Combinatorial Aspects of Finite Linear Groups

DSc dissertation

Attila Maróti

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences

Budapest, Hungary

maroti.attila@renyi.mta.hu

2017

dc_1451_17

Contents

1 Introduction

Group actions on sets and vector spaces are an indispensable and powerful tool to answer many questions in different areas of mathematics. The latter gives rise to representation theory. Both group theory and representation theory are among the oldest and most active branches of modern mathematics.

Groups manifest themselves as symmetry groups of various physical systems, such as crystals, atoms and molecules. Thus group theory and the closely related representation theory have many applications in physics and chemistry.

One of the highlights of twentieth century mathematics is the celebrated Classification Theorem of Finite Simple Groups, announced in 1983 and completed in 2004. This theorem is notable not only for the wealth of the ideas involved in proving it but also for the number of applications it has. It is a work of over a hundred mathematicians over a period of a century.

One may think that this massive theorem put an end to finite group theory. This is certainly not the case. Tremendous effort has been made not only to shorten the proof of the theorem, but to better understand the properties of finite simple groups for the various applications. There are statements in finite group theory for which, mysteriously, the only proof known is via the classification. At the time when the proof of the classification theorem was foreseen, Richard Brauer was asked whether this would be the end of finite group theory. He said "this is just the beginning".

Indeed, in the representation theory of finite groups, for example, the Classification Theorem of Finite Simple Groups became a major and indispensable tool in attacking several deep conjectures. In the past decade there has been significant progress towards the solutions of McKay's conjecture, Alperin's weight conjecture, and Brauer's height zero conjecture.

The topic of this thesis lies on the borderline of finite group theory and the representation theory of finite groups. The central theme is finite groups acting on finite vector spaces. We use structural information and representation theoretic tools to study special invariants of finite groups such as size, number of conjugacy classes, base size, number of certain characters, dimension of fixed point spaces. The thesis is influenced indirectly but significantly by problems of Brauer.

We begin with a problem of Brauer whose roots are more than a century old.

A group acts on itself by conjugation and the orbits of this action are called the conjugacy classes of the group. For a finite group G we denote the number of conjugacy

classes of G by $k(G)$. One reason why this invariant is important in finite group theory is that it is equal to the number of complex irreducible characters of the group.

Answering a question of Frobenius, Landau [70] proved in 1903 that for a given k there are only finitely many finite groups having k conjugacy classes. Making this result explicit, we have $k(G) > \log\log|G|$ for any non-trivial finite group G (see Brauer [6], Erdős and Turán [20], Newman [88]). (Here and throughout the thesis the base of the logarithms will always be 2 unless otherwise stated.) Problem 3 of Brauer's famous list of problems [6] is to give a substantially better lower bound for $k(G)$ than this.

The first general lower bound, beyond the methods of Landau, for the number of conjugacy classes of an arbitrary finite group, was obtained by Pyber in [94] where it is shown that there exists a universal constant $\epsilon > 0$ such that every finite group of order at least $n \geq 4$ has at least $\epsilon \cdot (\log n/(\log\log n)^8)$ conjugacy classes. In 2011 Keller [61] improved an ingredient of Pyber's proof concerning solvable groups. In particular he showed that there exists a universal constant $c > 0$ such that every finite solvable group G with trivial Frattini subgroup satisfies $k(G) \geq |G|^c$. This enabled him to show that there exists a universal constant $\epsilon > 0$ such that the following two statements hold: every finite group G of order $n \geq 4$ has at least $\epsilon \cdot (\log n/(\log\log n)^7)$ conjugacy classes, furthermore if G is solvable then it has at least $\epsilon \cdot (\log n/\log\log n)$ conjugacy classes.

In [4] (but not in this thesis) we obtain the strongest lower bound to date for the number of conjugacy classes of an arbitrary finite group in terms of its order.

Theorem 1.1 (Baumeister, Maróti, Tong-Viet; [4]). *For every $\epsilon > 0$ there exists a $\delta > 0$ such that every finite group of order $n \geq 4$ has at least $\delta \cdot (\log n/(\log\log n)^{3+\epsilon})$ conjugacy classes.*

The conjecture whether there exists a universal constant $c > 0$ such that $k(G) > c\log|G|$ for any finite group G has been intensively studied by many mathematicians including Bertram. He speculates whether $k(G) > \log_3|G|$ is true for every finite group G. In [4] (but not in this thesis) we answer Bertram's question in the affirmative for groups with a trivial solvable radical.

Theorem 1.2 (Baumeister, Maróti, Tong-Viet; [4]). *Let G be a finite group with a trivial solvable radical. Then $k(G) > \log_3|G|$.*

Brauer's above-mentioned Problem 3 has a modular version and this is Problem 21 (see [6]). To state this problem we will need some definitions.

Brauer initiated the study of the modular representation theory of finite groups. Among many objects he introduced the notion of a block and a defect group. Let G be a finite group, p a prime, and F an algebraically closed field of characteristic p. A (p-)block of G is defined to be a minimal two sided ideal of the group algebra FG. For every simple FG-module M there is a unique block B of G which does not annihilate M. In this case we say that M belongs to or is contained in B. It is also said that the Brauer character of M is contained in B. A Brauer character of G is a certain complex valued

class function on the set of so-called p-regular elements of G, that is, on the set of those elements of G which have orders not divisible by p. This suggests a way to associate a complex irreducible character χ of G to a block B of G. Let $\hat{\chi}$ be the class function of G obtained by restricting χ to the set of p-regular elements of G. It turns out that $\hat{\chi}$ is not only the sum of Brauer characters of G, but the sum of such Brauer characters of G which belong to a unique block B of G. In this case we say that χ belongs to B. Finally let $k(B)$ denote the number of complex irreducible characters of G which belong to the block B.

