume that the action of $H_1$ on $\Delta_1$ is not large. $MN/N$ is a direct product of isomorphic simple groups and moreover it is a transitive normal subgroup of $K$. So by the induction hypothesis $d(K) \leq 8$ or $K$ is an alternating or symmetric group of degree at least 9 in its natural action on $\Gamma$. If $d(K) \leq 8$ then by Corollary 1.2.3 $d(G) \leq 4 \cdot \lceil \sqrt[m]{8} \rceil \leq 8$ for $m \geq 3$, and by Lemma 1.2.2 $d(G) \leq 2 \cdot \lceil \sqrt[2]{8} \rceil \leq 8$ for $m = 2$. Now suppose that the latter case holds. If $m \geq k - 1$, then again by Corollary 1.2.2 $d(G) \leq 4 \cdot \lceil \sqrt[k-1]{k} \rceil \leq 8$. If $m < k - 1$, consider the image $\overline{M}$ of $M$ under the natural homomorphism from $G$ to $K = G/N$. Since $M \lhd G$ acts transitively on $\Gamma$, 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 $k \geq 9$. 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 $\Delta_1$ in $M$ acts trivially on $\Delta_1$, and this contradicts with the transitivity of $M$.

If the action of $H_1$ on $\Delta_1$ is large, then $R = \mathrm{soc}(N)$ is a subdirect product of $k$ many copies of $\mathrm{Alt}(m)$, so it is isomorphic to a direct product of, say, $r$ copies of $\mathrm{Alt}(m)$ where $m \geq 5$ (by Proposition 1.2.4). Furthermore, since $G$ acts transitively on $\Gamma$, 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 $\Gamma$ 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 $\Gamma$, 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 $N$ is $k$.

By Lemma 1.2.5, $d(G) \leq 2 \cdot \lceil \sqrt[k]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil = 4 \cdot \lceil \sqrt[m]{d(K)} \rceil$. By the induction hypothesis, $d(K) \leq 8$ (in which case $d(G) \leq 8$ by the previous inequality) or $K$ is an alternating or a symmetric group of degree $k \geq 9$. But in the latter case $\mathrm{Alt}(m) \cong MN/N = \mathrm{Soc}(K)$, so $m = k$ (and $d(K) \leq m$). Thus $\lceil \sqrt[m]{d(K)} \rceil = 2$ and so $d(G) \leq 8$ by Lemma 1.2.5. □

Now we are ready to calculate the upper bound for the distinguishing number of transitive permutation groups.

**Theorem 1.2.8.** *Let $G$ be a transitive permutation group of degree $n > 1$. Then $\sqrt[n]{|G|} < d(G) \leq 24\sqrt[n]{|G|}$.*

*Proof.* First suppose that $G \leq \mathrm{Sym}(\Omega)$ is a quasi-primitive permutation group. By Lemma 1.2.6, we may assume that $n = |\Omega| \geq 24$ and $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$. In this case we have $d(G) \leq n < 24\sqrt[n]{n!/2} \leq 24\sqrt[n]{|G|}$ 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 $\Omega$, so $M$ is isomorphic to a direct product of isomorphic simple groups. Let an orbit of $M$ on $\Omega$ be $\Delta$, and let $\Gamma$ be the set of orbits of $M$ on $\Omega$. Let the size of $\Gamma$ be $k$ and $H$ be the stabilizer of $\Delta$ in $G$. As before, denote the distinguishing number of $H$ acting on $\Delta$ by $d_\Delta(H)$. Since $M \lhd H$ is transitive on $\Delta$, Theorem 1.2.7 implies that $d_\Delta(H) \leq 8$ or $\mathrm{Alt}(\Delta) \leq H/C_H(\Delta) \leq \mathrm{Sym}(\Delta)$.

Case 1. $d_\Delta(H) \leq 8$.

By Lemma 1.2.2, $d(G) \leq 8 \left\lceil \sqrt[m]{d(K)} \right\rceil$ where $K$ is the action of $G$ on $\Gamma$ and $m = |\Delta|$. Since $K$ is a transitive group on $k$ points, by induction we have $d(K) \leq 24\sqrt[k]{|K|}$. If $m \geq 8$, then

$$d(G) \leq 8 \left\lceil \sqrt[m]{d(K)} \right\rceil \leq 8 \left\lceil \sqrt[m]{24\sqrt[k]{|K|}} \right\rceil \leq 16\sqrt[m]{24\sqrt[k]{|K|}} \leq 24\sqrt[n]{|K|} \leq 24\sqrt[n]{|G|}.$$

If $m \leq 7$ then we can use the previous estimate with 8 replaced by $m$. Using that $2m\sqrt[m]{24} < 24$ for $m \leq 7$ we get that $d(G) \leq 24\sqrt[n]{|G|}$ .

Case 2. $\mathrm{Alt}(\Delta) \leq H/C_H(\Delta) \leq \mathrm{Sym}(\Delta)$ with $|\Delta| = m \geq 9$.

In this case the action of $H$ on $\Delta$ is large. Let the kernel of the action of $G$ on $\Gamma$ be $N$ with linking factor $t$. 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 1.2.5 implies that

$$d(G) \leq 2\lceil \sqrt[t]{m} \rceil \lceil \sqrt[m]{d(K)} \rceil \leq 4\epsilon \sqrt[t]{m} \sqrt[m]{d(K)} = 4\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)}.$$

Set $c = 4 \cdot 2^{1/mt} \cdot 3^{1/t}$. By use of the inequality $\frac{1}{2}(m/3)^m < m!/2 = |\mathrm{Alt}(m)|$, we have that $d(G)$ is at most

$$4\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)} < 4\epsilon \sqrt[mk]{((m!/2) \cdot 2 \cdot 3^m)^{k/t}} \sqrt[m]{d(K)} = c \cdot \epsilon \sqrt[n]{(|\mathrm{Alt}(m)|)^{k/t}} \sqrt[m]{d(K)}.$$

As noted in Equation 1.1, 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 $d(K) \leq 24\sqrt[k]{|K|}$. Thus

$$d(G) < c \cdot \epsilon \sqrt[m]{24} \sqrt[n]{|N|} \sqrt[n]{|K|} \leq 4 \cdot \epsilon \cdot 2^{1/9t} 3^{1/t} \sqrt[9]{24} \sqrt[n]{|G|} < 24\sqrt[n]{|G|}.$$

□

# Chapter 2

# The Base Size of Finite Permutation Groups

## 2.1 The Concept of the Base

The concept of a base for a permutation group was first introduced by Sims [66] in the 1960s. Let $G$ be a permutation group acting on a finite set $\Omega$ of size $n$. A subset (or an ordered list) $\Sigma$ of $\Omega$ is called a *base* for $G$ if the pointwise stabilizer of $\Sigma$ in $G$ is trivial.

If $g \in G$ then its action is uniquely determined by its action on a base. Assume not and let there be another element $h \in G$ that acts on the base the same way as $g$. Then $gh^{-1}$ fixes all the points of the base so it must be the identity element, that is, $g = h$. If we can find a base with small size then we need less memory to store the elements of the permutation group.

Let $\Sigma = [x_1, \ldots, x_b]$ be a base of $G$ where the elements are denoted as an ordered sequence. Let $G_i$ be the pointwise stabilizer of $[x_1, \ldots, x_i]$ in $G$. A generating set $S$ for $G$ with base $\Sigma$ is called a *strong generating set* relative to $\Sigma$ if $\langle S \cap G_i \rangle = G_i$ for $0 \leq i \leq b$. Bases and strong generating sets are used in many permutation group theoretic algorithms [65], such as calculating the order, testing whether $g \in G$ for some $g \in \mathrm{Sym}(\Omega)$, identifying the isomorphism type of a given simple group, choosing a random element of $G$. The permutation group algorithms usually run faster if we have a small base.

A base is minimal if no proper subset of it is a base and the base size of $G$ on $\Omega$, denoted by $b(G)$, is the cardinality of the smallest base for $G$. In general, a minimal base is not necessarily the smallest one (which has the smallest size among all bases of the group). For example, if $G = \mathrm{Sym}(3)$ acting on $\Omega = \{1, 2, \ldots, 9\}$ where $\Omega_1 = \{1, 2, 3\}$ and $\Omega_2 = \{4, 5, \ldots, 9\}$ are the orbits of $G$ such that $G$ acts on $\Omega_1$ in the natural way and on $\Omega_2$ in a regular way, then both $\{1, 2\}$ and $\{4\}$ are minimal bases for $G$.

If $\Sigma = [x_1, \ldots, x_b]$ is a base of $G$ then $G = G_0 \geq G_1 \geq G_2 \geq \ldots \geq G_b = 1$ is a chain of subgroups of $G$. If no base point is fixed by the stabiliser of the previous points in the base, i.e. all the inclusions of the subgroup chain is strict, then the base is called irredundant. Irredundancy may change with the reordering of the base elements. For example, if $G = \{(1), (35)(46), (12)(3456), (12)(3654)\}$ then both $[1, 3]$ and $[3]$ are irredundant bases. But if we reorder the first base, $[3, 1]$ is not an irredundant base

anymore. However if $\Sigma$ is minimal then it is irredundant in any ordering.

Some straightforward examples are given below.

**Example 2.1.1.**

(1) A permutation group has base size 1 if and only if it has a regular orbit.

(2) If $G \leq \mathrm{Sym}(\Omega)$ is sharply $k$-transitive (i.e. for any two $k$-tuples of distinct elements of $\Omega$, there is a unique element in $G$ mapping one to the other) then $b(G) \leq k$ since the stabiliser of any $k$-tuple is trivial.

(3) The base sizes of $\mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$ with their natural action on $\Omega$ are $|\Omega| - 1$ and $|\Omega| - 2$, respectively.

(4) Considering the natural action of $G = GL(V)$ on $V$, a set of vectors $B \subset V$ is a smallest base for $G$ if and only if $B$ is a basis of $V$ in a linear algebraic sense.

Let $\Sigma$ be a minimal base for $G$. If we color each point of $\Sigma$ and the set $\Omega \setminus \Sigma$ with a different color then we get a distinguishing partition. Therefore;

**Proposition 2.1.2.** $d(G) \leq b(G) + 1$.

If $\Sigma = [x_1, \ldots, x_b]$ is a minimal base then $|G_i : G_{i+1}| \geq 2$ for all $i \in \{1, \ldots, b\}$ since $G_i \gneqq G_{i+1}$. Moreover, every element of $G$ is uniquely determined by its action on the base. Therefore we have the following bounds:

**Proposition 2.1.3.** $2^{b(G)} \leq |G| \leq n^{b(G)}$.

Let $B$ be an irredundant base for $G$ with size $d$. Then $2^d \leq |G| \leq n^{b(G)}$, and $d \leq b(G) \log n$ (base of the logarithms is 2 unless otherwise stated).

We can find a base with using the greedy algorithm and approximate $b(G)$. The greedy algorithm of Blaha [8] says that always choose a base point $\alpha_i \in \Omega$ from a largest orbit of $G_{i-1}$. The point is that, we want to reach the identity as soon as possible by the chain of point stabilizers. He proved the following:

**Theorem 2.1.4** (Blaha, [8, Theorem 4.4])**.** *Let $G$ be a permutation group with minimal base size $b(G)$. Then any base found by the greedy algorithm has size at most $O(b(G) \log \log n)$.*

*Proof.* Let $H$ be a subgroup in $G$ and let $\Sigma$ be a smallest base for $G$ on $\Omega$, so $|\Sigma| = b(G)$. Denote $\Sigma$ as an ordered $b(G)$-tuple $[x_1, \ldots, x_{b(G)}]$. $H$ acts on the set of $b(G)$-tuples of $\Omega$ and the $H$-orbit of $\Sigma$ is regular since $\Sigma$ is a base for $H$. Assume that all the orbits of $H$ on $\Omega$ has size smaller than $|H|^{1/b(G)}$. Then the size of the orbit of $\Sigma$ can not be as big as the order of $|H|$. So $H$ has an orbit of size at least $|H|^{1/b(G)}$. If $\alpha$ is an element from the largest orbit of $H$, then by Orbit-Stabilizer theorem we get that $|H_\alpha||O_\alpha| = |H|$ where $O_\alpha$ is the orbit of $\alpha$ under the action of $H$. By the assumption, $|O_\alpha| \geq |H|^{1/b(G)}$ and so $|H_\alpha| \leq |H|^{1-1/b(G)}$.

Now we use the greedy algorithm to choose $b(G) \log \log n$ base points. Their stabilizer has order at most

$$|G|^{\left(1-\frac{1}{b(G)}\right)^{b(G)\log\log n}} \leq (n^{b(G)})^{e^{-\frac{1}{b(G)}b(G)\log\log n}} = (n^{b(G)})^{\frac{1}{e^{\log\log n}}} = n^{\frac{b(G)}{\log n}} = 2^{b(G)};$$

so if we choose $b(G)$ more base points by any irredundant method completes a base. □

Now, I would like to briefly mention the computational complexity of finding minimum bases. In Computational Complexity Theory a problem is assigned to be in P if its solution time is bounded by a polynomial time. So P class basically includes all the problems that can be solved by a reasonably fast program. NP stands for 'non-deterministic polynomial time'. NP includes all the problems where checking whether a given solution is really a solution takes a reasonable amount of time. A problem is called NP-hard if an algorithm for solving it can be translated into one for solving any NP problem. If a problem is both NP and NP-hard then it is called an NP-complete problem.

In 1972 Karp [43] gave a list of 21 problems which are NP-complete. One of these problems is the 'exact cover problem'. Let $X$ be a set and $C$ be a collection of subsets of $X$. An exact cover is a subcollection $C'$ of $C$ such that each element in $X$ is contained in exactly one subset in $C'$. The exact cover problem is a decision problem to determine whether an exact cover exists. If $|X| = 3q$ and $C$ is a collection of 3 element subsets of $X$, then the exact cover problem is denoted by X3C.

Blaha [8] showed that the problem of finding $b(G)$ for a permutation group $G$ is NP-hard. He proved that the corresponding decision problem, which is called the 'minimum base problem' and denoted by MB, is NP-complete. Let $G$ be a subgroup of $\mathrm{Sym}(n)$ given by generators and $N \leq n$ be a positive integer. MB asks whether there exists a base for $G$ of size no more than $N$.

Blaha reduced the problem of having an exact cover by three-sets to MB. First he proved the NP-completeness of MB in cyclic groups in the following theorem:

**Theorem 2.1.5** (Blaha [8, Theorem 3.1])**.** *MB is NP-complete even if $G$ is constrained to be a cyclic group.*

*Proof.* Let $X$ be a set of cardinality $3q$ and $C$ be a collection of three element subsets of $X$ where $|C| = r$. Assume without loss of generality that each $x \in X$ is contained in at least one $c \in C$. Let $P = \{p_1, p_2, \ldots, p_{3q}\}$ be the set of the first $3q$ primes. Define an injective map $f : X \to P$. For $c = \{x, y, z\} \in C$ let $s_c = f(x)f(y)f(z)$. Now let $n = \sum_{c\in C} s_c$ and construct an element $\sigma$ of $\mathrm{Sym}(n)$ with cycle decomposition consisting of $r$ disjoint cycles where there is a cycle of length $s_c$ for each $c \in C$. So an instance of MB is created with $G = \langle\sigma\rangle$ and $N = q$. Prime number theorem implies that $n$ is $\mathcal{O}(r(q\log q)^3)$. Hence the reduction above is polynomial-time.