The invariant $k(B)$ is closely related to the size of a defect group of B. Loosely speaking, a defect group of a block B is a Sylow p-subgroup of the centralizer of a certain element of G which can be associated to B. Alternatively, the block B, viewed as an $F[G \times G]$-module, has a vertex which is a diagonal subgroup of $G \times G$ whose projection to any of the two coordinates is a p-subgroup, called a defect group of B. (Here, by definition, B is an indecomposable $F[G \times G]$-module, and a vertex Q of B is defined to be a p-subgroup of $G \times G$, unique up to conjugacy in $G \times G$, such that B is a direct summand of $(B_H)^{G \times G}$ for a subgroup H of $G \times G$, if and only if, H contains a conjugate of Q.) This means that the set of defect groups of a block of G form a single conjugacy class of p-subgroups in G. The size $|D| = p^d$ of a defect group D of a block B of a finite group G is a measure of the deviation of B, as an algebra, from being semisimple. The integer d is called the defect of B.

In Problem 21 of his famous list of problems, Brauer [6] asks for a lower bound $f(|D|)$ for $k(B)$, where D is a defect group of the p-block B of a finite group G, such that $f(|D|) \to \infty$ as $|D| \to \infty$. This conjecture was solved for p-solvable groups G by Külshammer [68]. In this thesis we aim to give a weaker but explicit lower bound, not for $k(B)$, but for $k(G)$.

Let G be a finite group such that the order of G contains a prime p with exact exponent 1. Pyber observed that results of Brauer [5] imply that G contains at least $2\sqrt{p-1}$ conjugacy classes. Motivated by this observation Pyber asked various questions concerning lower bounds for $k(G)$ in terms of the prime divisors of $|G|$. In response to these questions (and motivated by trying to find explicit lower bounds for the number of complex irreducible characters in a block) Héthelyi and Külshammer obtained various results [48], [49] for solvable groups. For example they proved in [48] that every solvable finite group G whose order is divisible by p has at least $2\sqrt{p-1}$ conjugacy classes. Later Malle [77, Section 2] showed that if G is a minimal counterexample to the inequality $k(G) \geq 2\sqrt{p-1}$ with p dividing $|G|$ then G has the form HV where V is an irreducible faithful H-module for a finite group H with $(|H|, |V|) = 1$ where p is the prime dividing $|V|$. He also showed that H cannot be an almost quasisimple group. Using these results, Keller [60] showed that there exists a universal constant C so that whenever $p > C$ then $k(G) \geq 2\sqrt{p-1}$. In a later paper Héthelyi, Horváth, Keller and Maróti [47] proved that by disregarding at most finitely many non-solvable p-solvable groups G, we have $k(G) \geq 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$. However since the constant C in Keller's theorem was unspecified, there

had been no quantitative information on what was meant by at most finitely many in the afore-mentioned theorem.

In this thesis we answer this question for all primes p.

Theorem 1.3 (Maróti; [83]). *Every finite group G whose order is divisible by a prime p has at least $2\sqrt{p-1}$ conjugacy classes. Equality occurs if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$.*

Can a stronger lower bound for $k(G)$ be given in case a higher (than 1) power of the prime p divides the order of a finite group G? Héthelyi and Külshammer [49] proved that if G is a finite solvable group whose order is divisible by the square of a prime p then $k(G) \geq (49p+1)/60$. However this line of thought has a limit in view of an example of Kovács and Leedham-Green [63] of groups G of orders p^p (p odd) with $k(G) = \frac{1}{2}(p^3 - p^2 + p + 1)$ (see also [94]).

Going back to blocks, Héthelyi and Külshammer [48, Page 671] asks whether $k(B) \geq 2\sqrt{p-1}$ holds for any p-block B of positive defect for any finite group. No general result is known about this question.

Problem 21 of Brauer and also the above-mentioned results of Héthelyi and Külshammer are closely linked to the so-called McKay conjecture. Let p be a prime and G a finite group. Denote the set of complex irreducible characters of G whose degrees are prime to p by $\mathrm{Irr}_{p'}(G)$. The McKay conjecture (in its original form) states that $|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(N_G(P))|$ where $N_G(P)$ is the normalizer of a Sylow p-subgroup P in G. This conjecture is known for various classes of finite groups including solvable groups and more generally including p-solvable groups. Here we only mention a paper by Isaacs, Malle, Navarro [58] in which McKay's conjecture was reduced to a set of questions on quasisimple groups. (Following this influential paper other deep conjectures in the representation theory of finite groups were recently reduced to certain problems about quasisimple groups.) Using [58] Malle and Späth [79] very recently established McKay's conjecture for $p = 2$.

There is a (stronger) block version of McKay's conjecture which was shown [69] to imply Brauer's Problem 21.

Theorem 1.3 and its proof can be used (but not in this thesis) to bound $|\mathrm{Irr}_{p'}(G)|$ for any finite group G and prime p.

Theorem 1.4 (Malle, Maróti; [78]). *Let G be a finite group and p a prime divisor of the order of G. Then $|\mathrm{Irr}_{p'}(G)| \geq 2\sqrt{p-1}$.*

Our proof of Theorem 1.4 shows that $|\mathrm{Irr}_{p'}(G)|$ is smallest possible for a finite group G whose order is divisible by a prime p if and only if the normalizer of a Sylow p-subgroup of G has a certain special structure. This may be natural in view of the (unsolved) McKay conjecture. In [78] there is a complete description of finite groups G with the property that $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$ for a prime divisor p of the order of G, consistent with the McKay conjecture.