Let $B = \{b_1, b_2, \ldots, b_k\} \subseteq [n]$ where $b_i$ is a point from the cycle with length $s_{c_i}$ and $k \leq q$. An element $\sigma^t$ of $G$ fixes $b_i$ if and only if $s_{c_i}$ divides $t$. Thus, $\sigma^t$ pointwisely fixes $B$ if and only if $s := lcm(s_{c_1}, s_{c_2}, \ldots, s_{c_k})|t$. So, the pointwise stabiliser of $B$ is $\langle\sigma^s\rangle$. If $B$ is a base, then $\sigma^s$ must be the identity element. Therefore, $|G|$ must divide $s$. Since each $x \in X$ is contained in at least one $c \in C$, every prime from $P$ divides a suitable $s_{c_i}$. This implies that $|G| = \prod_{i=1}^{3q} p_i$. Since all $s_{c_i}$ are the product of exactly 3 primes, a base

of size $k$ exists if and only if $s = \prod_{i=1}^{3q} p_i = |G|$. $s = |G|$ if and only if $k = q$ and the $s_{c_i}$ are relatively prime where $1 \leq i \leq k$. The $s_{c_i}$ are relatively prime if and only if the three element sets $c_i$ are disjoint. Therefore $B = \{b_1, b_2, \ldots, b_k\}$ is a base for $G$ with $k \leq q$ if and only if $k = q$ and the sets $c_1, c_2, \ldots, c_k$ cover $X$. □

In the above reduction if we increase $3q$, the size of X3C, then the sizes of the orbits of the cyclic group increases as well. To avoid the possibility that if the orbits of the group are restricted then MB problem can be solved efficiently, Blaha shoved that MB is still NP-complete for an elementary abelian group.

**Theorem 2.1.6** (Blaha [8, Theorem 3.2])**.** *MB is NP-complete even if $G$ is constrained to be an elementary abelian 2-group with orbits of size 8.*

Finally, I give the following remark which states a relation between the base size on the power set and the distinguishing number:

**Remark 2.1.7.** For the action of $G$ on the power set $P(\Omega)$ of $\Omega$ we have $b_{P(\Omega)}(G) = \lceil \log(d(G)) \rceil$. More in general for the action of $G$ on the set $P^q(\Omega)$ of all partitions of $\Omega$ into at most $q$ parts, we have $b_{P^q(\Omega)}(G) = \lceil \log_q(d(G)) \rceil$.

## 2.2 The Base Size of Primitive Permutation Groups

In this chapter, I would like to briefly remind the discoveries that have been made about the base sizes of primitive permutation groups. Pyber [58] showed that there exists a universal constant $c > 0$ such that almost all subgroups $G$ of $\mathrm{Sym}(n)$ satisfy that $b(G) > cn$. So, if one wants to find a better upper bound on $b(G)$, then restriction on $G$ is needed. Since the primitive permutation groups are the building blocks of every finite permutation group, it is very natural to restrict our group as primitive.

Since the nineteenth century the minimal base size of primitive permutations groups which are not containing the alternating group is widely studied. In 1889 Bochert [9] showed that if $G$ is a primitive permutation group of degree $n$ not containing the alternating group then $b(G) \leq n/2$. This bound was improved by Babai [3] to $b(G) < 4\sqrt{n} \log n$ for uniprimitive (primitive but not doubly transitive) groups $G$, and to the estimate $b(G) < 2^{c\sqrt{\log n}}$ for a universal constant $c > 0$, for doubly transitive groups, in [4]. The bound for the doubly transitive primitive permutation groups was improved to $b(G) < c(\log n)^2$ where $c$ is a universal constant by Pyber [59]. These estimates are elementary in the sense that their proofs do not require the Classification of Finite Simple Groups (CFSG). Using CFSG Liebeck [47] 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 [19] 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 [19]. Later in [18, p. 122] Cameron wrote that $c$ can probably be taken to be 7, and the only extreme case is the Mathieu group $M_{24}$ in its natural action. He added that perhaps, with finitely many exceptions, the correct bound is actually 5. The Cameron-Kantor conjecture was proved by Liebeck and Shalev in [50], and Camerons's bound of 7 was established in the series of papers [52], [54], [10], [12], [13], [11]. The proofs are probabilistic and use bounds on fixed point ratios.

Let $d$ be a fixed positive integer. Let $\Gamma_d$ 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 and Pálfy [5] 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 $\Gamma_d$. Seress [63] proved this for $G$ a solvable primitive group by establishing the bound $b(G) \leq 4$. Babai's conjecture was proved by Gluck, Seress, Shalev [31]. Later, Liebeck and Shalev [50] showed that in Babai's conjecture the function $g(d)$ can be taken to be linear in $d$.

We have already seen that $\log |G|/\log n \leq b(G)$ holds for any finite permutation group $G \leq \mathrm{Sym}(\Omega)$ with $n = |\Omega|$. It was asked by Pyber [58] that whether $\log |G|/\log n$ is the right magnitude for $b(G)$, at least if $G$ is primitive. More precisely, he asked, whether there exists a universal constant $c > 0$ such that

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

for every finite primitive permutation group $G$ of degree $n$. Here the primitivity condition is needed. Assume not and let $G = \mathbb{Z}_2 wr \mathbb{Z}_k$ with its natural action. $G$ is a transitive imprimitive group of degree $2k$ and $b(G) = k = \log |G| - \log k$. If it satisfies the inequality above then $\log |G| - \log k < c\frac{\log |G|}{\log 2k}$ for some constant $c$. Since $|G| = 2^k k$ we get the inequality $\log 2^k \log 2k < c \log 2^k k$. Whatever is the constant $c$, there is always a $k$ which does not satisfy the inequality. Therefore for the conjecture the primitivity condition is necessary.

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

In the past, 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 treated by Gluck, Seress, Shalev [31, Remark 4.3] and Fawcett [27]. 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 $n$.

In the next chapter we finish the proof of Pyber's conjecture by showing that there

exists an absolute constant $c$ such that

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

holds for every finite primitive permutation group of affine type. Recently, Halasi, Liebeck and Maróti [34] improved this result. They showed that 45 can be replaced by 2 for every finite primitive permutation group. Moreover, they also stated that 2 is the best possible multiplicative constant.

# Chapter 3

# Pyber's Base Size Conjecture for Groups of Affine Type

## 3.1 Introduction

A primitive permutation group of affine type $G$ acting on a set $\Omega$ is defined to be a primitive permutation group with a unique regular abelian normal subgroup $V$. $V$ is elementary abelian and regular, hence we can identify $\Omega$ with $V$. Denote the stabilizer of the zero vector in $G$ by $H$. The group $H$ can be viewed as a subgroup of $GL(V)$ and $G = V \rtimes H \leq AGL(V)$. It is obvious that $b(G) = b_V(G) = b_V(H) + 1$.

For an affine primitive permutation group $G = V \rtimes H$, where $(|H|, |V|) = 1$, Pyber's conjecture was first established by Gluck and Magaard in [30] by showing that $b(G) \leq 95$. They investigated the regular orbits of $H$-modules. Halasi and Podoski decreased this bound to 3 in [36] by showing that coprime linear groups have a base of size 2. 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 [63] and Halasi and Maróti [35] established the best possible bound; $b(G) \leq 4$. Fawcett and Praeger [28] proved Pyber's conjecture for affine primitive permutation groups $G = V \rtimes H$ in case where H preserves a direct sum decomposition $V = V_1 \oplus \ldots \oplus V_t$ and $H$ is close to a full wreath product $GL(V_1)wrL$ with $L$ a permutation group of degree $t$ satisfying any of four given properties.

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. We call $H$ an imprimitive linear group or a primitive linear group if $V$ is imprimitive or primitive, respectively.

Liebeck and Shalev [52], [53] proved Pyber's conjecture for the case where $H$ is a primitive linear group. They gave a characterization of primitive linear groups of unbounded base size. (There is a similar characterization of primitive linear groups of large orders due to Jaikin-Zapirain and Pyber [40, Proposition 5.7].) They calculated the folloving bound for $H$ where it acts on $V$ primitively:

**Theorem 3.1.1** (Liebeck, Shalev [52],[53])**.** *There exists a universal constant $c > 0$ such that if $H$ acts primitively on $V$, then $b_V(H) \leq \max\{18\frac{\log|H|}{\log|V|} + 30, c\}$.*

In this chapter, 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 irreducible $\mathbb{F}_p H$-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 $\Pi = \{V_1, \ldots, V_t\}$ since it is irreducible on $V$. 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 $P \simeq H/N$.

**Lemma 3.1.2.** *If $K_1$ is trivial, then $b_V(H) = \lceil \log_{|V_1|} d_\Pi(P) \rceil$.*

*Proof.* $K_1 = 1$ implies that every orbit of $H$ in $\cup_{i=1}^{t} V_i$ contains exactly one element from every subspace $V_i$. Thus we can define a one-to-one correspondence $\alpha_{ij} : V_i \to V_j$ between any pair of subspaces $V_i$ and $V_j$ such that $\alpha_{ij}(v) = h(v)$ for every $v \in V$ and for every $h \in H$ satisfying $h(V_i) = V_j$.

Assume that $b$ is 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 $V = \oplus_{i=1}^{t} V_i$. Let $\sim$ be an equivalence relation on $\Pi$ where $V_i \sim V_j$ if and only if $(v_1^{(i)}, \ldots, v_b^{(i)})$ corresponds to $(v_1^{(j)}, \ldots, v_b^{(j)})$ under $\alpha_{ij}$, i.e. $\alpha_{ij}(v_s^{(i)}) = v_s^{(j)}$ for every $1 \leq s \leq b$. The partition defined by $\sim$ is a distinguishing partition for $P$ on $\Pi$ if and only if the set $\{w_1, \ldots, w_b\}$ is a base for $H$ on $V$. For any $i$, the number of different vectors of the form $(v_1^{(i)}, \ldots, v_b^{(i)})$ with entries from $V_i$ is $|V_1|$. So $b_V(H)$ is the smallest integer such that $|V_1|^{b_V(H)}$ is at least $d_\Pi(P)$. Thus $b_V(H) = \lceil \log_{|V_1|} d_\Pi(P) \rceil$. □

In the proof above the transitivity of $P$ is not needed. Hence it is also correct if $P$ is not transitive and $K_i = 1$ for all $i \in \{1, \ldots, t\}$.

Now we find a bound for the base size of $H$ where $K_1$ is not trivial but has a bounded base size on $V_1$.

**Theorem 3.1.3.** *Assume that $b_{V_1}(K_1) \leq b$ for some constant $b$. Then we have*

$$b_V(H) \leq b + 1 + \log 24 + \frac{\log |P|}{\log |V|}.$$

*Proof.* For every $K_i$ choose a base $\{v_1^{(i)}, v_2^{(i)}, \ldots, v_b^{(i)}\} \subset V_i$ where $1 \leq i \leq t$. Let $w_s = \sum_{i=1}^{t} v_s^{(i)}$ for every $1 \leq s \leq b$ and $L = \cap_s C_H(w_s)$. Hence $L \cap H_i = C_L(V_i)$ for every $i$. So we can apply Lemma 3.1.2 for $L$, and we get $b_V(H) \leq b + \lceil \log_{|V_1|} d_\Pi(P) \rceil$. By Theorem 1.2.8 $d_\Pi(P) \leq 24\sqrt[t]{|P|}$. Therefore

$$b_V(H) \leq b + 1 + \log_{|V_1|}(24\sqrt[t]{|P|}) \leq b + 1 + \log 24 + \frac{\log |P|}{t \log |V_1|} = b + 1 + \log 24 + \frac{\log |P|}{\log |V|}.$$

□

Thus Pyber's conjecture is valid if $b_{V_1}(K_1)$ is bounded. From now on we will focus on the case where $K_1$ doesn't have a bounded base on $V_1$. In the following section I explain the tools that are going to be used later while examining this case.

## 3.2 Preliminaries

After this point, it will be more useful for us to use group representation approach. So, instead of considering $H$ as a fixed subgroup of $GL(V)$, let it be a fixed abstract group and let $X : H \to GL(V)$ be a representation of $H$. With this method we can reduce the problem of finding a suitable small base for $H$ to some representations of $H$ where $X(H)$ is easier to deal with.

The second modification is to extend the base field to consider vector spaces over $\mathbb{F}_q$ where $q$ is a $p$-power. We might need this to be able to use Theorem 1 of Liebeck and Shalev [53], in which they gave the structure of primitive linear groups of unbounded base size. Clearly, $b_V(X(H))$ doesn't depend on whether we view $V$ as an $\mathbb{F}_p$-space or as an $\mathbb{F}_q$-space. If $V$ is a vector space over $\mathbb{F}_q$, we use $V(p)$ to denote $V$ as an $\mathbb{F}_p$ vector space.

Again we assume that $V = \oplus_{i=1}^{t} V_i$ is a direct sum decomposition of $V$ where $V_i$ are $\mathbb{F}_q$-spaces for $i \in \{1, \ldots, t\}$. Let $X : H \to GL(V)$ be a representation of $H$ where $X(H)$ permutes the set $\Pi = \{V_1, \ldots, V_t\}$ transitively. 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 $H_1$. The third modification is to generalize the concept of linear and projective representations in order to make the reduction argument work.

**Definition 3.2.1.** 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 3.2.2.** 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 $g \in G$.

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

$$b_X(H) := b_V(X(H)T). \tag{3.1}$$

Equivalent $\pmod T$-representations have the same base size. In the special case when $H \leq GL(V)$ and $X : H \to GL(V)$ is the inclusion map, then $b_V(H) \leq b_X(H)$ holds.

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

Now 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 $\pmod T$-representations of $H$ means that they are projectively equivalent. Slightly more generally, if $X : H \to GL(V(p))$ is any map satisfying (1) of Definition 3.2.1 (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 $X : H \to \Gamma L(V)$ a projective representation. Furthermore, for any projective representation $X : H \to \Gamma L(V)$, we will denote the associated homomorphism $H \to P\Gamma L(V)$ by $\mathfrak{X}$ (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

$$T_V = \{g \in GL(V) | g(V_i) = V_i \text{ and } g|_{V_i} \in Z(GL(V_i)) \ \forall 1 \leq i \leq t\} \simeq (\mathbb{F}_q^{\times})^t. \tag{3.2}$$

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 formula.

If $q > 2$ and $X : H \to GL(V)$ is an arbitrary map, then $X$ satisfies (1) of Definition 3.2.1 (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 $H_1$.

In the following two sections we consider two special cases, which we will respectively call alternating-induced and classical-induced classes. Here alternating-induced means that $K_1 = H_1/C_{H_1}(V_1)$ 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 $F_{q^0} \leq F_q$) with its natural action on $V_1$. Then in the last section of this chapter we show how the general case can be reduced to one of these modules.



## 3.3 Alternating-induced Representations

In this section we 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 $k$ where $k$ is at least 7, and $K_i$ acts on $V_i$ such that, as an $\mathbb{F}_q K_i$ -module ($q$ is a power of $p$), $V_i$ 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 $F_q$. 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 $V_i$ . This is a well-known construction (see [44, p. 185], for example).

**Proposition 3.3.1.** *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*

$$U_0 = \Big\{ \sum_i \alpha_i e_i \mid \alpha_i \in \mathbb{F}_q,\ \sum_i \alpha_i = 0 \Big\} \quad \text{and} \quad W = \Big\{ \alpha\big(\sum_i e_i\big) \mid \alpha \in \mathbb{F}_q \Big\}.$$

*(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 $p|k$, 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 $U$.*

We can apply this proposition to each pair $K_i$ , $V_i$ to define $\mathbb{F}_q K_i$ -modules $U_i$ and their submodules $U_{i,0}$ and $W_i$ such that either $V_i \simeq U_{i,0}$ (for $p \nmid k$) or $V_i \simeq U_{i,0}/W_i$ (for $p|k$). Then the original action of $H$ on $V$ may be defined by 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 3.3.1 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 3.3.2.** *With the above notation, $b_V(H) \leq 2b_U(H) + 3$ for $k \geq 7$.*

*Proof.* First we define three vectors $w_1, w_2, w_3 \in U_{1.0} \oplus U_{2,0} \ldots \oplus U_{t,0}$ as linear combinations of $\{e_j^{(i)} |\ 1 \leq i \leq t,\ 1 \leq j \leq k\}$, the basis vectors of $U$, as the following.

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

Let $L = C_H(w_1, w_2, w_3)$ be the pointwise stabilizer of these three vectors in $H$. 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 vectors $u^e, u^f \in U_{1,0} \oplus U_{2,0} \oplus \ldots \oplus U_{t,0}$ as the following. Write $u = \sum_{i,j} a_{ij} e_j^{(i)}$ and define

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

The above definition of the $\beta_i$ and $\gamma_i$ 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 $L$-invariant subsets of the basis vectors that are mentioned above, 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 $\sum_i \sum_{j\leq 2} a_{ij} e_j^{(i)}$. As a consequence, every element of $C_L(u^e, u^f)$ must also fix $\sum_i \sum_{j>2} a_{ij} e_j^{(i)} + \sum_i \sum_{j\leq 2} a_{ij} e_j^{(i)} = u$. 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 $U_{1,0} \oplus U_{2,0} \oplus \ldots \oplus U_{t,0}$.

If $p \nmid k$, since $V \simeq U_{1,0} \oplus \ldots \oplus U_{t,0}$ as $\mathbb{F}_q H$-modules, we are done.

Now assume that $p|k$ 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 $1 \leq i \leq t$. For any $x \in U$, let $\bar{x} = x + W \in U/W$ be the associated element of $x$ in the factor space. 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 $1 \leq i \leq t$, so $\{z_1, \ldots, z_t\}$ is a basis for $W$. An element $g \in H$ fixes $\overline{w}_s$ (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 $\{e_j^{(i)} \,|\, 1 \leq i \leq t,\ 1 \leq j \leq k\}$ and also the subspaces $\{U_{i,0} \,|\, 1 \leq i \leq t\}$. 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 $\{e_j^{(i)} \,|\, 1 \leq j \leq k\}$. Since $k \geq 7$, this can happen only if $\lambda_i = 0$ for every $1 \leq i \leq t$, i.e. when $g$ fixes $w_s$. So $C_H(\overline{w}_s) = C_H(w_s)$ for every $s$ with $1 \leq s \leq 3$. The same argument can be applied to prove that $C_H(\overline{u}_s^f) = C_H(u_s^f)$ for every $1 \leq s \leq b$.

Finally, let us assume that $g \in C_H(\overline{w}_1, \overline{w}_2, \overline{w}_3) = L$ and $g(\overline{u}_s^e) = \overline{u}_s^e$ for some $1 \leq s \leq b$. 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 $\{e_j^{(i)} \,|\, j \neq 2,\ 1 \leq i \leq t\}$, 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. $C_L(\overline{u}_s^e) = C_L(u_s^e)$ holds. We proved that

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

as claimed. □

We can now prove Pyber's conjecture for alternating-induced groups.

**Theorem 3.3.3.** *If $H \leq GL(V)$ is an alternating-induced linear group, then*

$$b_V(H) \leq 15 + 2\frac{\log|H|}{\log|V|}.$$

*Proof.* By definition, $k \geq 7$. With using the same notation as above let $H$ act on $U$ by permuting the basis $B = \{e_j^{(i)} \mid 1 \leq i \leq t,\ 1 \leq j \leq k\}$. This action is clearly transitive, so we can use Theorem 1.2.8 to conclude that we can color the basis vectors by using at most $24\sqrt[kt]{|H|}$ colors such that only the identity of $H$ fixes this coloring, i.e. $d_B(H) \leq 24\sqrt[kt]{|H|}$. 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 Remark 2.1.7, it follows that

$$b_U(H) \leq \lceil \log_q(d_B(H)) \rceil \leq \lceil \log_q(24\sqrt[kt]{|H|}) \rceil < 6 + \frac{\log|H|}{kt\log q} = 6 + \frac{\log|H|}{\log|U|}.$$

By Lemma 3.3.2, $b_V(H) \leq 2b_U(H) + 3 \leq 15 + 2(\log|H|/\log|V|)$. □

## 3.4 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 Equation 3.2. 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 $H_i$, $\Pi$, $N$ defined in Section 3.2.

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. 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 $\Pi$ induces an action of $L$ on $\Pi$.

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 $\mathrm{Aut}(S)$.

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 $V_\Delta$ for all $h \in N_H(\Delta)$. In particular, $X_\Pi = X$ and $X_{\{V_i\}} = X_i$ holds for each $V_i \in \Pi$. Moreover, 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 $\widetilde{S_\Delta} \leq N_H(\Delta)$ be the inverse image of $S_\Delta$ 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 $S_\Delta$, which we also denote by $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$.

The next defined condition will be our additional assumption in this subsection.

**Definition 3.4.1** (Multiplicity 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 3.4.2.** *Suppose that $X$ 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 $|\Delta| \leq 2$.*

*Proof.* First note that $\Delta' \subset \Delta$ is any $H$-block, then the assumption $S_\Delta \simeq S$ implies that $S_{\Delta'} \simeq S$. For simpler notation, let us assume that $\Delta = \{V_1, \ldots, V_d\}$ for $d = |\Delta|$. By assumption, $S_\Delta$ is a diagonal subgroup of $S_1 \times \ldots \times S_d \simeq S^d$. So, $S_\Delta$ can be identified with $\{(s, s^{z_2}, \ldots, s^{z_d}) |\ s \in S\}$, where $z_2, \ldots, z_d \in \mathrm{Aut}(S)$ are fixed automorphisms. 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 $\Delta$. Using that $|\mathrm{Aut}(S) : \mathrm{IDF}(S)| \leq 2$ and the first sentence of the proof, we get that there is an $H$-block $\Delta' \subset \Delta$ such that $|\Delta'| \geq |\Delta|/2$, $S_{\Delta'} \simeq S$ 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 section let $\Delta \subseteq \Pi$ be an $H$-block. The group $S_\Delta$ is either trivial or is a subdirect product of isomorphic simple classical groups. As in Proposition 1.2.4, this means that $S_\Delta$ is a direct product of diagonal subgroups corresponding to a partition $\Delta = \cup_i \Delta_i$ of $\Delta$ into equal-size parts. Again, we call the size of the parts of this partition the linking factor of $S_\Delta$. Note that the $\Delta_i$ themselves are $H$-blocks and $S_{\Delta_i} \simeq S$ for each $i$. Hence, by Proposition 3.4.2, the linking factor of $S_\Delta$ is at most 2. As before, let $N = C_H(\Pi)$ be the kernel of the action of $H$ on $\Pi$.

Recall that $X_1 : H_1 \to \Gamma L(V_1)$ and $K_1 = \mathfrak{X}_1(H_1)$. The base size of $K_1$ is defined as in the Equation 3.1. The following result is a consequence of the Theorem 3.1.1.

**Theorem 3.4.3.** *With the above assumption, there exists a universal constant $c > 0$ such that $b_{X_1}(K_1) \leq 18 \frac{\log |K_1|}{\log |V_1|} + c$.*

Now we can prove Pyber's conjecture for such classical-induced representations.

**Theorem 3.4.4.** *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 $b_X(H) \leq 45 \frac{\log |H|}{\log |V|} + c$.*

*Proof.* Suppose that $\mathfrak{X}(N) \neq 1$. Then $\mathrm{Soc}(\mathfrak{X}(N)) = S_\Pi$ for the $H$ block $\Pi$, 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 [33, Page 18]). Therefore, by the Theorem 3.4.3 above, we have the following

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

By modifying the Theorem 3.1.3, we get $b_X(H) \leq 45 \frac{\log |H|}{\log |V|} + c$ for another universal constant $c > 0$.

From now on we assume that $\mathfrak{X}(N) = 1$. This means that $L = \mathfrak{X}(H)$ acts faithfully on $\Pi$. Let $M$ be a normal subgroup of $H$ which strictly contains $\ker(\mathfrak{X})$ such that $\mathfrak{X}(M)$ is a minimal normal subgroup of $L$ and let $\Delta$ be an orbit of $M$ on $\Pi$. 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 $M_\Delta$ is a direct product of isomorphic simple groups.

We first assume that $S_\Delta \neq 1$. Then $S_\Delta$ is a subdirect product of the non-abelian, isomorphic simple classical groups from the set $\{S_i | V_i \in \Delta\}$.

If $M_\Delta$ centralizes $S_\Delta$, 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 $\Delta$. This contradicts our multiplicity-free assumption. So we assume that $M_\Delta$ does not centralize $S_\Delta$. Since both $M_\Delta$ and $S_\Delta$ are normal subgroups in $L_\Delta$, this implies that $M_\Delta \cap S_\Delta \neq 1$. In particular $M_\Delta$ and $M_\Delta \cap S_\Delta$ are isomorphic to some powers of the (non-abelian) simple classical group $S$. Since $M_\Delta$ is transitive on $\Delta$, we have that $|\Delta| \geq 5$ and $S_\Delta$ cannot contain a nontrivial, proper $M_\Delta$-invariant normal subgroup. But $M_\Delta \cap S_\Delta \neq 1$ is normal in both $M_\Delta$ and $S_\Delta$. Since any subnormal subgroup of $M_\Delta$ is normal in $M_\Delta$, we get that $S_\Delta$ is simple, so $S_\Delta \simeq S$ has linking factor $|\Delta| \geq 5$. This contradicts with 3.4.2.

Now only the case where $S_\Delta = 1$ is left. Then $L_\Delta$ and $M_\Delta$ act faithfully and transitively on $\Delta$. Moreover $M_\Delta$ is a normal subgroup of $L_\Delta$ and it is isomorphic to a direct product of isomorphic simple groups. By Theorem 1.2.7 $d_\Delta(L_\Delta) \leq 8$ or $\mathrm{Alt}(\Delta) \leq L_\Delta \leq \mathrm{Sym}(\Delta)$.

If $d_\Delta \leq 9$, then by Remark 2.1.7 $b_{P(\Delta)}(L_\Delta) \leq 3$, and so $b_{V_\Delta}(L_\Delta) \leq 3$ (any subset of $\Delta$ can be represented by a vector in $V_\Delta$ whose projection to $V_i \in \Delta$ is non-zero if and only if $V_i$ is an element of the subset). Thus, $b_{X_\Delta}(N_H(\Delta)) \leq b_{V_\Delta}(L_\Delta) + b_{V_\Delta}(T_{V_\Delta}) \leq 4$. If we apply Theorem 3.1.3 for $V_\Delta$ instead of $V_1$ we get the following

$$b_X(H) \leq b_{X_\Delta}(N_H(\Delta)) + 1 + \log 24 + \frac{\log|P|}{\log|V|} \leq \frac{\log|H|}{\log|V|} + 10.$$

If $d_\Delta(L_\Delta) > 9$, then $m := |\Delta| \geq 9$ and $\mathrm{Alt}(\Delta) \leq L_\Delta \leq \mathrm{Sym}(\Delta)$. In this case for any $V_i \in \Delta$, either $\mathfrak{X}_\Delta(H_i) \simeq \mathrm{Alt}([m-1])$ or $\mathfrak{X}_\Delta(H_i) \simeq \mathrm{Sym}([m-1])$ must hold. But this is a contradiction since $S_i$ is composition factor of $\mathfrak{X}_\Delta(H_i)$ ant it is a simple classical group. □



## 3.5 Eliminating Small Tensor Product Factors From the $\mathbf{K}_i$

In this section we will reduce the affine case to the case where 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. So we will reduce the affine case to the case where the action of $H$ is alternating-induced or multiplicity-free classical-induced. This will close the affine case since bounds for these types were proven in the previous two subsections.

**Lemma 3.5.1.** *Let $L$ be a finite group and let $W$ 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 $W$. Set $b := \lceil b'/l \rceil$ and denote the vectors

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

The set $\{y_1, y_2, \ldots, y_b\}$ 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 3.5.2.** *With the above notation we have $b_X(H) \leq \lceil b_Y(H)/l \rceil + 4$.*

*Proof.* We use the construction of Liebeck and Shalev (see the proof of [51, 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

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

Additionally, for some generator $\alpha$ of $\mathbb{F}_q^\times$ and for each $1 \leq i \leq t$, let $v_4^{(i)} = \alpha v_1^{(i)}$. Let $v_j = \sum_{i=1}^{t} v_j^{(i)}$ for $j \in \{1, 2, 3, 4\}$ and $L := C_H(v_1, v_2, v_3, v_4)$. The choice of $v_1^{(i)}$ and $v_4^{(i)}$ guarantees that $X_i(L \cap H_i) \subset GL(U_i) \otimes GL(W_i)$ for each $i$. So, by the displayed formula above $X_i(L \cap H_i) \subset id_{U_i} \otimes GL(W_i)$. Therefore, 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 $\Pi$, $V_{\Delta_j} = \oplus_{V_i \in \Delta_j} V_i$ and $W_{\Delta_j} = \oplus_{V_i \in \Delta_j} W_i$ for every $1 \leq i \leq s$. Then $V_{\Delta_j}$'s are $X(L)$-invariant, meaning 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 $V_{\Delta_j}$. We 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 $V_\alpha \in \Delta_j$ is arbitrary, then $X_{\Delta_j} = \mathrm{Ind}_{L\cap H_\alpha}^{L}(X_\alpha)$ and $Y_{\Delta_j} = \mathrm{Ind}_{L\cap H_\alpha}^{L}(Y_\alpha)$. Since $X_\alpha$ on $L$ is projectively equivalent to the $l$ multiple of $Y_\alpha$ on $L$, and induction of representations preserves multiplicity, we get that $X_{\Delta_j}$ is $\pmod{T_V}$-equivalent to the $l$ multiple of $Y_{\Delta_j}$ on $L$ for every $1 \leq j \leq s$. So, $X = \oplus_{j=1}^{s} X_{\Delta_j}$ is $\pmod{T_V}$-equivalent to the $l$ multiple of $Y$ on $L$. By Lemma 3.5.1, we get that $b_X(L) = \lceil b_Y(L)/l \rceil$. Since $b_X(H) \leq b_X(L) + 4$ and $b_Y(L) \leq b_Y(H)$ hold trivially, the result follows. □

**Corollary 3.5.3.** *With the same notation, if $b_Y(H) \leq c_1 \cdot \frac{\log|H|}{\log|W|} + c_2$ for some constants $c_1$ and $c_2 \geq 10$, then $b_X(H) \leq c_1 \cdot \frac{\log|H|}{\log|V|} + c_2$.*

*Proof.* By Lemma 3.5.2 and by the assumption

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

□

Since Theorem 3.1.3 gives a bound for the base size where $K_1 \leq GL(V_1) \simeq GL(k,p)$ has a bounded base, $K_1$ is a primitive irreducible linear group with unbounded base size.

Primitive groups of unbounded base size were characterized by Liebeck and Shalev in [52, Theorem 1, Proposition 2]. In the following, we collect some of these properties in a form which will be most convenient for our use. In these papers, the authors stated their theorems 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.

We use some notation which are mostly taken from [32]. Let $U = U_k(p)$ be a vector space of dimension $k$ over $\mathbb{F}_p$. Let $H \leq GL(U_k(p))$ 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 $H \leq \Gamma L(U_{k/f}(q)) \leq GL(U_k(p))$.

If $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$, then $\mathrm{Cl}(r, q_0) \leq GL(U_k(p))$ denotes a classical linear group over $\mathbb{F}_{q_0}$ for some subfield $\mathbb{F}_{q_0} \leq \mathbb{F}_q$ and for some $r \geq 9$. (This lower bound on $r$ is assumed because we want to apply the result of Section 3.4.)

**Theorem 3.5.4** (Liebeck, Shalev [51],[53])**.** *Let $H \leq GL(U_k(p))$ be a primitive linear group of unbounded base size and $q = p^f$ be maximal such that $H \leq \Gamma L(U_{k/f}(q))$. Then there is a tensor product decomposition $U = U_1 \otimes U_2$ over $\mathbb{F}_q$ such that $1 \leq \dim(U_1) < \dim(U_2)$ and $H$ preserves this tensor product decomposition, that is, $H \leq N_{\Gamma L(U_{k/f}(q))}(GL(U_1) \otimes GL(U_2))$. 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 $H_2^0 := \{b \in GL(U_2) \mid \exists a \in GL(U_1) : a \otimes b \in H^0\}$. 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 $p|m$, 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 $r = \dim_{\mathbb{F}_q}(U_2)$.*

Now we apply this theorem 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 3.5.4. 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 $T_V \simeq \mathbb{F}_q^\times$.