For any prime p with $\sqrt{p-1}$ an integer there are in fact infinitely many finite solvable groups G with $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$. We remark that it is an open problem first posed by Landau whether there are infinitely many primes p with $\sqrt{p-1}$ an integer.

So far we discussed topics on lower bounds for the number of conjugacy classes of a finite group. There are also questions on precise formulas for $k(G)$ where G is a finite group. A famous open problem due to Higman asks if the number of conjugacy classes in the group of n-by-n unipotent upper triangular matrices over the field with q elements can be expressed as a polynomial function of q for every fixed n. This problem has a long history and here we only mention one recent publication, that of Halasi and Pálfy [44].

There are many upper bounds in the literature for $k(G)$ where G is a finite group and these seem to originate from one of the deepest unsolved problems of representation theory. Brauer's $k(B)$ problem [7] was posed in 1959 and is the following. If B is any block of any finite group, then $k(B) \leq |D|$ where D is a defect group of B. It is known [7] that $k(B) \leq (1/4)|D|^2 + 1$. In 1962 Nagao [84] showed that for p-solvable groups the $k(B)$ problem is equivalent to the so-called $k(GV)$ problem which is the following. Let V be a finite faithful FG-module for some finite field F and finite group G. Form the semidirect product GV of V by G and denote the number of conjugacy classes in GV by $k(GV)$. The $k(GV)$ problem is to show that $k(GV) \leq |V|$ whenever $|G|$ is coprime to $|F|$. This bound is sharp when G is a Singer cycle acting on V. Building on a work of Robinson and Thompson [98], the $k(GV)$-problem was eventually solved [31] in 2004 by combined efforts of many mathematicians. The full proof is approximately 500 journal pages long. Schmid has written a book [100] about the solution of this problem. The so-called non-coprime $k(GV)$ problem [42] is stated and considered (see also [38]) in order to generalize the previous works and to gain deeper understanding of Brauer's $k(B)$-problem.

We remark here that there are ongoing efforts, in the spirit of [58], to reduce Brauer's $k(B)$ problem to questions on linear group actions and questions on quasisimple groups.

An important special case and tool in the proof of the $k(GV)$ theorem, the non-coprime $k(GV)$ problem, and beyond is to bound $k(G)$ when G is a permutation group of degree n. Kovács and Robinson [65] proved that $k(G) \leq 5^{n-1}$ and reduced the proposed bound of $k(G) \leq 2^{n-1}$ to the case when G is an almost simple group. This latter bound was later proved by Liebeck and Pyber [72] for arbitrary finite groups G. Kovács and Robinson [65] also proved that $k(G) \leq 3^{(n-1)/2}$ for G a solvable permutation group of degree $n \geq 3$. Later Riese and Schmid [97] proved the same bound for $3'$, $5'$ and $7'$-groups, and in [82] Maróti obtained the bound $k(G) \leq 3^{(n-1)/2}$ for an arbitrary finite permutation group G of degree $n \geq 3$.

By imposing restrictions on the set of composition factors of the permutation group G, one can obtain stronger bounds on $k(G)$. For example, in [82] it was shown that $k(G) \leq (5/3)^n$ whenever G has no composition factor isomorphic to C_2, and more recently Schmid [99] proved that $k(G) \leq 7^{(n-1)/4}$ for $n \geq 5$ where G has no non-Abelian composition factor isomorphic to an alternating group or a group in [10]. However it

seems hard to generalize these bounds for arbitrary groups. In this thesis the following is proved.

Theorem 1.5 (Garonzi, Maróti; [28]). *A permutation group of degree $n \geq 4$ has at most $5^{(n-1)/3}$ conjugacy classes.*

The direct product of $n/4$ copies of S_4 or D_8 is a permutation group of degree n with exactly $5^{n/4}$ conjugacy classes (whenever n is a multiple of 4). But even more can be said. Pyber has pointed out (see [65] and also [72]) that for each constant $0 < c < 5^{1/4}$ there are infinitely many transitive permutation groups G with $k(G) > c^{n-1}$. In fact, G can be taken to be the transitive 2-group $D_8 \wr C_{n/4} \leq S_n$ whenever n is a power of 2 at least 4. (This can be seen by (1) of Lemma 3.1.)

For special subgroups of primitive permutation groups G, one may give better than exponential bounds for $k(G)$. A transitive permutation group G is called primitive if the stabilizer of any point is a maximal subgroup in G. This is equivalent to saying that the only blocks of imprimitivity for G are the singleton sets and the whole set on which G acts. The symmetric group S_n is always primitive and it is easy to see that $k(S_n) = p(n)$, the number of partitions of n. Hardy and Ramanujan [46] and independently but later Uspensky [109] gave an asymptotic formula for $p(n)$ and this is less than exponential. It is a natural question whether $k(G) \leq p(n)$ for any primitive permutation group of degree n. This was shown to be true for sufficiently large n by Liebeck and Pyber [72] and later for all normal subgroups of all primitive groups by Maróti [81]. In this thesis we go even further by showing that for any subgroup H of any primitive permutation group G of degree n, apart from the alternating group A_n and S_n, we have $k(H) \leq p(n)$ (see Theorem 3.4). This result is used to give a general upper bound for $k(G)$ for a transitive permutation group G from knowledge of the partition function (see Theorem 3.6). Finally, this result is used to derive Theorem 1.5.