Now we can prove Pyber's conjecture for affine groups. The following theorem proves a more general statement for $\pmod{T_V}$-representations. To get the original statement, take an irreducible imprimitive linear group $H \leq GL(V)$ with the identity.

**Theorem 3.5.5.** *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 3.1.1, we may assume that $V$ is an imprimitive $X(H)T_V$-module, i.e. $t > 1$.

We use induction on the dimension of $V_1$. Note that if $\dim(V_i)$ is bounded (or, more generally, if $b_{X_1}(H_1)$ is bounded), then the result follows from Theorem 3.1.3.

By our assumption, $X_1(H_1)Z(GL(V_1)) \leq \Gamma L(V_1)$ is a primitive semilinear group, so Theorem 3.5.4 can be applied. Thus, an $\mathbb{F}_q$ vector space structure can be defined on each $V_i$ (where $\mathbb{F}_q$ is a (not necessarily 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 $(\mathrm{mod}\ T_W)$-representation for $W = \oplus_{i=1}^t W_i$ defined in the paragraph before Lemma 3.5.2, 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 3.5.3.

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 3.5.4, 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 $b_{X'}(H) \leq 2(\log|H|/\log|W|) + 15$ by Theorem 3.3.3. Finally, $b_X(H) \leq b_{X'}(H)$ by Lemma 3.5.2 and $|W| = |V|$, so $b_X(H) \leq 2(\log|H|/\log|V|) + 19$ and we are done.

From now on, we may assume that $X_1(H_1)Z(GL(V_1))$ satisfies the second part of Theorem 3.5.4, where $X$ is classical induced. In order to use Theorem 3.4.4, we should reduce it to satisfy the multiplicity-free condition. For this let $\Delta \subset \Pi$ 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 $\Delta = \{V_1, V_2, \ldots, V_s\}$ with $s = |\Delta| > 1$ and $k = \dim V_1$. Let $X_\Delta : N_H(\Delta) \to GL(V_\Delta(p))$ be the $(\mathrm{mod}\ T_{V_\Delta})$-representation defined by the restriction of $X$ (where $T_{V_\Delta}$ 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 $U_\Delta$ be an $s$-dimensional vector space over $\mathbb{F}_q$ with fixed basis $f_1, \ldots, f_s$ and let $W_\Delta$ be a $k$-dimensional vector space over $\mathbb{F}_q$ with fixed basis $e_1, \ldots, e_k$. Furthermore, let $\{b_1, \ldots, b_k\}$ 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, $\{\varphi_i(b_j) | 1 \leq i \leq s, 1 \leq j \leq k\}$ is a basis of $V_\Delta$. 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 $V_\Delta$ and $U_\Delta \otimes W_\Delta$ via $\Phi$, we get that for any $h \in \widetilde{S_\Delta}$, the matrix form of $X_\Delta(h)$ with respect to the basis $\{f_1 \otimes e_1, f_1 \otimes e_2, \ldots, f_s \otimes e_k\}$ is the Kronecker product of matrices $D(h) \otimes A(h)$ where is the matrix form of $X_1(h)$ with respect to the basis $\{b_1, \ldots, b_k\}$ while $D(h)$ is the diagonal matrix with entries $\lambda_1(h), \ldots, \lambda_s(h)$ in its main diagonal. Since $X_\Delta(\widetilde{S_\Delta})$ is normalized by $X_\Delta(N_H(\Delta))$, we can apply [44, 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 $X_\Delta$ 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 $\Delta$. Furthermore, let $U := \oplus_i U_{\Delta_i}$, $W := \oplus_i W_{\Delta_i}$, where $\{\Delta = \Delta_1, \ldots, \Delta_{t/|\Delta|}\}$ is the orbit of $\Delta$ under the action of $H$ on the power set of $\Pi$. 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 Theorem 3.1.3 where $b = 1$, so we get $b_X(H) \leq \frac{\log|H|}{\log|V|} + 10$ by Corollary 3.5.3.

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 3.4.4 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 3.5.3 again, we get that $b_X(H) \leq 45\frac{\log|H|}{\log|V|} + c$ holds. □

# Chapter 4

# Random Bases For Coprime Linear Groups

## 4.1 Introduction

Let $V$ be a finite vector space. A linear group $G \leq GL(V)$ is called coprime if $(|G|, |V|) = 1$. Gluck and Magaard [30] proved that if $G$ is a coprime linear group then $b(G) \leq 94$. In [36] Halasi and Podoski improved this result by showing that the minimal base size of a coprime linear group is bounded by 2 and moreover this bound is sharp. Burness, Liebeck and Shalev [12] proved that if $G$ is a finite almost simple group in a primitive faithful non-standard action then $b(G) \leq 7$ (with equality if and only if $G$ is a Mathieu group $M_{24}$ in its natural action of degree 24). Moreover, they showed that if $G$ is a finite almost simple group, and $\Omega$ is a primitive non-standard $G$-set then the probability that a random 6-tuple in $\Omega$ is a base for $G$ tends to 1 as $|\Omega| \to \infty$. Based on this random base result and the bound estimated by Halasi and Podoski, Pyber [60] asked the following question: If $G \leq GL(V)$ is a coprime linear group, is there an absolute constant $c$ such that the probability of a random $c$-tuple in $V$ being a base for $G$ tends to 1 as $|V| \to \infty$.

In our joint paper with Halasi and Podoski * we answered this question affirmatively by showing that if $G$ is a coprime primitive linear group then the probability that a random 11-tuple in $V$ is a base for $G$ tends to 1 as $|V| \to \infty$. In this chapter we deal with this question and our answer to it.

For any positive integer $c$ let us define the probability

$$Pb(c, G, V) := P(\text{random } v_1, \ldots, v_c \in V \text{ is a base for } G).$$

**Remark 4.1.1.** Let $V$ be an $n$-dimensional vector space over the finite field $\mathbb{F}_q$.

(1) Let $Z = Z(GL(V)) \simeq \mathbb{F}_q^\times$ denote the group of scalar transformations on $V$. If $G \leq GL(V)$ is a coprime linear group on $V$, then so is $GZ \geq G$ and we have $Pb(c, G, V) \geq Pb(c, GZ, V)$. Therefore, for the rest of this paper we will always assume that $G$ contains $Z$.

(2) The assumption "primitive" is necessary here. To see this, let $H \leq GL(n, q)$ be the group of all invertible diagonal matrices, so $H \simeq (\mathbb{F}_q^\times)^n$. Then $v_1, \ldots, v_c \in \mathbb{F}_q^n$

is a base for $H$ if and only if for each $1 \leq i \leq n$ the $i$-th component of some $v_j$ is non-zero. For any fixed $i$, this has probability $(1 - 1/q^c)$, so we have

$$Pb(c, H, \mathbb{F}_q^n) = \left(1 - \frac{1}{q^c}\right)^n,$$

which is close to zero for any fixed $c$ and big enough $n$. If $(q, n) = 1$, then one can add the regular permutation action of $C_n$ on the components of $\mathbb{F}_q^n$ to get the coprime irreducible linear group $G = H \rtimes C_n \leq GL(n, q)$ satisfying $\lim_{n\to\infty} Pb(c, G, \mathbb{F}_q^n) = 0$.

## 4.2 Bounds on $Pb(c, G, V)$ in Terms of Supports and Character Ratios

**Definition 4.2.1.** For a linear group $G \leq GL(V)$ and a $g \in G$ the *fixed-point space* and the *support* of $g$ are defined as

$$\mathrm{Fix}(g) := \{v \in V \mid g(v) = v\} \quad \text{and} \quad \mathrm{Supp}(g) := \dim(V) - \dim(\mathrm{Fix}(g)).$$

Furthermore, let the *minimum support* of $G$ be defined as

$$\mathrm{MinSupp}(G) := \min_{1 \neq g \in G} \mathrm{Supp}(g).$$

We use the notation $\mathrm{Fix}_V(g), \mathrm{Supp}_V(g)$ and $\mathrm{MinSupp}_V(G)$ if we also want to highlight the vector space on which the group acts.

Let $Z = Z(GL(V)) \simeq \mathbb{F}_q^\times$ denote the group of scalar transformations on $V$.

**Remark 4.2.2.** If $G$ strictly contains $Z$, then $\mathrm{MinSupp}(G)$ equals

$$\min_{g \in G \setminus Z} \big(\dim(V) - \max_{\lambda \in \mathbb{F}_q^\times}(\dim(\ker(g - \lambda \cdot \mathrm{id}_V)))\big).$$

In order to get bounds for $\mathrm{MinSupp}_V(G)$ in case of $G \leq GL(V)$ is a quasisimple coprime linear group, we will use results from character ratios of complex irreducible characters of such groups.

**Definition 4.2.3.** For a finite group $G$ and $\chi \in \mathrm{Irr}(G)$ with $\chi(1) \neq 1$ let us define the *maximal character ratios*

$$\mathrm{mr}(G, \chi) := \max_{g \notin Z(\chi)} \frac{|\chi(g)|}{\chi(1)} \quad \text{and} \quad \mathrm{mr}(G) := \max_{\chi \in \mathrm{Irr}(G),\, \chi(1) \neq 1} \mathrm{mr}(G, \chi).$$

Clearly, $\mathrm{mr}(G) < 1$ for every finite group $G$.

The connection between minimal support and maximal character ratio is described in the following Lemma.

**Lemma 4.2.4.** *Let $V$ be an $n$-dimensional vector space over the finite field $\mathbb{F}_q$ and let $G \leq GL(V)$ be a non-Abelian coprime irreducible linear group. Then we have*

$$\mathrm{MinSupp}_V(G) \geq \frac{\dim(V)}{2}\Big(1 - \mathrm{mr}(G)\Big).$$

*Moreover, if $\chi \in \mathrm{Irr}(G)$ is any irreducible component of the Brauer character associated to $V$, then*

$$\mathrm{MinSupp}_V(G) \geq \frac{1}{2}\Big(\chi(1) - \max_{g \notin Z(\chi)} |\chi(g)|\Big).$$

*Proof.* Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$ and let $\overline{V} = V \otimes \overline{\mathbb{F}}_q$ be the $\overline{\mathbb{F}}_q G$-module arising from the $\mathbb{F}_q G$-module $V$. Let $\overline{V} = V_1 \oplus \ldots \oplus V_t$ be the decomposition of $\overline{V}$ into irreducible $\overline{\mathbb{F}}_q G$-modules. Then the corresponding representations $G \mapsto GL(V_i)$ form a single Galois conjugacy class by [38, Theorem 9.21], so $\mathrm{Supp}_{V_i}(g) = \frac{1}{t}\mathrm{Supp}_V(g)$ holds for every $g \in G$. Let $\chi_i : G \mapsto \mathbb{C}$ be the irreducible Brauer character associated to $V_i$ for each $1 \leq i \leq t$. Since $(q, |G|) = 1$, we get $\chi_i \in \mathrm{Irr}(G)$ by [38, Theorem 15.13]. Furthermore,

$$\chi_i(1) = \dim(V_i) \quad \text{and} \quad [\chi_i\langle g\rangle, 1_{\langle g\rangle}] = \dim(\mathrm{Fix}_{V_i}(g)).$$

For any $g \in G$ we have $\chi_1(g) = (\chi_1(1) - k)\cdot 1 + \varepsilon_1 + \ldots + \varepsilon_k$ where $k = \mathrm{Supp}_{V_1}(g)$ and $\varepsilon_1, \ldots, \varepsilon_k$ are $o(g)$-th root of unity. Then $|\chi_1(g)| \geq \chi_1(1) - 2k = \chi_1(1) - 2\,\mathrm{Supp}_{V_1}(g)$ holds, so $2\,\mathrm{MinSupp}_{V_1}(G) \geq \chi_1(1) - \max_{g \notin Z(\chi_1)} |\chi_1(g)|$. (Note that the assumption that $G$ is non-Abelian implies that the $\chi_i$ are non-linear characters. Furthemore, if $1 \neq g \in Z(\chi_1)$, then $\mathrm{Supp}_V(g) = \dim(V)$, so $\mathrm{MinSupp}_V(G) = \min_{g \notin Z(\chi_1)} \mathrm{Supp}_V(g)$ must hold.) It follows that

$$\begin{aligned} 2\,\mathrm{MinSupp}_V(G) &= 2t\,\mathrm{MinSupp}_{V_1}(G) \geq t(\chi_1(1) - \max_{g \notin Z(\chi_1)} |\chi_1(g)|) \\ &= t\chi_1(1)(1 - \mathrm{mr}(G, \chi_1)) \geq \dim(V)(1 - \mathrm{mr}(G)). \end{aligned}$$

Now, the first inequality proves the second claim, while the second inequality proves the first claim. □

**Lemma 4.2.5.**

$$Pb(c, G, V) \geq 1 - \sum_{1 \neq g \in G} \frac{1}{q^{c\cdot \mathrm{Supp}(g)}} \geq 1 - \frac{|G|}{q^{c\cdot \mathrm{MinSupp}(G)}} \geq 1 - \frac{1}{|V|^{c(1-\mathrm{mr}(G))/2-2}}.$$

*In particular, $Pb(c, G, V) \geq 1 - \frac{1}{|V|^{\varepsilon}}$ for $c \geq \frac{4+2\varepsilon}{1-\mathrm{mr}(G)}$.*

*Proof.*

$$\begin{aligned} P(\{v_1, \ldots, v_c\} \subseteq V \text{ is not a base for } G) &\leq \sum_{1 \neq g \in G} P(g(v_i) = v_i,\ \forall\, 1 \leq i \leq c) \\ &= \sum_{1 \neq g \in G} \left(\frac{|\,\mathrm{Fix}(g)|}{|V|}\right)^c = \sum_{1 \neq g \in G} \frac{1}{q^{c\cdot \mathrm{Supp}(g)}} \leq \frac{|G|}{q^{c\cdot \mathrm{MinSupp}(G)}} \\ &\leq \frac{|V|^2}{(q^n)^{c(1-\mathrm{mr}(G))/2}} = \frac{1}{|V|^{c(1-\mathrm{mr}(G))/2-2}}, \end{aligned}$$

and the claim follows. □

## 4.3 Bounds for Character Ratios and for Minimal Supports of Quasisimple Linear Groups

The goal of this section is to give lower bounds for minimal supports of coprime quasisimple groups $G \leq GL(V)$ in terms of $|G|$ and $\dim(V)$.

First we handle the case when $G$ is a sporadic group or a finite quasisimple group of Lie type. For such groups, we use bounds for their maximal character ratios $\mathrm{mr}(G)$.

**Theorem 4.3.1.** *Let $G$ be a finite quasisimple group such that $G/Z(G)$ is not an alternating group.*

*(1) If $G/Z(G)$ is a sporadic simple group, then $\mathrm{mr}(G) < 0.54$.*

*(2) If $G = G(r)$ is a finite quasisimple group of Lie type over the field $\mathbb{F}_r$, then*

$$\mathrm{mr}(G) \leq \begin{cases} \max\left(\frac{1}{\sqrt{r}-1}, \frac{9}{r}\right) & \text{if } r > 9; \\ \frac{19}{20} & \text{if } r \leq 9. \end{cases}$$

*Proof.* We checked part (1) for the covering groups of the sporadic simple groups by using the GAP [68] Character table library and also the undeposited GAP package FUtil to turn cyclotomic complex numbers into floating ones in order to be able to compare the values of $|\chi(g)|$ for various $g$ and $\chi$.

Regarding part (2), it is a simplified version of a result of Gluck [29]. (For a summary of his results, see also [48, Theorem 2.4]). □

**Remark 4.3.2.** For simple groups of alternating type there is no general upper bound for $\mathrm{mr}(G)$ smaller than 1. Moreover it can be shown that for every $\varepsilon > 0$, the number of irreducible characters $\chi \in \mathrm{Irr}(S_m)$ (or $\chi \in \mathrm{Irr}(A_m)$) satisfying $\mathrm{mr}(S_m, \chi) > 1 - \varepsilon$ is not bounded if $m$ is large enough.

**Corollary 4.3.3.** *Let $V$ be a vector space over the finite field $\mathbb{F}_q$ and let $G = Z \cdot G_0 \leq GL(V)$ where $G_0$ is a coprime quasisimple irreducible linear group which is not of alternating type. Then $\mathrm{MinSupp}_V(G) \geq \frac{1}{40}\dim(V)$.*

*Proof.* By Theorem 4.3.1, we have $\mathrm{mr}(G) = \mathrm{mr}(G_0) \leq \frac{19}{20}$, so the claim follows from Lemma 4.2.4. □

Now, we handle the case when $\mathrm{Soc}(G/Z(G))$ is an alternating group.

**Theorem 4.3.4.** *Let $G = S_m$ and $\chi = \chi^{(\lambda)} \in \mathrm{Irr}(G)$ corresponding to the partition $\lambda = (\lambda_1 \geq \ldots \geq \lambda_k)$ of $[m]$. Then $\chi^\lambda(1) - \chi^\lambda((123)) \geq \frac{1}{m-1}\chi^\lambda(1)$ unless*

$$\lambda \in \{(m);\ (1, \ldots, 1)\}.$$

*Proof.* First, we introduce some notation. Let $\lambda = (\lambda_1 \geq \ldots \geq \lambda_k)$ be a partition of $m$, different from the two exceptional ones given in the theorem. For any natural numbers $i_1, \ldots, i_k$ let $\chi^{\lambda - \{i_1, \ldots, i_k\}}$ be the character of $S_{m-k}$ corresponding to the Young diagram obtained from the diagram of $\lambda$ by deleting the last cells of the $i_1$-th,...,$i_k$-th row in

that order with the assumption that $\lambda - \{i_1, \dots, i_s\}$ is a valid Young diagram for each $1 \leq s \leq k$. Otherwise, we define $\chi^{\lambda - \{i_1,\dots,i_k\}}$ as the constant zero function on $S_{m-k}$.

By the Murnaghan-Nakayama rule (see [41, 21.1]),

$$\begin{aligned}\chi^\lambda((123)) &\leq \sum_{\nu \in \{\lambda - rh(3)\}} \chi^\nu(1) + \sum_{\nu \in \{\lambda - rh(1,1,1)\}} \chi^\nu(1) \\ &= \sum_{\nu \in \{\lambda - rh(3)\}} \chi^\nu(1) + \sum_{\nu \in \{\overline{\lambda} - rh(3)\}} \chi^\nu(1)\end{aligned}$$

where $\{\lambda - rh(*)\}$ denotes the set of partitions of $m-3$ which we can get from the Young-diagram of $\lambda$ be removing a rim 3-hook of type $(*)$ such that the remaining cells form a valid Young diagram.

On the other hand, by using the branching rule (three times) one gets

$$\chi^\lambda(1) = \sum_{i,j,k} \chi^{\lambda - \{i,j,k\}}(1).$$

Let $\nu \in \{\lambda - rh(3)\}$. Then $\nu = \lambda - \{i,i,i\}$ for some (unique) $i$. Now, there is a $j \neq i$ such that $\tau = \lambda - \{i,i,j\}$ is a valid Young diagram. Then both induced characters $(\chi^\tau)^{S_{m-2}}$ and $(\chi^\nu)^{S_{m-2}}$ contain $\chi^{\lambda-\{i,i\}}$ as a component which results $\chi^\nu(1) \leq \chi^{\lambda-\{i,i\}}(1) \leq (m-2)\chi^\tau(1)$. The same argument can be applied to any $\nu \in \{\overline{\lambda} - rh(3)\}$. It follows that

$$\begin{aligned}\chi^\lambda(1) &\geq \sum_i \chi^{\lambda-\{i,i,i\}}(1)\Big(1 + \frac{1}{m-2}\Big) + \sum_i \chi^{\overline{\lambda}-\{i,i,i\}}(1)\Big(1 + \frac{1}{m-2}\Big) \\ &\geq \frac{m-1}{m-2}\chi^\lambda((123)).\end{aligned}$$

Hence $\chi^\lambda(1) - \chi^\lambda((123)) \geq \frac{1}{m-1}\chi^\lambda(1)$ which proves the claim. □

This result will be adequate for our purposes only if the degree of $\chi$ is large enough. In order to get an overall picture about the form of Young diagrams defining characters of small degree, we will use a result of Rasala [61]. In what follows, we use the terminology from Rasala's paper. For any partition $\lambda$ of $m$, let $|\lambda| = m$ be the order of $\lambda$ and let $\lambda^*$ be the partition dual to $\lambda$. The partition $\lambda$ is called primary, if $\lambda \geq \lambda^*$, where $\geq$ denotes the standard ordering on partitions. If $\lambda = (\lambda_1 \geq \ldots \geq \lambda_k)$ is a partition of $k$ and $m \geq \lambda_1 + k$, then let $m/\lambda$ denote the partition of $m$ defined as $m/\lambda = (m - k \geq \lambda_1 \geq \ldots \geq \lambda_k)$ and let $\varphi_\lambda(m) := \chi^{m/\lambda}(1)$ be the degree of the character of $S_m$ associated to $m/\lambda$. (Note that $\varphi_\lambda(m)$ is a polynomial in $m$ by [61, Theorem A].) For any set $P$ of partitions of $k$ and for $m$ large enough, let $L(P,m) := \{\varphi_\lambda(m) \mid \lambda \in P\}$ and let $\delta(P,m)$ be the largest degree in $L(P,m)$. Then $P$ is said to be $m$-minimal, if for every primary partition $\mu$ of $m$ either $\chi^\mu(1) > \delta(L,P)$ or $\mu = m/\lambda$ for some $\lambda \in P$.

By [61, Main Theorem 1.] (for $k = 3$) we have

**Theorem 4.3.5.** *Let $P_3$ be the set of all partitions of order at most 3, that is, $P_3 = \{\emptyset; (1); (2); (1,1); (3); (2,1); (1,1,1)\}$. Then $P_3$ is $m$-minimal for every $m \geq 15$.*

Thus, by using the hook length formula and the Murnaghan-Nakayama rule we can calculate the exact values of $\chi^\lambda(1)$ and $\chi^\lambda((123))$ when $\chi^\lambda(1)$ is among the first seven

smallest character degrees of $S_m$ for $m \geq 15$. Otherwise, we get a reasonably large lower bound for $\chi^\lambda(1)$. (Note that $\lambda$ or $\lambda^*$ is primary and $\chi^\lambda(1) = \chi^{\lambda^*}(1)$, $\chi^\lambda((123)) = \chi^{\lambda^*}((123))$ holds for every partition $\lambda$ of $m$.)

**Corollary 4.3.6.** *Let $\lambda$ be a partition of $m$ for $m \geq 15$ and let $\chi^\lambda \in \mathrm{Irr}(S_m)$ be the character of $S_m$ associated to $\lambda$. Then $\chi^\lambda(1)$ and $\chi^\lambda((123))$ are as given in Table 4.1 or*

| $\lambda$ or $\lambda^*$ | $\chi^\lambda(1) = \chi^{\lambda^*}(1)$ | $\chi^\lambda((123)) = \chi^{\lambda^*}((123))$ |
|---|---|---|
| $(m)$ | $1$ | $1$ |
| $(m-1,1)$ | $m-1$ | $m-4$ |
| $(m-2,2)$ | $\frac{1}{2}m(m-3)$ | $\frac{1}{2}(m-3)(m-6)$ |
| $(m-2,1,1)$ | $\frac{1}{2}(m-1)(m-2)$ | $\frac{1}{2}(m-4)(m-5)$ |
| $(m-3,3)$ | $\frac{1}{6}m(m-1)(m-5)$ | $\frac{1}{6}(m-3)(m-4)(m-8)+1$ |
| $(m-3,2,1)$ | $\frac{1}{3}m(m-2)(m-4)$ | $\frac{1}{3}(m-3)(m-5)(m-7)-1$ |
| $(m-3,1,1,1)$ | $\frac{1}{6}(m-1)(m-2)(m-3)$ | $\frac{1}{6}(m-4)(m-5)(m-6)+1$ |

Table 4.1: Character values of $S_m$ when the degree is small.

$\chi^\lambda(1) > \frac{1}{3}m(m-2)(m-4)$.

Now, we give an analogue of Corollary 4.3.3 for alternating-type groups.

**Corollary 4.3.7.** *Let $V$ be a vector space over the finite field $\mathbb{F}_q$ and let $G = Z \cdot G_0 \leq GL(V)$ where $G_0$ is a coprime irreducible linear group and $G_0/Z(G_0) \simeq A_m$ for some $m \geq 5$. Let us assume that $V$ is not a component of the natural permutation $\mathbb{F}_qA_m$-module. Then* $\mathrm{MinSupp}_V(G) \geq \frac{1}{16}\sqrt{\dim(V)}$.

*Proof.* As in the proof of Lemma 4.2.4, $\mathrm{MinSupp}_V(G) = t \cdot \mathrm{MinSupp}_{V_1}(G)$ and $\dim(V) = t \cdot \dim(V_1)$ where $V_1$ is an (absolutely) irreducible component of $\overline{\mathbb{F}}_qG$-module $V \otimes \overline{\mathbb{F}}_q$. Then the claim clearly follows if we prove that $\mathrm{MinSupp}_{V_1}(G) \geq \frac{1}{16}\sqrt{\dim(V_1)}$. In other words, we can assume that $V$ is absolutely irreducible. First let us assume that $G_0 \simeq A_m$ for some $m \geq 9$. Let $\varphi \in \mathrm{Irr}(A_m)$ be the Brauer character associated to $V$ and $\chi \in \mathrm{Irr}(S_m)$ above $\varphi$, i.e. $[\chi_{A_m}, \varphi] \neq 0$. Then either $\chi_{A_m} = \varphi$ (if $\chi$ is not self-dual) or $\chi_{A_m} = \varphi + \varphi^{(12)}$ (if $\chi$ is self-dual). In the latter case $\varphi((123)) = \chi((123))/2$, since the conjugacy class $(123)^{S_m}$ does not split in $A_m$. Let $\epsilon$ be 1 or 1/2 according to these cases, so $\varphi(1) = \epsilon\chi(1)$ and $\varphi((123)) = \epsilon\chi((123))$. By [61, Result 2.], we have $\dim(V) = \epsilon\chi(1) \geq \frac{1}{2}m(m-3)$. If $\varphi((123)) < 0$, then $\mathrm{Supp}_V((123)) \geq \frac{1}{2}\dim(V) \geq \frac{1}{4}\sqrt{\dim(V)}$ holds trivially. Otherwise, by using Lemma 4.2.4 and Theorem 4.3.4 we get that

$$\mathrm{Supp}_V((123)) \geq \frac{1}{2}(\varphi(1) - |\varphi((123))|) = \frac{\epsilon}{2}(\chi(1) - \chi((123))) = \frac{\epsilon\chi(1)}{2(m-1)}$$
$$= \frac{\dim(V)}{2(m-1)} \geq \frac{\sqrt{m(m-3)/2}\sqrt{\dim(V)}}{2(m-1)} \geq \frac{1}{4}\sqrt{\dim(V)}.$$

For any element $1 \neq g \in A_m$ there are $x, y \in A_m$ such that $[g, x, y]$ is a three-cycle. Applying Lemma 4.4.3 twice, we get that $\mathrm{Supp}_V(g) \geq \frac{1}{4}\mathrm{Supp}_V((123)) \geq \frac{1}{16}\sqrt{\dim(V)}$. Now, let us assume that $m > 7$ and $G_0$ is the universal covering group of $A_m$, so $G_0 \simeq 2.A_m$. Let $z \in G_0$ be the generator of $Z(G_0) \simeq C_2$ and let $\bar{g} \in A_m$ denote the image of any $g \in G_0$ under the natural surjection by $G_0 \mapsto A_m$. Then $z$ acts on $V$ as a scalar transformation $z(v) = -v$ for all $v \in V$, so $\mathrm{Supp}_V(z) = \dim(V)$. Let $t \in G_0$ such that $\bar{t} = (12)(34)$. By Theorem [37, Theorem 3.9], $t$ and $tz$ are conjugate, so $z = [h, t]$ for some $h \in G_0$. It follows that $\mathrm{Supp}_V(t) \geq \frac{1}{2}\mathrm{Supp}_V(z) = \frac{\dim(V)}{2}$ by Lemma 4.4.3. (In fact, by using this argument to $tz$ instead of $t$ one can prove equality here.) Now, for any $g \in G_0 \setminus Z$ one can choose $x, y \in G$ such that $[\bar{g}, \bar{x}, \bar{y}]$ is conjugate to $\bar{t}$. Using again Lemma 4.4.3 twice, we get that $\mathrm{Supp}_V(g) \geq \frac{1}{4}\mathrm{Supp}_V(t) = \frac{1}{8}\dim(V) \geq \frac{1}{16}\sqrt{\dim(V)}$.

For the remaining cases, $\dim(V) \leq \sqrt{|G_0|} < 16^2$, so $\frac{1}{16}\sqrt{\dim(V)} < 1 \leq \mathrm{MinSupp}_V(G)$ follows. □

The next result gives a bound to the order of most coprime quasisimple linear groups similar to that of $|G| \leq |V|^2 = q^{2\dim(V)}$ but using the minimal support $\mathrm{MinSupp}_V(G)$ instead of $\dim(V)$.

**Theorem 4.3.8.** *Let $V$ be a vector space over the finite field $\mathbb{F}_q$ and let $G = Z \cdot G_0 \leq GL(V)$ where $G_0$ is a coprime quasisimple irreducible linear group.*

*Then one of the following holds:*

*(1)* $\log_q |G| \leq d \cdot \mathrm{MinSupp}_V(G)$ *with* $d = 5$.

*(2)* $G_0 \simeq A_m$ *and $V$ is the non-trivial irreducible component of the natural permutation module of $A_m$ over $\mathbb{F}_q$.*

*(3)* $G_0 = G_0(r)$ *is a finite quasisimple group of Lie type over the finite field $\mathbb{F}_r$ with $r \leq 43$, and $|V|$ is bounded by an absolute constant.*

*Proof.* For any sporadic group $S$, let $\widehat{S}$ be its universal covering group and let $q(S)$ be the smallest prime not dividing the order of $S$. By using GAP [68], we checked that for every $\chi \in \mathrm{Irr}(\widehat{S})$, the inequlity

$$\log_{q(S)} |\widehat{S}| < d \cdot (\chi(1) - \max_{g \in \widehat{S} - Z(\chi)} |\chi(g)|)/2$$

holds with $d > 4.22$. (The largest value is attained for $2.J_2$.) Now, if $G \leq GL(V)$ is any finite quasisimple group with sporadic simple quotient $S = G/Z(G)$, then $G$ is a homomorphic image of $\widehat{S}$, and we can view $V$ as an irreducible $\mathbb{F}_q\widehat{S}$-module (where $q \geq q(S)$). Now, if $\chi \in \mathrm{Irr}(\widehat{S})$ is any irreducible component of the Brauer character corresponding to $V \otimes \overline{\mathbb{F}}_q$, then

$$\begin{aligned} \log_q |G| \leq \log_{q(S)} |\widehat{S}| &< d \cdot (\chi(1) - \max_{g \in \widehat{S} - Z(\chi)} |\chi(g)|)/2 \\ &\leq d \cdot \mathrm{MinSupp}_V(\widehat{S}) \leq d \cdot \mathrm{MinSupp}_V(G) \end{aligned}$$

also holds with $d > 4.22$ by Lemma 4.2.4.