Weaker bounds as in Theorem 1.5 were used in key steps of the solution of the $k(GV)$ problem. This fact may seem natural to the reader, however the proof of the $k(GV)$ theorem remains mysterious. The general idea is that if V is a vector space on which a finite group G acts with $(|G|, |V|) = 1$ and if V contains a (single) vector v such that $C_G(v)$ has a suitable property then we automatically have $k(GV) \leq |V|$. Such conditions on centralizers are called centralizer criteria. From the several centralizer criteria developed towards the proof of the $k(GV)$ theorem here we mention an unexpected consequence of one of these. Halasi and Podoski [45] showed that if G is a finite group acting faithfully on a finite vector space V with $(|G|, |V|) = 1$, then there exist v, w in V such that $C_G(v) \cap C_G(w) = 1$.

This result of Halasi and Podoski [45] can be viewed as a theorem on base size. For a finite permutation group $H \leq \mathrm{Sym}(\Omega)$, a subset of the finite set Ω is called a base, if its pointwise stabilizer in H is the identity. The minimal base size of H (on Ω) is denoted by $b(H)$. Notice that $|H| \leq |\Omega|^{b(H)}$.

One of the highlights of the vast literature on base sizes of permutation groups is the

celebrated paper of Seress [104] in which it is proved that $b(H) \leq 4$ whenever H is a solvable primitive permutation group. Since a solvable primitive permutation group is of affine type, this result is equivalent to saying that a solvable irreducible linear subgroup G of $GL(V)$ has a base of size at most 3 (in its natural action on V) where V is a finite vector space.

There are a number of results on base sizes of linear groups. For example, Gluck and Magaard [30, Corollary 3.3] have shown that a subgroup G of $GL(V)$ with $(|G|, |V|) = 1$ admits a base of size at most 94. If in addition it is assumed that G is supersolvable or of odd order then $b(G) \leq 2$ by results of Wolf [116, Theorem A] and Dolfi [15, Theorem 1.3]. Later Dolfi [16, Theorem 1.1] and Vdovin [111, Theorem 1.1] generalized this result to solvable coprime linear groups. Finally, Halasi and Podoski [45, Theorem 1.1] improved this result significantly, by proving that even the solvability assumption can be dropped, and $b(G) \leq 2$ for any coprime linear group G.

We note that for a solvable subgroup G of $GL(V)$ acting completely reducibly on V we have $b(G) \leq 2$ if the Sylow 2-subgroups of GV are Abelian (see [17, Theorem 2]) or if $|G|$ is not divisible by 3 (see [117, Theorem 2.3]).

The following definition has been introduced by Liebeck and Shalev in [73]. For a linear group $G \leq GL(V)$ we say that $\{v_1, \ldots, v_k\} \subseteq V$ is a strong base for G if any element of G fixing $\langle v_i \rangle$ for every $1 \leq i \leq k$ is a scalar transformation. The minimal size of a strong base for G is denoted by $b^*(G)$. It is known that $b(G) \leq b^*(G) \leq b(G) + 1$ (see [73, Lemma 3.1]). Furthermore, also $b^*(G) \leq 2$ holds for coprime linear groups by [45, Lemma 3.3 and Theorem 1.1].

The following theorem generalizes the above-mentioned result of Seress [104] and extends that of Halasi and Podoski [45] to p-solvable groups.

Theorem 1.6 (Halasi, Maróti; [43])**.** *Let V be a finite vector space over a field of order q and of characteristic p. If $G \leq GL(V)$ is a p-solvable group acting completely reducibly on V, then $b^*(G) \leq 2$ unless $q \leq 4$. Moreover if $q \leq 4$ then $b^*(G) \leq 3$.*

We note that the bounds in Theorem 1.6 are best possible for all values of q. Indeed, there are infinitely many irreducible solvable linear groups $G \leq GL(V)$ with $|G| > |V|^2$ for $q = 2$ or 3 (see [89, Theorem 1] or [115, Proposition 3.2]) and there are even infinitely many odd order completely reducible linear groups $G \leq GL(V)$ with $|G| > |V|$ for $q \geq 5$ (see [90, Theorem 3B] and the remark that follows). For $q = 4$ we note that [27] shows that there are primitive, irreducible solvable linear subgroups H of $\mathrm{GL}_3(4)$ with $b(H) = 3$ and thus there are infinitely many imprimitive, irreducible solvable linear groups $G = H \wr S \leq \mathrm{GL}_{3r}(4)$ with $b(G) = 3$ where S is a solvable transitive permutation group of degree r.

Theorem 1.6 has been applied in [11] to Gluck's conjecture.

One of the motivations of Seress [104] was a famous result of Pálfy [89, Theorem 1] and Wolf [115, Theorem 3.1] from 1982 stating that a solvable primitive permutation group of degree n has order at most $24^{-1/3} n^{1+c_1}$ where $c_1 = \log_9(48 \cdot 24^{1/3}) = 2.243\ldots$,

that is to say, a solvable irreducible subgroup G of $GL(V)$ has size at most $24^{-1/3}|V|^{c_1}$. (This bound is attained for infinitely many groups.) In the following we generalize this result to p-solvable linear groups G.

Theorem 1.7 (Halasi, Maróti; [43]). *Let V be a finite vector space over a field of characteristic p. If $G \leq GL(V)$ is a p-solvable group acting completely reducibly on V, then $|G| \leq 24^{-1/3}|V|^{c_1}$ where c_1 is as above.*

Theorem 1.7 will be used to show the more general Theorem 1.12, however this latter result has a long story. The core of the proofs of the following results involve finite linear group actions.