Next, let $G \simeq A_m$ for some $m \geq 15$. Then we have $m < q$ by the coprime assumption. Let us assume that $V$ is not a component of the natural permutation $\mathbb{F}_q A_m$-module. Let $\varphi \in \mathrm{Irr}(A_m)$ be an irreducible component of the Brauer character associated to $V$ and $\chi \in \mathrm{Irr}(S_m)$ above $\varphi$. By the proof of Corollary 4.3.7, we have $\varphi(1) = \varepsilon\chi(1)$, and $\varphi((123)) = \varepsilon\chi((123))$, where $\varepsilon$ is $1/2$ or $1$ if $\chi$ is self-dual or not. If $\chi$ is one of the characters given in Table 4.1, then $\chi$ is not self-dual. In that case we have

$$\mathrm{Supp}_V((123)) \geq \frac{1}{2}(\chi(1) - |\chi(123)|) \geq \frac{3}{2}(m-3)$$

by using Lemma 4.2.4 and the last five rows of Table 4.1. Otherwise, $\chi(1) > \frac{1}{3}m(m-2)(m-4)$, so we have

$$\begin{aligned}\mathrm{Supp}_V((123)) &\geq \frac{1}{2}(\varphi(1) - |\varphi(123)|) \geq \frac{1}{4}(\chi(1) - |\chi(123)|) \\ &\geq \frac{\chi(1)}{4(m-1)} > \frac{m(m-2)(m-4)}{12(m-1)} \geq m-3\end{aligned}$$

holds if $\varphi(123) \geq 0$. However, if $\varphi(123) < 0$, then $\mathrm{Supp}_V((123)) \geq \frac{1}{2}\dim(V) \geq m-3$ holds trivially. Thus, $\mathrm{Supp}_V((123)) \geq m-3$ holds in any case. Now, for any element $1 \neq g \in A_m$ there are $x, y \in A_m$ such that $[g, x, y]$ is a three-cycle. Applying Lemma 4.4.3 twice, we get that $\mathrm{Supp}_V(g) \geq \frac{1}{4}\mathrm{Supp}_V((123)) \geq \frac{m-3}{4}$ holds for any $1 \neq g \in A_m$. Thus, $d \cdot \mathrm{MinSupp}_V(G) \geq \frac{d(m-3)}{4} \geq m \geq \log_m(m!) \geq \log_q |G|$ holds for $d \geq 5$.

Now, let $m \geq 12$ and let $G_0$ be the universal covering group of $A_m$, so $G_0 \simeq 2.A_m$. By the proof of Corollary 4.3.7, we have $\mathrm{MinSupp}_V(G) \geq \frac{1}{8}\dim(V)$. Using [45, Main Theorem] we get that

$$\begin{aligned}d \cdot \mathrm{MinSupp}_V(G) &\geq \frac{d}{8}\dim(V) \geq \frac{d}{8}\min\{\chi(1) \,|\, \chi \in \mathrm{Irr}(G),\, \chi(z) \neq \chi(1)\} \\ &\geq d \cdot 2^{\lfloor m/2 \rfloor - 4} \geq m \geq \log_q |G|\end{aligned}$$

holds for $d \geq 3.25$. For the remaining members of Alternating groups and their covers (i.e for $A_m,\ 12 \leq m \leq 14$), for $2.A_m (m = 5 \text{ or } 8 \leq m \leq 11)$ and for $6.A_6, 6.A_7$ we used the same algorithm as for sporadic groups.

Finally, let $G_0 = G_0(r)$ be a quasisimple group of Lie type over a finite field $\mathbb{F}_r$ with $(r, q) = 1$. In that case we will use results about character ratios of such groups given by Gluck in [29]. (For a summary of his results, see also [48, Theorem 2.4]).

First, suppose that $r \geq 47$. By [29], we have

$$\mathrm{mr}(G) \leq \max\Big(\frac{1}{\sqrt{r}-1}, \frac{9}{r}\Big) < \frac{1}{5}.$$

By using [57, Theorem 1.] and Lemma 4.2.4,

$$\log_q |G| \leq 2n = 5 \cdot \frac{2n}{5} \leq 5 \cdot \mathrm{MinSupp}_V(G)$$

For the rest of the proof, suppose that $r \leq 43$. Since $\chi(1) - 2\,\mathrm{Supp}(g) \leq |\chi(g)|$ for any $\chi \in \mathrm{Irr}(G)$, we have that

$$\frac{1}{2}\chi(1)\Big(1 - \frac{|\chi(g)|}{\chi(1)}\Big) \leq \mathrm{Supp}(g).$$

Using that $\mathrm{mr}(G) \leq \frac{19}{20}$ also holds for all quasisimple groups of Lie-type by [29], we obtain that

$$\frac{\dim(V)}{8} \leq 5\,\mathrm{MinSupp}_V(G)$$

by using Lemma 4.2.4 again. Since (see [44, Table 5.3.A]) $\dim(V) \geq r^{\mathcal{O}(m)}$ (where $m$ denotes the rank of $G_0(r)$) and $\log_q |G| = \mathcal{O}(m^2 \log r)$, there exist only finitely many possible pairs $(m, r)$ such that $\log_q |G| > 5\,\mathrm{MinSupp}_V(G)$. Furthermore, for any fixed $(m, r)$, the inequality $\log_q |G| \leq 5\,\mathrm{MinSupp}_V(G)$ still holds provided that $|V|$ is large enough. □

We close this section by handling the case (2) in Theorem 4.3.8. In this case $\mathrm{MinSupp}_V(G)$ is bounded. (It is 1 and 2 for $G_0 \simeq S_m$ and $G_0 \simeq A_m$, respectively.)

**Theorem 4.3.9.** *Let $U$ be an $m$-dimensional vector space over $\mathbb{F}_q$, and let $G = S_m$ with its natural permutation action on $U$. Assuming that $(|G|, |U|) = 1$, we have*

$$P(\textit{random } \underline{u} \in U^c \textit{ is a base for } G) > 1 - \frac{1}{m^{c-2}} \textit{ for any } c \geq 3.$$

*Hence three random vectors form a base for $G$ with high probability if $m$ is large.*

*Proof.* The $\mathbb{F}_q G$-module $V^c$ can be naturally identified with $M^{m\times c}(q)$, the space of $m \times c$-matrices over $\mathbb{F}_q$. Under this identification, $G$ acts on $M^{m\times c}(q)$ by permuting the rows of each element of $M^{m\times c}(q)$ in a natural way. Hence, a matrix $a \in M^{m\times c}(q)$ is a base for $G$ if and only if the rows of $a$ are pairwise different elements of $M^{1\times c}(q)$, the space of $c$-dimensional row vectors over $\mathbb{F}_q$. Thus, the probability in question is equal to the probability that $m$ random elements of $M^{1\times c}(q)$ are pairwise different, which is

$$\prod_{i=0}^{m-1} \frac{q^c - i}{q^c} > \left(\frac{q^c - q}{q^c}\right)^m \geq \left(1 - \frac{1}{m^{c-1}}\right)^m \geq 1 - \frac{1}{m^{c-2}},$$

where the first and second inequalities follows since $m < q$ by the coprime assumption. The claim follows. □

**Corollary 4.3.10.** *Let $V$ be an $n$ dimensional vector space over the finite field $\mathbb{F}_q$ and let $G = Z \cdot G_0 \leq GL(V)$ be a coprime linear group, where $G_0 \simeq S_m$ or $G_0 \simeq A_m$ and $V$ is the non-trivial irreducible component of the natural $\mathbb{F}_q G_0$-module. Then we have*

$$P(\textit{random } \underline{v} \in V^c \textit{ is a base for } G) > 1 - \frac{1}{n^{c-2}} \textit{ for any } c \geq 3.$$

*Proof.* First, note that $\mathrm{Fix}(g) = 0$ for every $g \in G \setminus G_0$, so a $\underline{v} \in V^c$ is a base for $G$ if and only if it is a base for $G_0$. Second, let $U = V \oplus U_0$, where $U_0$ is the trivial module for $G_0$. For any random vectors $u_1, \ldots, u_c \in U$ let $v_i$ be the projection of $u_i$ to $V$ along $U_0$. Then $u_1, \ldots, u_c$ is a base for $G_0$ if and only if $v_1, \ldots, v_c$ is a base for $G_0$, so the claim follows from Theorem 4.3.9. □

## 4.4 Proof of the Main Theorem

In this section we prove the following theorem

**Theorem 4.4.1.** *Let $V$ be an $n$-dimensional vector space over the finite field $\mathbb{F}_q$ and let $G \leq GL(V)$ be a coprime primitive linear group. Then for any $c \geq 11$, the probability $Pb(c, G, V)$ is close to zero if $|V|$ is large enough. More precisely, one of the following holds.*

*(1)* $Pb(c, G, V) \geq 1 - \frac{3}{q^{(\frac{c}{2}-5)\sqrt{n}}}$;

*(2) There is an $\mathbb{F}_q^k$ vector space structure on $V$ for some field extension $\mathbb{F}_q^k \geq \mathbb{F}_q$ (possibly $k = 1$) and a tensor product decomposition $V = V_1 \otimes_{\mathbb{F}_q^k} U$ over $\mathbb{F}_q^k$ with $1 \leq \dim(U) < \dim(V_1) \leq n/k$ such that $G \leq \Gamma L(\mathbb{F}_q^k, n/k)$ and $H = G \cap GL((\mathbb{F}_q^k, n/k)$ preserves this tensor product decomposition. Furthermore, $H = H_1 \otimes H_2$ with $H_1 \leq GL(V_1)$, $H_2 \leq GL(U)$ are absolutely irreducible linear groups, and $S_1 = \mathrm{Soc}(H_1/Z(H_1))$ is a non-Abelian simple group.*

*(a) If $S_1$ is not an alternating group, then*

$$Pb(c, G, V) \geq 1 - \Big(\frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + \frac{2}{|V|^{(c-10)/80}}\Big);$$

*(b) If $S_1 \simeq A_m$ for some $m$ and $V_1$ is not an irreducible component of the natural permutation $\mathbb{F}_q^k A_m$-module, then*

$$Pb(c, G, V) \geq 1 - \frac{3}{q^{\frac{c-10}{16}\sqrt{\dim(V)}}};$$

*(c) If $S_1 \simeq A_m$ for some $m$ and $V_1$ is the non-trivial irreducible component of the natural permutation $\mathbb{F}_q^k A_m$-module, then*

$$Pb(c, G, V) \geq 1 - \frac{3}{n^{c-2}}.$$

In other words, this theorem proves that for a coprime primitive linear group, the probability that a random 11-tuple in $V$ is a base for $G$ tends to 1 as $|V| \to \infty$.

Let $V$ be an $n$-dimensional vector space over the finite field $\mathbb{F}_q$ and let $G \leq GL(V) = GL(n, q)$ be a coprime primitive linear group, which is maximal, i.e. there is no coprime subgroup $L \leq GL(V)$ strictly containing $G$. In the following, we give a structure theorem of such groups very similar to a result about maximal solvable primitive linear group (see [64, Lemma 2.2] and [67, §§19–20]). Our proof uses ideas similar to those can be found in [32], [36], and [67].

In the following, we extend the vector space structure on $V$ by defining multiplication on $V$ with elements from a (possibly) larger field $\mathbb{F}_{q^k} \geq \mathbb{F}_q$ for some $k \mid n$. In that way, $V$ will be both an $\mathbb{F}_q$-vector space and an $\mathbb{F}_{q^k}$-vector space at the same time.

We will use the notation $V = V_n(q)$, $V = V_d(q^k)$ or $V = V(q^k)$ if we would like to highlight the base field and/or the dimension of $V$.

**Theorem 4.4.2.** *Let $V = V_n(q)$ be an $n$-dimensional vector space over the finite field $\mathbb{F}_q$ and let $G \leq GL(V)$ be a maximal coprime primitive linear group. Then the following statements hold.*

*(1) There is a unique maximal Abelian subgroup $Z \leq GL(V)$, which is normalised by $G$. Moreover, $Z$ is contained in $G$.*

*(2) $Z$ is cyclic and $Z \cup \{0\} \simeq \mathbb{F}_{q^k}$ for some $k \mid n$.*

*(3) There is a (unique and maximal) $\mathbb{F}_{q^k}$ vector space structure $V = V_d(q^k)$ on $V$ for $d = n/k$ such that $G \leq \Gamma L(d, q^k))$.*

*(4) Let $H := G \cap GL(d, q^k)$. Then $Z \leq H = C_G(Z) \lhd G$, furthermore $Z = Z(GL(d, q^k))$ is the group of scalar transformations on $V_d(q^k)$ and $G/H$ is included into the Galois group $\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.*

*(5) Let $N = F^*(H)$ be the generalised Fitting subgroup of $H$. Then $N/Z$ is the socle of $H/Z$. Furthermore, $V_d(q^k)$ is an absolutely irreducible $\mathbb{F}_{q^k}N$-module.*

*(6) Let $N_1, \ldots, N_t$ be the set of minimal normal subgroups of $H$ above $Z$. Then there is an absolutely irreducible $\mathbb{F}_{q^k}N_i$-module $V_i$ for every $i$ such that $V \simeq V_1 \otimes_{\mathbb{F}_{q^k}} \ldots \otimes_{\mathbb{F}_{q^k}} V_t$. Furthermore, $N = N_1 \otimes N_2 \otimes \ldots \otimes N_t$ and $H = H_1 \otimes H_2 \otimes \ldots \otimes H_t$ where $N_i \lhd H_i \leq GL(V_i(q^k))$ for every $i$.*

*(7) If $N_i/Z$ is Abelian, then $N_i = ZR_i$ where $R_i \leq N_i$ is an extraspecial $r_i$-group for some prime $r_i$ of order $r_i^{2l_i+1}$. Furthermore, $|N_i/Z| = r_i^{2l_i}$ and $\dim_{\mathbb{F}_{q^k}}(V_i) = r_i^{l_i}$.*

*(8) If $N_i/Z$ is a direct product of $s$ many isomorphic non-Abelian simple groups, then there is a tensor product decomposition $V_i = W_1 \otimes \ldots \otimes W_s$ preserved by $N_i$. Then $N_i = K_1 \otimes \ldots \otimes K_s$ where $K_i = S_i Z$ for each $i$, and the $S_i \leq GL(W_i)$ are isomorphic quasisimple absolutely irreducible groups. Finally, $H_i$ permutes the $K_i$-s and the $W_i$-s in a transitive way.*

*Proof.* Let $A \leq GL(V)$ be any Abelian subgroup normalised by $G$ and $P$ is the (unique) Sylow-$p$ subgroup of $A$ for $p = \mathrm{char}(\mathbb{F}_q)$. Then $P$ is normalised by $G$. Then $0 \neq \mathrm{Fix}_V(P) = \cap_{p \in P} \mathrm{Fix}_V(p) \leq V$ is $G$-invariant. Since $V$ is an irreducible $\mathbb{F}_q G$-module, we get that $P = 1$, so $|A|$ is coprime to $|V|$. Therefore, $GA \geq G$ is a coprime linear group, so $A \leq G$ by the maximality of $G$ and part of (1) is proved.

Let $Z \leq GL(V)$ be a maximal Abelian subgroup normalised by $G$. By the previous paragraph, $Z \lhd G$. Since $G \leq GL(V)$ is primitive linear, $V$ is a homogeneous $\mathbb{F}_q Z$-module. If $V = V_1 \oplus \ldots \oplus V_d$ is a decomposition of $V$ into (isomorphic) irreducible $\mathbb{F}_q Z$-modules, then $Z \simeq Z_{V_i} \leq \mathrm{End}_Z(V_i) \simeq \mathbb{F}_{q^k}$ for some $k \geq 1$ by using Schur Lemma. Then $\langle Z \rangle_{\mathbb{F}_q}$ (the subalgebra of $\mathrm{End}(V)$ generated by $Z$) is isomorphic to the field $\mathbb{F}_q^k$, and it is invariant under the conjugation by elements of $G$. It follows that $\langle Z \rangle_{\mathbb{F}_q} \setminus \{0\} \simeq \mathbb{F}_q^*$ is an Abelian subgroup of $GL(V)$ normalised by $G$. Therefore, (2) follows by the maximality of $Z$.

Identifying $Z \cup 0 \leq \mathrm{End}(V)$ with $\mathbb{F}_q^k$, it defines an $\mathbb{F}_{q^k}$ vector space structure on $V$. The conjugation action of $G$ on $Z \cup \{0\} = \mathbb{F}_{q^k}$ defines a homomorphism $\sigma : G \mapsto \mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$. Now, for any $g \in G$, $\alpha \in \mathbb{F}_q^k$ and $v \in V$ we have $g(\alpha v) = (g \alpha q^{-1}) g(v) = \alpha^{\sigma(g)}(v)$, so $G$ is

included into the semilinear group $\Gamma L(V_d(q^k)) = \Gamma L(d, q^k)$. The subgroup $H$ is just the kernel of $\sigma$, so (4) and part of (3) follows.

Let $B \lhd G$ be any Abelian normal subgroup, $\alpha \in Z$ a generator of $Z$ and $b \in B$. Then $b\alpha b^{-1} = \alpha^{\sigma(b)} = \alpha^{q^s}$ for some $0 \leq s < k$, so $[b, \alpha] = \alpha^{q^s-1} \in B$ is centralised by $b$. Changing $b$ to $b^{-1}$ if necessary, we can assume that $0 \leq s \leq k/2$. This means $(\alpha^{q^s-1})^{q^s} = \alpha^{q^s-1}$, so $q^k - 1 \mid (q^s-1)^2 < q^k - 1$. Therefore, $s = 0$. Thus, $B \leq C_G(Z)$, so $BZ \geq Z$ is an Abelian normal subgroup in $G$. By the maximality of $Z$, we get $B \leq Z$, which completes the proof of both (1) and (3).

Let $M = F(H)$ be the Fitting subgroup of $H$. Then $Z(M)$ is an Abelian normal subgroup of $G$, so $Z(M) = Z$ by the maximality of $Z$. Let $n$ by the nilpotency class of $M$. If $n = 1$ then $M = Z$. Otherwise, we claim that $n = 2$. Assuming that $n \geq 3$, we have $1 \neq \gamma_n(M) \leq Z$, and $[\gamma_{n-1}(M), \gamma_{n-1}(M)] \leq [\gamma_2(M), \gamma_{n-1}(M)] \leq \gamma_{n+1}(M) = 1$, so $\gamma_{n-1}(M)$ is an Abelian normal subgroup of $G$, so it must contained in $Z$. This forces $\gamma_n(M) = 1$, a contradiction. Therefore, $n \leq 2$, that is, $M/Z$ is Abelian.

Let $R$ be a Sylow-$r$-subgroup of $M$ for some prime $r$ dividing $|M/Z|$. The commutator map defines a symplectic bilinear function from $R/Z$ into $Z(R) = R \cap Z$. Therefore, for any $x, y \in R$ we have $[x^r, y^r] = [x, y]^{r^2} = [x^{r^2}, y]$. If $r^s$ is the exponent of $R/(R \cap Z)$ for some $s \geq 2$, then $R^{r^{s-1}}Z$ is an Abelian normal subgroup of $G$, so $R^{r^{s-1}} \leq Z$, a contradiction. Thus, we get $R/(R \cap Z)$ is an elementary Abelian $r$-group. Using this and the above commutator identity it also follows that $R' \leq Z$ is of exponent $r$. It follows that $R = (R \cap Z)R_0$ for some extraspecial $r$-group $R_0$.

By the previous two paragraphs, $F(H)/Z$ is exactly the direct product of the minimal Abelian normal subgroups of $H$, so $F(H)/Z$ is contained in $\mathrm{Soc}(H/Z)$. Since $N = F^*(H)$ is the central product of $F(H)$ and the layer $E(H)$, where $E(H)/Z$ is the direct product of the minimal non-Abelian normal subgroups of $H/Z$ it follows that $N/Z = \mathrm{Soc}(H/Z)$ as claimed. By [32, Lemma 12.1], $V_d(q^k)$ is an absolutely irreducible $\mathbb{F}_{q^k}H$-module. If the irreducible $\mathbb{F}_{q^k}N$-components of $V_d(q^k)$ were not be absolutely irreducible, then $Z(C_{GL(V_d(q^k))}(N))$ would be the multiplicative group of a proper field extension of $\mathbb{F}_{q^k}$ normalised by $G$, which again contradicts with the maximility of $Z$. Now, let us assume that $V_d(q^k) = U \oplus \ldots \oplus U$ is a direct sum of $s$ many isomorphic absolutely irreducible $\mathbb{F}_{q^k}N$-modules for some $s \geq 2$. By [44, Lemma 4.4.3(ii)], there is a tensor product decomposition $U \otimes_{\mathbb{F}_{q^k}} W$ of $V_d(q^k)$ such that $N \leq GL(U) \otimes 1_W \leq GL(U) \otimes GL(W)$ and $G \leq N_{\Gamma L(V)}(N) \leq N_{\Gamma L(V)}(GL(U) \otimes GL(W))$. Let $L = \{1_U \otimes h_W \mid \exists h_U \in GL(U) \text{ such that } h_U \otimes h_W \in H\}$. If $L = Z$, then $V_d(q^k)$ is not irreducible as an $\mathbb{F}_{q^k}H$-module, a contradiction. We have $L \leq GL(V)$ is a coprime linear group normalised by $G$, so $LG \leq GL(V)$ is coprime. Using the maximality of $G$ we get that $L < G$. But then $Z < L \leq H$ clearly centralises $N = F^*(H)$, a contradiction. So, $V_d(q^k)$ is an absolutely irreducible $\mathbb{F}_{q^k}N$-module, and (5) is proved. Now, (6) follows by a combined use of [55, Corollary 18.2/(a)] and [44, Lemma 4.4.3(iii)].

If $N_i/Z$ is Abelian, then it is a minimal Abelian normal subgroup of $H/Z$ so it is elementary Abelian $r_i$-group for some prime $r_i$. Using the same argument as in paragraph 6 of this proof, one can find the extraspecial $r_i$-group $R_i$ by taking the full inverse image of a maximal non-degenerate subspace of $R/R'$ where $R$ is the Sylow-$r_i$ subgroup of $N_i$. For this subgroup, it clearly follows that $N_i = ZR_i$, and $|R_i| = r_i^{2l_i+1}$ for some integer. Furthermore, since $V_i$ is an absolutely irreducible $\mathbb{F}_{q^k}N_i$-module, it must be an absolutely irreducible $\mathbb{F}_{q^k}R_i$-module. It is well-known that extraspecial $r_i$-group of order $r_i^{2l_i+1}$ has

a unique faithfull absolutely irreducible ordinary representation, and this representation has degree $r_i^{l_i}$, which finishes the proof of (7).

Finally, (8) can again be deduced from [55, Corollary 18.2/(a)] and from the fact that $N_i/Z$ is a minimal normal subgroup in $H_i/Z$. □

**Lemma 4.4.3.** *Let $G$ be a group, $K$ be a field and let $V$ be an arbitrary finite dimensional $KG$-module.*

*(1) For any $g, h \in G$ we have* $\mathrm{Supp}([g,h]) \leq 2\,\mathrm{Supp}(g)$.

*(2) If $N \lhd G$ such that $V$ is absolutely irreducible as a $KN$-module, then* $\mathrm{MinSupp}(N) \leq 2\,\mathrm{MinSupp}(G)$.

*Proof.* Let us consider the subspaces $U = \mathrm{Fix}(g)$ and $W = \mathrm{Fix}(h^{-1}gh)$ of $V$. Then we have

$$\dim(U) + \dim(W) - \dim(U \cap W) = \dim(U + W) \leq \dim(V).$$

Using that $\dim(U) = \dim(W) = \dim(V) - \mathrm{Supp}(g)$ we get $\dim(U \cap W) \geq \dim(V) - 2\,\mathrm{Supp}(g)$. On the other hand $U \cap W \leq \mathrm{Fix}([g,h])$ holds trivially, so

$$\begin{aligned}\mathrm{Supp}([g,h]) &= \dim(V) - \dim(\mathrm{Fix}([g,h])) \leq \dim(V) - \dim(U \cap W)\\ &\leq \dim(V) - (\dim(V) - 2\,\mathrm{Supp}(g)) = 2\,\mathrm{Supp}(g),\end{aligned}$$

and part (1) follows.

For part (2), let $1 \neq g \in G$ be any element. If $[g, N] = 1$, then $g$ acts as a scalar transformation on $V$ by [38, Theorem 9.2], so $\mathrm{Supp}(g) = \dim(V) \geq \mathrm{MinSupp}(N)$. Otherwise, there is an element $n \in N$ such that $[g,n] \neq 1$. Then we have $\mathrm{MinSupp}(N) \leq \mathrm{Supp}([g,n]) \leq 2\,\mathrm{Supp}(g)$. Thus, $\mathrm{MinSupp}(N) \leq 2\,\mathrm{Supp}(g)$ for every $1 \neq g \in G$, which proves that $\mathrm{MinSupp}(N) \leq 2\,\mathrm{MinSupp}(G)$. □

**Lemma 4.4.4.** *Let $V_1, \ldots, V_k$ be finite dimensional vector spaces over the field $\mathbb{F}_q$ and $Z < G_1 \leq GL(V_1), \ldots, Z < G_k \leq GL(V_k)$ be coprime linear groups. Consider the group $G := G_1 \otimes \ldots \otimes G_k$ acting on the tensor product $V := V_1 \otimes \ldots \otimes V_k$ in a natural way.*

*(1) Let $g = g_1 \otimes \ldots \otimes g_k \in G$ with $g_j \in G_j$ for each $j$ and let us assume that $g_i \notin Z$ for some $i$. Then*

$$\mathrm{Supp}_V(g) \geq \mathrm{MinSupp}_{V_i}(G_i) \cdot \frac{\dim(V)}{\dim(V_i)}$$

*or* $\mathrm{Supp}_V(g) \geq \frac{1}{2}\dim(V)$.

*(2) As a consequence*

$$\mathrm{MinSupp}_V(G) = \min_i \left\{ \mathrm{MinSupp}_{V_i}(G_i) \cdot \frac{\dim(V)}{\dim(V_i)} \right\},$$

*or* $\mathrm{MinSupp}_V(G) \geq \frac{1}{2}\dim(V)$.

*Proof.* To prove part (1), first we consider the case $k = 2$. Let $n_1 = \dim(V_1)$, $n_2 = \dim(V_2)$, so $n = \dim(V) = n_1 n_2$. Furthermore, let $1 \neq g = g_1 \otimes g_2 \in G_1 \otimes G_2$ be an element of $G$ with $g_1 \notin Z$. Since the action is coprime, $g_1$ and $g_2$ are diagonalisable over

$\overline{\mathbb{F}}_q$. Let $\alpha_1, \dots \alpha_s \in \overline{\mathbb{F}}_q$ be the different eigenvalues of $g_1$ with multiplicity $k_1, k_2, \dots, k_s$. We can assume that $k_1$ is the largest among the $k_i$. Let $l_1, \dots, l_s$ be the multiplicities of $\alpha_1^{-1}, \dots, \alpha_s^{-1}$ in the characteristic polynomial of $g_2$ (Some of them can be zero). Then

$$\begin{aligned}\mathrm{Supp}_V(g) = \mathrm{Supp}_V(g_1 \otimes g_2) &= n - \dim(\mathrm{Fix}_V(g_1 \otimes g_2)) \\ &= n - \sum_{i=1}^{s} k_i l_i \geq n - \sum_{i=1}^{s} k_1 l_i \geq (n_1 - k_1) n_2.\end{aligned}$$

If $\alpha_1 \in \mathbb{F}_q$, then we can substitute $g_1$ by $\alpha_1^{-1} g_1$ and $g_2$ by $\alpha_1 g_2$ (since both $G_1$ and $G_2$ contains all the scalar transformations), so we can assume that $\alpha_1 = 1$. Now, since $g_1 \neq 1$, we get $\mathrm{Supp}_V(g) \geq (n_1 - k_1)n_2 = \mathrm{Supp}_{V_1}(g_1)n_2 \geq \mathrm{MinSupp}_{V_1}(G_1) \cdot \dim(V_2)$.

Now, let us assume that $\alpha_1 \notin \mathbb{F}_q$. Then there is an algebraic conjugate element of $\alpha_1$ (different from $\alpha_1$) under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q, \mathbb{F}_q)$ which is also an eigenvalue of $g_1$ with the same multiplicty as $\alpha_1$. In particular, $k_1 \leq n_1/2$. Thus,

$$\mathrm{Supp}_V(g) \geq (n_1 - k_1)n_2 \geq (n_1/2)n_2 = \frac{\dim(V)}{2}.$$

By changing the role of $g_1$ and $g_2$ in the proof and by using induction on $k$, we get the claim of part (1).

Finally, if $\mathrm{Supp}_{V_i}(g_i) = \mathrm{MinSupp}_{V_i}(G_i)$ for some $g_i \notin Z$, then

$$\mathrm{Supp}_V(1 \otimes \dots \otimes 1 \otimes g_i \otimes 1 \otimes \dots \otimes 1) = \mathrm{MinSupp}_{V_i}(G_i) \cdot \frac{\dim(V)}{\dim(V_i)},$$

so part (2) follows by using part (1). □

*Proof of Theorem 4.4.1.* Let $G \leq GL(V)$ be a coprime primitive linear group. Without loss of generality we can assume that $G$ is maximal among such subgroups of $GL(V)$. Let $Z$ be the unique maximal Abelian subgroup in $GL(V)$ which is normalised by $G$ and $H$ be the intersection of $G$ and $GL(d, q^k)$ as in Theorem 4.4.2. If $g \in G \setminus H$ then there is a $z \in Z$ such that $[g, z] \neq 1$. By Lemma 4.4.3, $\mathrm{Supp}_V(g) \geq \frac{1}{2}\mathrm{Supp}_V([g, z]) = \frac{1}{2}\dim(V)$. Therefore if $c > 4$, then

$$\sum_{g \in G \setminus H} \frac{1}{q^{c \cdot \mathrm{Supp}_V(g)}} \leq \frac{|G \setminus H|}{q^{\frac{c}{2}\dim(V)}} \leq \frac{|V|^2}{|V|^{\frac{c}{2}}} \leq \frac{1}{|V|^{\frac{c}{2}-2}}.$$

Now let $g$ be an element of $H = H_1 \otimes \dots \otimes H_t$. So $g = (g_1, \dots, g_t)$ where $g_i \in H_i$ for all $i \in [t]$ and $g$ preserves the tensor product decomposition $V = V_1 \otimes \dots \otimes V_t$ over $\mathbb{F}_q^k$ as in Theorem 4.4.2 (6) and $\dim_{\mathbb{F}_{q^k}}(V_i) = d_i$ for all $i$ (therefore $d = \dim_{\mathbb{F}_{q^k}}(V) = \prod_{i=1}^t d_i$ and $\dim(V) = \dim_{\mathbb{F}_q}(V) = k \cdot \prod_{i=1}^t d_i$). We can assume that in this decomposition the dimensions of the vector spaces are decreasing, i.e. $d_1 \geq d_2 \geq \dots \geq d_t \geq 2$. Let $g_i \notin Z$ for some $i \neq 1$. Then by Lemma 4.4.4,

$$\mathrm{Supp}_V(g) \geq \mathrm{MinSupp}_{V_i}(H_i) \cdot \frac{\dim(V)}{\dim(V_i)} \geq k \prod_{j \neq i} d_j.$$

Since $2\prod_{j \neq i} d_j \geq 2^{t-1} d_1 \geq \sum_{i=1}^t d_1$ and $k \prod_{j \neq i} d_j \geq k\sqrt{\prod_{j=1}^t d_j} \geq \sqrt{\dim(V)}$ we get that

$$c \cdot \mathrm{Supp}_V(g) \geq 2k \sum_{i=1}^{t} d_i + (c-4)\sqrt{\dim(V)}.$$

Hence,

$$\sum_{g\in H\setminus H_1}\frac{1}{q^{c\cdot\mathrm{Supp}_V(g)}}\leq\frac{\prod_{i=1}^t|H_i|}{q^{2k\sum_{i=1}^t d_i+(c-4)\sqrt{\dim(V)}}}$$
$$\leq\frac{q^{2k\sum_{i=1}^t d_i}}{q^{2k\sum_{i=1}^t d_i+(c-4)\sqrt{\dim(V)}}}=\frac{1}{q^{(c-4)\sqrt{\dim(V)}}}.$$

Now assume that $g\in H_1$. In this case $\mathrm{Supp}_V(g)=\mathrm{Supp}_{V_1}(g)\cdot\frac{d}{d_1}$. By Theorem 4.4.2, $Z\leq N_1\leq H_1\leq GL(V_1(q^k))$ where $N_1$ is a minimal normal subgroup above $Z$ and $N_1/Z$ is characteristically simple. Therefore, it is either an elementary Abelian group, a direct product of non-Abelian simple groups, or a non-Abelian simple group.