Aschbacher and Guralnick showed [3] that if A is a finite permutation group of degree n and A' is its commutator subgroup, then $|A : A'| \leq 3^{n/3}$, furthermore if A is primitive, then $|A : A'| \leq n$. These results were motivated by a problem in Galois theory. For another motivation we need a definition. Let $\mathcal{N}$ be a normal series for a finite group X such that every quotient in $\mathcal{N}$ either involves only noncentral chief factors or is an elementary Abelian group with at least one central chief factor. Define $\mu(\mathcal{N})$ to be the product of the exponents of the quotients which involve central chief factors. Let $\mu(X)$ be the minimum of the $\mu(\mathcal{N})$ for all possible choices of $\mathcal{N}$. This invariant is an upper bound for the exponent of X/X'. In [34] it was shown that if A is a permutation group of degree n, then $\mu(A) \leq 3^{n/3}$, furthermore if A is transitive, then $\mu(A) \leq n$, and if A is primitive with $A'' \neq 1$, then the exponent of A/A' is at most $2 \cdot n^{1/2}$. These results were also motivated by Galois theory. In this thesis we prove similar statements.

Let G be a normal subgroup of a permutation group A of finite degree n. In this thesis the factor group A/G is studied. It is often assumed that G is transitive (this is very natural from the point of view of Galois groups and the results are much weaker without this assumption). As mentioned earlier, throughout the thesis the base of the logarithms is 2 unless otherwise stated.

Theorem 1.8 (Guralnick, Maróti, Pyber; [40]). *Let G and A be permutation groups of finite degree n with $G \lhd A$. Suppose that G is primitive. Then $|A/G| < n$ unless G is an affine primitive permutation group and the pair $(n, A/G)$ is $(3^4, \mathrm{O}_4^-(2))$, $(5^4, \mathrm{Sp}_4(2))$, $(3^8, \mathrm{O}_6^-(2))$, $(3^8, \mathrm{SO}_6^-(2))$, $(3^8, \mathrm{O}_6^+(2))$, $(3^8, \mathrm{SO}_6^+(2))$, $(5^8, \mathrm{Sp}_6(2))$, $(3^{16}, \mathrm{O}_8^-(2))$, $(3^{16}, \mathrm{SO}_8^-(2))$, $(3^{16}, \mathrm{O}_8^+(2))$, or $(3^{16}, \mathrm{SO}_8^+(2))$. Moreover if A/G is not a section of $\Gamma\mathrm{L}_1(q)$ when $n = q$ is a prime power, then $|A/G| < n^{1/2} \log n$ for $n \geq 2^{14000}$.*

The $n - 1$ bound in Theorem 1.8 is sharp when n is prime and G is a cyclic group of order n. For more information about the eleven exceptions in Theorem 1.8 and for a few other examples see Section 5.2. Note that for every prime p there are infinitely many primes r such that the primitive permutation group $G \leq \mathrm{A}\Gamma\mathrm{L}_1(q)$ of order $np = qp = r^{p-1}p$ satisfies $|N_{\mathrm{S}_n}(G)/G| = (n-1)(p-1)/p$. It will also be clear from our proofs that the bound $n^{1/2} \log n$ in Theorem 1.8 is asymptotically sharp apart from a constant factor at least $\log_9 8$ and at most 1.

We next consider the size of the outer automorphism group $\mathrm{Out}(G)$ of a primitive subgroup G of the finite symmetric group S_n.

Theorem 1.9 (Guralnick, Maróti, Pyber; [40]). *Let $G \leq \mathrm{S}_n$ be a primitive permutation group. Then $|\mathrm{Out}(G)| < n$ unless G is an affine primitive permutation group and one of the following holds.*

1. *$n = 3^4$, $G = (C_3)^4 : (D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_4^-(2)$.*
2. *$n = 5^4$, $G = (C_5)^4 : (C_4 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{Sp}_4(2)$.*
3. *$n = 3^8$, $G = (C_3)^8 : (D_8 \circ D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_6^-(2)$.*
4. *$n = 3^8$, $G = (C_3)^8 : (D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_6^+(2)$.*
5. *$n = 5^8$, $G = (C_5)^8 : (C_4 \circ D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{Sp}_6(2)$.*
6. *$n = 3^{16}$, $G = (C_3)^{16} : (D_8 \circ D_8 \circ D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_8^-(2)$.*
7. *$n = 3^{16}$, $G = (C_3)^{16} : (D_8 \circ D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_8^+(2)$.*
8. *$n = q^2$ with $q = 2^e$, $e > 1$, $G = (C_2)^{2e} : \mathrm{L}_2(q)$ and $|\mathrm{Out}(G)| = q(q-1)e$.*

If G is any of the groups in (1)-(7) of Theorem 1.9, then $\mathrm{Out}(G) \cong N_{\mathrm{S}_n}(G)/G$. This indicates why there are only seven exceptional groups in the statement of Theorem 1.9 and not eleven as in the statement of Theorem 1.8. (For in four cases in Theorem 1.8 the group A has index 2 in $N_{\mathrm{S}_n}(G)$.)

Next we state an asymptotic version of Theorem 1.9. For this we need a definition. Let $\mathcal{C}$ be the class of all affine primitive permutation groups G with an almost simple point-stabilizer H with the property that the socle $\mathrm{Soc}(H)$ of H acts irreducibly on the socle of G and $\mathrm{Soc}(H)$ is isomorphic to a finite simple classical group such that its natural module has dimension at most 6.

Theorem 1.10 (Guralnick, Maróti, Pyber; [40]). *Let $G \leq \mathrm{S}_n$ be a primitive permutation group. Suppose that if $n = q$ is a prime power then G is not a subgroup of $\mathrm{A\Gamma L}_1(q)$. If G is not a member of the infinite sequence of examples in Theorem 1.9, then $|\mathrm{Out}(G)| < 2 \cdot n^{3/4}$ for $n \geq 2^{14000}$. Moreover if G is not a member of $\mathcal{C}$, then $|\mathrm{Out}(G)| < n^{1/2} \log n$ for $n \geq 2^{14000}$.*

As mentioned earlier, the bound $n^{1/2} \log n$ in Theorem 1.10 is asymptotically sharp apart from a constant factor close to 1.

The proof of Theorem 1.8 requires a careful analysis of the Abelian and the non-Abelian composition factors of A/G where A and G are finite groups. For this purpose for a finite group X we denote the product of the orders of the Abelian and the non-Abelian composition factors of a composition series for X by $a(X)$ and $b(X)$ respectively. (The latter invariant is different from the minimal base size defined earlier.) Clearly $|X| = a(X)b(X)$.

The next result deals with $b(A/G)$ in the general case when G is transitive and in the more special situation when G is primitive.

Theorem 1.11 (Guralnick, Maróti, Pyber; [40]). *Let A and G be permutation groups with $G \lhd A \leq \mathrm{S}_n$. If G is transitive, then $b(A/G) \leq n^{\log n}$. If G is primitive, then $b(A/G) \leq (\log n)^{2 \log \log n}$.*

In order to give a sharp bound for $a(A/G)$ when G is a primitive permutation group, interestingly, it is first necessary to bound $a(A)$ (for A primitive). As mentioned earlier, in 1982 Pálfy [89] and Wolf [115] independently showed that $|A| \leq 24^{-1/3} n^{1+c_1}$ for a solvable primitive permutation group A of degree n. Equality occurs infinitely often. In fact $a(A) \leq 24^{-1/3} n^{1+c_1}$ holds [95] for any primitive permutation group A of degree n. Using the Classification Theorem of Finite Simple Groups we extend these results to the following, where for a finite group X and a prime p we denote the product of the orders of the p-solvable composition factors of X by $a_p(X)$.

Theorem 1.12 (Guralnick, Maróti, Pyber; [40]). *Let $G \leq \mathrm{S}_n$ be primitive, let p be a prime divisor of n and let c_1 be as before. Then $a_p(G)|\operatorname{Out}(G)| \leq 24^{-1/3} n^{1+c_1}$.*

Wolf [115] also showed that if G is a finite nilpotent group acting faithfully and completely reducibly on a finite vector space V, then $|G| \leq |V|^{c_2}/2$ where c_2 is the constant $\log_9 32$ close to 1.57732. In order to generalize this result we set $c(X)$ to be the product of the orders of the central chief factors in a chief series of a finite group X. In particular we have $c(X) = |X|$ for a nilpotent group X. The following theorem (whose proof is omitted from this thesis) extends Wolf's result.

Theorem 1.13 (Guralnick, Maróti, Pyber; [40]). *Let $G \leq \mathrm{S}_n$ be a primitive permutation group. Then $c(G) \leq n^{c_2}/2$ where c_2 is as above.*

The invariant $\operatorname{ncf}(G) := |G|/c(G)$ will be investigated later.

Some technical, module theoretic results enable us to show that if $G \lhd A \leq \mathrm{S}_n$ are transitive permutation groups, then $a(A/G) \leq 6^{n/4}$ (see Theorem 5.22). In fact, we show that $a(A/G) \leq 4^{n/\sqrt{\log n}}$ whenever $n \geq 2$ (see Theorem 5.24). This together with Theorem 1.11 give the following.

Theorem 1.14 (Guralnick, Maróti, Pyber; [40]). *We have $|A : G| \leq 4^{n/\sqrt{\log n}} \cdot n^{\log n}$ whenever G and A are transitive permutation groups with $G \lhd A \leq \mathrm{S}_n$ and $n \geq 2$.*

For an exponential bound in Theorem 1.14 we can have $168^{(n-1)/7}$ (see Theorem 5.33). See [95, Proposition 4.3] for examples of transitive p-groups (p a prime) showing that Theorem 1.14 is essentially the best one could hope for apart from the constant 4. It is also worth mentioning that a $c^{n/\sqrt{\log n}}$ type bound fails in case we relax the condition $G \lhd A$ to $G \lhd\lhd A$. Indeed, if A is a Sylow 2-subgroup of S_n for n a power of 2 and G is a regular elementary Abelian subgroup inside A, then $|A : G| = 2^n/2n$. The next result shows that an exponential bound in n holds in general for the index of a transitive subnormal subgroup of a permutation group of degree n.

Theorem 1.15 (Guralnick, Maróti, Pyber; [40]). *Let $G \lhd\lhd A \leq \mathrm{S}_n$. If G is transitive, then $|A : G| \leq 5^{n-1}$.*

The proof of Theorem 1.15 is omitted from this thesis and it avoids the use of the Classification Theorem for Finite Simple Groups. Using the classification it is possible to replace 5^{n-1} from the bound with 3^{n-1}. It would be interesting to know whether $|A : G| \leq 2^n$ holds for transitive permutation groups G and A with $G \lhd\lhd A \leq \mathrm{S}_n$.

We note that we have sharp bounds for $|A : G|$, $b(A/G)$ and $a(A/G)$ in case A is a primitive permutation group of degree n and G is a transitive normal subgroup of A. These are $n^{\log n}$ in the first two cases (see [80] and Theorem 5.10), and it is $24^{-1/3}n^{c_1}$ in the third case (see Corollary 5.17).

Let G be a finite group, F a field, and V a finite dimensional FG-module. If one wishes to bound $k(GV)$ directly, it is necessary to know the number of orbits of G on V, which, by the orbit counting theorem, is the arithmetic mean of the sizes of the fixed point spaces of the elements of G acting on V. Motivated by this observation here we consider a slightly different invariant.