First, if $N_1/Z$ is elementary Abelian, then $N_1=Z\cdot P$ where $P$ is an extraspecial $r$-group for a prime $r$ with $r\mid q^k-1$. Then $V_1(q^k)$ is an absolutely irreducible $\mathbb{F}_{q^k}P$-module. If $n\in P\setminus Z$ then $n$ has exactly $r$ different eigenvalues on $V_1$ (or on $V$) each with the same multiplicity. It follows that $\mathrm{MinSupp}_V(N_1)\geq\frac{r-1}{r}\dim(V)\geq\frac{1}{2}\dim(V)$, so $\mathrm{MinSupp}_V(H_1)\geq\frac{1}{4}\dim(V)$ by Lemma 4.4.3. In this case,

$$\sum_{g\in H_1}\frac{1}{q^{c\cdot\mathrm{Supp}_V(g)}}\leq\frac{|H_1|}{q^{\frac{c}{4}\dim(V)}}\leq\frac{|V|^2}{q^{2\dim(V)+(\frac{c}{4}-2)\dim(V)}}\leq\frac{1}{|V|^{\frac{c}{4}-2}}.$$

Next, let $N_1/Z$ is a direct product of $s\geq 2$ many isomorphic non-Abelian simple groups. By Theorem 4.4.2 (8), the action of $N_1=K_1\otimes\ldots\otimes K_s$ on $V_1$ preserves a tensor product decomposition $V_1=W_1\otimes\ldots\otimes W_s$ over $\mathbb{F}_q^k$ , where $\dim_{\mathbb{F}_{q^k}}(W_i)=\sqrt[s]{d_1}\geq 2$ for every $i$. Using [57, Theorem 1], we get that

$$|N_1|\leq\prod_{i=1}^s|K_s|\leq\prod_{i=1}^s|W_i|^2=q^{2ks\sqrt[s]{d_1}}.$$

On the other hand, $H_1/N_1$ acts faithfully on $\{W_1,\ldots,W_s\}$ and $|H_1/N_1|$ is coprime to $q$, so $|H_1/N_1|\leq q^s$ by [36, Corollary 2.4]. Therefore, $|H_1|\leq q^{2ks\sqrt[s]{d_1}+s}$. By Lemma 4.4.3 and by Lemma 4.4.4,

$$\mathrm{Supp}_{V_1}(g)\geq\frac{1}{2}\,\mathrm{MinSupp}_{V_1}(N_1)\geq\frac{k}{2}\cdot\frac{d_1}{\sqrt[s]{d_1}}.$$

Therefore,

$$c\,\mathrm{Supp}_V(g)\geq 5kd_1{}^{(s-1)/s}+\Big(\frac{c}{2}-5\Big)k\sqrt{d_1}\cdot\frac{d}{d_1}\geq 2ks\sqrt[s]{d_1}+s+\Big(\frac{c}{2}-5\Big)\sqrt{\dim(V)}.$$

So,

$$\sum_{1\neq g\in H_1}\frac{1}{q^{c\cdot\mathrm{Supp}_V(g)}}\leq\frac{|H_1|}{q^{c\cdot\mathrm{MinSupp}_V(H_1)}}\leq\frac{q^{2ks\sqrt[s]{d_1}+s}}{q^{2ks\sqrt[s]{d_1}+s+(\frac{c}{2}-5)\sqrt{\dim(V)}}}$$
$$\leq\frac{1}{q^{(\frac{c}{2}-5)\sqrt{\dim(V)}}}.$$

Finally, let $N_1/Z$ be a non-Abelian simple group. If $d_1 \leq \sqrt{d}$, then we can use the same argument as in the previous paragraph to get that

$$\sum_{1\neq g\in H_1} \frac{1}{q^{c\cdot \mathrm{Supp}_V(g)}} \leq \frac{1}{q^{(c-2)\sqrt{\dim(V)}}}.$$

Summarizing the bounds given until this point, we get that

$$Pb(c,G,V) \geq 1 - \sum_{1\neq g\in G} \frac{1}{q^{c\cdot \mathrm{Supp}_V(g)}} \geq 1 - \Big(\frac{1}{|V|^{\frac{c}{2}-2}} + \frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + \frac{1}{q^{(\frac{c}{2}-5)\sqrt{\dim(V)}}}\Big) \geq 1 - \frac{3}{q^{(\frac{c}{2}-5)\sqrt{\dim(V)}}},$$

which is case (1) of Theorem 4.4.1.

Now, let us assume that $d_1 \geq \sqrt{d}$. If $|V_1| = q^{kd_1}$ is bounded by the constant appearing in part (3) of Theorem 4.3.8, then $|V|$ is also bounded. Hence we can assume that either part (1) or part (2) of Theorem 4.3.8 holds. By Lemma 4.4.3, we also have $\mathrm{MinSupp}_V(H_1) \geq \frac{1}{2}\mathrm{MinSupp}_V(N_1)$.

If $N_1/Z$ is not an alternating group, then $\mathrm{MinSupp}_V(N_1) \geq \frac{1}{40}\dim(V)$ and $5\cdot\mathrm{MinSupp}_V(N_1) \geq \log_q|H_1|$ by using Corollary 4.3.3, Theorem 4.3.8/(1) and Lemma 4.4.4/(2). Thus, we have

$$\sum_{1\neq g\in H_1} \frac{1}{q^{c\cdot \mathrm{Supp}_V(g)}} \leq \frac{1}{|V|^{(c-10)/80}}.$$

So, in this case we get that

$$Pb(c,G,V) \geq 1 - \Big(\frac{1}{|V|^{\frac{c}{2}-2}} + \frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + \frac{1}{|V|^{(c-10)/80}}\Big) \geq 1 - \Big(\frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + \frac{2}{|V|^{(c-10)/80}}\Big),$$

which is case (2)/a of Theorem 4.4.1.

Finally, let $N_1/Z \simeq A_m$ for some $m$. If $V_1$ is not an irreducible component of the natural $\mathbb{F}_q^k A_m$ permutation module, then we have $\mathrm{MinSupp}_V(N_1) \geq \frac{1}{16}\sqrt{\dim(V)}$ and $5\cdot\mathrm{MinSupp}_V(N_1) \geq \log_q|H_1|$ by using Corollary 4.3.7, Theorem 4.3.8/(1) and Lemma 4.4.4/(2). Thus, we have

$$\sum_{1\neq g\in H_1} \frac{1}{q^{c\cdot \mathrm{Supp}_V(g)}} \leq \frac{1}{q^{\frac{c-10}{16}\sqrt{\dim(V)}}}$$

and

$$Pb(c,G,V) \geq 1 - \Big(\frac{1}{|V|^{\frac{c}{2}-2}} + \frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + \frac{1}{q^{\frac{c-10}{16}\sqrt{\dim(V)}}}\Big) \geq 1 - \frac{3}{q^{\frac{c-10}{16}\sqrt{\dim(V)}}}.$$

Finally, if $V_1$ is the non-trivial irreducible component of the natural $\mathbb{F}_q^k A_m$-module, then with the use of Corollary 4.3.10 we get that

$$Pb(c,G,V) \geq 1 - \Big(\frac{1}{|V|^{\frac{c}{2}-2}} + \frac{1}{q^{(c-4)\sqrt{\dim(V)}}} + 1 - Pb(c,H_1,V)\Big) \geq 1 - \frac{3}{n^{c-2}},$$

which completes the proof of Theorem 4.4.1. □

# Bibliography


[1] Albertson, M. O.; Collins, K. L. Symmetry breaking in graphs. *Electron. J. Combin.* **3** (1996), no. 1, RP #18.

[2] Aschbacher, M.; Scott, L., Maximal subgroups of finite groups. *J. Algebra* **92** (1985), 44–80.

[3] Babai, L. On the order of uniprimitive permutation groups. *Ann. of Math.* (2) **113** (1981), no. 3, 553–568.

[4] Babai, L. On the order of doubly transitive permutation groups. *Invent. Math.* **65** (1981/82), no. 3, 473–484.

[5] 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.

[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] Burnside, W. On some properties of groups of odd order. *Proc. Lond. Math. Soc.* no. 33, (1901), 162–185

[16] Cameron, P.J. Finite permutation groups and finite simple groups. *Bull. London Math. Soc* no.13, (1981), 1–22.

[17] Cameron, P.J. Regular orbits of permutation groups on the power set.*Discrete Math.***62** (1986), 307–309

[18] Cameron, P.J. Permutation Groups. London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999.

[19] Cameron, P. J.; Kantor, W. M. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.* **2** (1993), no. 3, 257–262.

[20] Cameron, P.J.; Neumann, P.M.; Saxl,J. On groups with no regular orbits on the set of subsets.*Arch. Math.* (Basel) **43** (1984), 295–296.

[21] Devillers, A.; Morgan, L.; Harper, S. The distinguishing number of quasiprimitive and semiprimitive groups. *Arch. Math.* (2019), 127–139.

[22] Dixon, J. D. ; Mortimer, B. Permutation groups. Springer, New York-Berlin-Heidelberg, 1996.

[23] Dolfi, S. Orbits of permutation groups on the power set. *Arch. Math.* **75** (2000), 321–327.

[24] Duyan, H.; Halasi, Z.; Maróti, A. A proof of Pybers base size conjecture. *Adv. Math.* **331** (2018), 720–747.

[25] Duyan, H.; Halasi, Z.; Podoski, K. Random bases for coprime linear groups. *Journal of Group Theory* **23** (2020), 133–157.

[26] Fawcett, J. B. The ONan-Scott Theorem for finite primitive permutation groups, and finite representability. Master's Thesis, University of Waterloo (2009).

[27] Fawcett, J. B. The base size of a primitive diagonal group. *J. Algebra* **375** (2013), 302–321.

[28] 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.

[29] Gluck, D. Sharper character value estimates for groups of Lie type *J. Algebra* **174** (1995), 229–266.

[30] Gluck, D.; Magaard, K. Base sizes and regular orbits for coprime affine permutation groups. *J. London Math. Soc.* (2) **58** (1998), 603–618.

[31] Gluck, D.; Seress, Á.; Shalev, A. Bases for primitive permutation groups and a conjecture of Babai. *J. Algebra* **199** (1998), no. 2, 367–378.

[32] 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.

[33] Guralnick, R. M.; Maróti, A.; Pyber, L. Normalizers of primitive permutation groups. *Adv. Math.* **310** (2017), 1017–1063.

[34] Halasi, Z.; Liebeck, M. W.; Maróti, A. Base sizes of primitive groups: Bounds with explicit constants. *Journal of Algebra* **521** (2019), 16–43.

[35] Halasi, Z.; Maróti, A. The minimal base size for a p-solvable linear group. *Proc. Amer. Math. Soc.* **144** (2016), 3231–3242.

[36] Halasi, Z.; Podoski, K. Every coprime linear group admits a base of size two. *Trans. Amer. Math. Soc.* **368** (2016), 5857–5887.

[37] Hoffman, P. N.; Humphreys, J. F. *Projective representations of the symmetric groups. Q-functions and shifted tableaux.* Oxford Mathematical Monographs. Oxford University Press, New York (1992)

[38] Isaacs,I. M. *Character theory of finite groups*, Pure and Applied Mathematics, No. 69. Academic Press, New York-London, 1976.

[39] Isaacs, I. M. Finite Group Theory. American Mathematical Society, Graduate Studies in Mathematics, 92, 2008.

[40] 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.

[41] James, G. D. *The representation theory of the symmetric groups.* Lect. Notes Math., vol. 682. Springer, Berlin (1978)

[42] Jordan, C. Trailé des substitutions, Paris, 1870.

[43] Karp, R. M. Reducibility among combinatorial problems. In Miller, R. E.; Thatcher, J. W.; Bohlinger, J. D. (eds.) *Complexity of Computer Computations (New York)*:Plenum., (1972), 85–103.

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

[45] Kleshchev, A. S.; Tiep, P. H. Small-dimensional projective representations of symmetric and alternating groups, *Algebra Number Theory* **6** (2012), 1773–1816.

[46] Kovacs, L. G. Maximal subgroups in composite finite groups. *J. Algebra* **99** (1986), 114–131.

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

[48] Liebeck, M. W. Character ratios for finite groups of Lie type, and applications, *Contemp. Math.*, **694**, Amer. Math. Soc., (2017), 193–208.

[49] Liebeck, M. W.; Praeger, C. E.; Saxl, J. On the ONan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc.* **44** (1988), 389–396.

[50] Liebeck, M. W.; Shalev, A. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.* **12** (1999), no. 2, 497–520.

[51] Liebeck, M. W.; Shalev, A. Bases of primitive linear groups. *J. Algebra* **252** (2002), 95–113.

[52] Liebeck, M. W.; Shalev, A. Bases of primitive permutation groups. *Groups, combinatorics & geometry* (Durham, 2001), 147–154, World Sci. Publ., River Edge, NJ, 2003.

[53] Liebeck, M. W.; Shalev, A. Bases of primitive linear groups II. *J. Algebra* **403** (2014), 223–228.

[54] 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.

[55] Malle, G.; Testerman, D. *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, vol. 133, Cambridge University Press, Cambridge, 2011.

[56] Neumann, B. H. Twisted wreath products of groups. *Archiv der Mathematik* **14** (1963), 1–6.

[57] Pálfy, P. P.; Pyber, L. Small groups of automorphisms, *Bull. London Math. Soc.* **30** (1998), 386–390.

[58] 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), 197–219.

[59] Pyber, L. On the orders of doubly transitive permutation groups, elementary estimates. *J. Combin. Theory Ser. A* **62** (1993), no. 2, 361–366.

[60] Pyber, L. personnel communication, Bielefeld, 2017.

[61] Rasala, R. On the minimal degrees of characters of $S_n$, *J. Algebra* **45** (1977), 132–181.

[62] Scott, L. L. Representations in characteristic $p$. The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979),*Proc. Sympos. Pure Math.* **37** (1980), 319–331.

[63] Seress, Á. The minimal base size of primitive solvable permutation groups. *J. Lond. Math. Soc.* (2) **53** (1996), no. 2, 243–255.

[64] Seress, Á. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc.* **29** (1997), 697–704.

[65] Seress, Á. Permutation group algorithms. Cambridge Tracts in Mathematics, 152. Cambridge University Press, Cambridge, 2003.

[66] Sims, C. C. Determining the conjugacy classes of a permutation group. *Computers in Algebra and Number Theory* (1971), 191–195.

[67] Suprunenko, D. A. *Matrix groups*, Amer. Math. Soc., Providence, RI, 1976.

[68] The GAP Group, *Groups, Algorithms, and Programming*, 2014.