For a non-empty subset S of G we define

$$\operatorname{avgdim}(S, V) = \frac{1}{|S|} \sum_{s \in S} \dim C_V(s)$$

to be the arithmetic average dimension of the fixed point spaces of all elements of S on V. Here $C_V(s)$ is the set of fixed points of s on V. In his 1966 DPhil thesis Neumann [86] conjectured that if V is an irreducible non-trivial FG-module then $\operatorname{avgdim}(G, V) \leq (1/2)\dim V$. This problem was restated in 1977 by Neumann and Vaughan-Lee [87] and was posted in 1982 by Vaughan-Lee in The Kourovka Notebook [66] as Problem 8.5. The conjecture was proved by Neumann and Vaughan-Lee [87] for solvable groups G and also in the case when $|G|$ is invertible in F. Later Segal and Shalev [103] showed that $\operatorname{avgdim}(G, V) \leq (3/4)\dim V$ for an arbitrary finite group G. This was improved by Isaacs, Keller, Meierfrankenfeld, and Moretó [57] to $\operatorname{avgdim}(G, V) \leq ((p+1)/2p)\dim V$ where p is the smallest prime factor of $|G|$. Here we prove the following.

Theorem 1.16 (Guralnick, Maróti; [39])**.** *Let G be a finite group, F a field, and V a finite dimensional FG-module. Let N be a normal subgroup of G that has no trivial composition factor on V. Then* $\operatorname{avgdim}(Ng, V) \leq (1/p)\dim V$ *for every $g \in G$ where p is the smallest prime factor of the order of G.*

The previous theorem not only solves the above-mentioned conjecture of Neumann and Vaughan-Lee but it also generalizes and improves the result in many ways. First of all, G need not be irreducible on V; the only restriction we impose is that G has no trivial composition factor on V. Secondly, we prove the bound $(1/2)\dim V$ not just for $\operatorname{avgdim}(G, V)$ but for $\operatorname{avgdim}(S, V)$ where S is an arbitrary coset of a normal subgroup of G with a certain property. Thirdly, Theorem 1.16 involves a better general bound, namely $(1/p)\dim V$ where p is the smallest prime divisor of $|G|$.

We next turn to the question of when we can have equality in Theorem 1.16. Note that the example [57, Page 3129] of a completely reducible FG-module V for an elementary

Abelian p-group G shows that $\operatorname{avgdim}(G,V) = (1/p)\dim V$ can occur in Theorem 1.16. There are examples for equality in Theorem 1.16 even when V is an irreducible module. Let p be an arbitrary odd prime, let G be the extraspecial p-group of order p^{1+2a} (for a positive integer a) of exponent p, let $N = Z(G)$, let F be an algebraically closed field of characteristic different from p, and let V be an irreducible FG-module of dimension p^a. Then for every element $x \in G \setminus N$ we have $\dim C_V(x) = (1/p)\dim V$ and so $\operatorname{avgdim}(Ng,V) = (1/p)\dim V$ for every $g \in G$. In particular we have $\operatorname{avgdim}(H,V) = (1/p)\dim V$ for every subgroup H of G containing N.

We give a different proof of Theorem 1.16 in characteristic 0 and combine the ideas of that proof with Theorem 1.16 to show:

Theorem 1.17 (Guralnick, Maróti; [39]). *Let G be a finite group, F a field, and V a finite dimensional FG-module with no trivial composition factor. Let p be the smallest prime factor of $|G|$. Then* $\operatorname{avgdim}(G,V) = (1/p)\dim V$ *if and only if $G/C_G(V)$ is a group of exponent p.*

In his DPhil thesis [86] Neumann showed that if V is a non-trivial irreducible FG-module for a field F and a finite solvable group G then there exists an element of G with small fixed point space. Specifically, he showed that there exists $g \in G$ with $\dim C_V(g) \leq (7/18)\dim V$. Neumann conjectured that in fact, there should exists $g \in G$ such that $\dim C_V(g) \leq (1/3)\dim V$. Segal and Shalev [103] proved, for an arbitrary finite group G, that there exists an element $g \in G$ with $\dim C_V(g) \leq (1/2)\dim V$. Later, under milder conditions (V is a completely reducible FG-module with $C_V(G) = 0$), Isaacs, Keller, Meierfrankenfeld, and Moretó [57] showed that there exists an element $g \in G$ with $\dim C_V(g) \leq (1/p)\dim(V)$ where p is the smallest prime divisor of $|G|$. Under even weaker conditions we improve this latter result.

Corollary 1.18 (Guralnick, Maróti; [39]). *Let G be a finite group, F a field, and V a finite dimensional FG-module. Let N be a normal subgroup of G that has no trivial composition factor on V. Let x be an element of G and let p be the smallest prime factor of the order of G. Then there exists an element $g \in Nx$ with $\dim C_V(g) \leq (1/p)\dim V$ and there exists an element $g \in N$ with $\dim C_V(g) < (1/p)\dim V$.*

Note that Corollary 1.18 follows directly from Theorem 1.16 just by noticing that $\dim C_V(1) = \dim V$. Note also that if V is irreducible and faithful in Corollary 1.18 then no non-trivial normal subgroup of G has a non-zero fixed point on V and so the N above can be any non-trivial normal subgroup of G. Neumann's above-mentioned conjecture was proved in [37]; if V is a non-trivial irreducible FG-module for a finite group G then there exists an element $g \in G$ such that $\dim C_V(g) \leq (1/3)\dim V$.

We continue with the first application of our result. Let $\mathrm{cl}_G(g)$ denote the conjugacy class of an element g in a finite group G, and for a positive integer n and a prime p let n_p denote the p-part of n. In [57] Isaacs, Keller, Meierfrankenfeld, and Moretó conjecture that for any primitive complex irreducible character χ of a finite group G the degree

of χ divides $|\mathrm{cl}_G(g)|$ for some element g of G. Using their result mentioned before the statement of Corollary 1.18 they showed that if χ is an arbitrary primitive complex irreducible character of a finite solvable group G and p is a prime divisor of $|G|$ then $\chi(1)_p$ divides $(|\mathrm{cl}_G(g)|)^3$ for some $g \in G$. Using Theorem 1.16 we may prove more than this.

Corollary 1.19 (Guralnick, Maróti; [39]). *Let χ be an arbitrary primitive complex irreducible character of a finite solvable group G and let p be a prime divisor of $|G|$. Then the number of $g \in G$ for which $\chi(1)_p$ divides $(|\mathrm{cl}_G(g)|)^3$ is at least $(2|G|)/(1+k)$ where $k = \log_p |G|_p$. Furthermore if $\chi(1)_p > 1$ then there exists a p'-element $g \in G$ for which $p^3 \cdot \chi(1)_p$ divides $(|\mathrm{cl}_G(g)|)^3$.*

Recall that a chief factor of a finite group is a section X/Y of G with $Y < X$ both normal in G such that there is no normal subgroup of G strictly between X and Y. Note that X/Y is a direct product of isomorphic simple groups. If X/Y is Abelian, then it is an irreducible G-module. If X/Y is non-Abelian, then G permutes the direct factors transitively. A chief factor is called central if G acts trivially on X/Y and non-central otherwise. Let G be a finite group acting on another finite group Z by conjugation. For a non-empty subset S of G define

$$\mathrm{geom}(S, Z) = \left(\prod_{s \in S} |C_Z(s)| \right)^{1/|S|}$$

to be the geometric mean of the sizes of the centralizers of elements of S acting on Z. Similarly, for a non-empty subset S of G define

$$\mathrm{avg}(S, Z) = \frac{1}{|S|} \sum_{s \in S} |C_Z(s)|$$

to be the arithmetic mean of the sizes of the centralizers of elements of S acting on Z. Our next result is a non-Abelian version of Theorem 1.16 proved using some recent work of Fulman and Guralnick [25].

Theorem 1.20 (Guralnick, Maróti; [39]). *Let G be a finite group with $X/Y = M$ a non-Abelian chief factor of G with X and Y normal subgroups in G. Then, for any $g \in G$, we find that $\mathrm{geom}(Xg, M) \leq \mathrm{avg}(Xg, M) \leq |M|^{0.41}$.*

In Theorem 1.13 we considered the invariant $c(G)$ for a finite group G. Next we will continue our investigations.

Let $c(G)$ and $\mathrm{ncf}(G)$ be the product of the orders of all central and non-central chief factors (respectively) of a finite group G. (In case these are not defined put them equal to 1.) These invariants are independent of the choice of the chief series of G. Let $F(G)$ denote the Fitting subgroup of G. Note that $F(G)$ acts trivially on every chief factor of G. Using Theorems 1.16 and 1.20 we prove

Theorem 1.21 (Guralnick, Maróti; [39]). *Let G be a finite group. Then*

$$\mathrm{geom}(G, G) \leq c(G) \cdot (\mathrm{ncf}(G))^{1/p}$$

where p is the smallest prime factor (if such exists) of the order of $G/F(G)$.

By taking the reciprocals of both sides of the inequality of Theorem 1.21 and multiplying by $|G|$, we obtain the following result.

Corollary 1.22 (Guralnick, Maróti; [39]). *Let G be a finite group. Then*

$$\mathrm{ncf}(G) \leq \Big(\prod_{g \in G} |\mathrm{cl}_G(g)| \Big)^{p/((p-1)|G|)}$$

where p is the smallest prime factor (if such exists) of the order of $G/F(G)$.

A group is said to be a BFC group if its conjugacy classes are finite and of bounded size. A group G is called an n-BFC group if it is a BFC group and the least upper bound for the sizes of the conjugacy classes of G is n. One of B. H. Neumann's discoveries was that in a BFC group the commutator subgroup G' is finite [85]. One of the purposes of this thesis is to give an upper bound for $|G'|$ in terms of n for an n-BFC group G. Note that $C_G(G')$ is a finite index nilpotent subgroup. Thus, $F(G)$ is well defined for BFC groups.

If G is a BFC group, then there is a finitely generated subgroup H with $H' = G'$ and $G = HC_G(G') = HF(G)$. Then H has a finite index central torsionfree subgroup N. Set $J = H/N$. So J' and G' are G-isomorphic. In particular, $\mathrm{ncf}(J) = \mathrm{ncf}(G)$. Clearly, $G/F(G) \cong J/F(J)$. Thus, for the next result, it suffices to consider finite groups. Our first main theorem on BFC groups follows from Corollary 1.22 (by noticing that $|\mathrm{cl}_G(1)| = 1$ and that in that result, we may always assume the action is faithful).

Theorem 1.23 (Guralnick, Maróti; [39]). *Let G be an n-BFC group with $n > 1$. Then we have $\mathrm{ncf}(G) < n^{p/(p-1)} \leq n^2$, where p is the smallest prime factor (if such exists) of the order of $G/F(G)$.*

Theorem 1.23 solves [87, Conjecture A].

Not long after B. H. Neumann's proof that the commutator subgroup G' of a BFC group is finite, Wiegold [114] produced a bound for $|G'|$ for an n-BFC group G in terms of n and conjectured that $|G'| \leq n^{(1/2)(1+\log n)}$ where the logarithm is to base 2. Later Macdonald [76] showed that $|G'| \leq n^{6n(\log n)^3}$ and Vaughan-Lee [110] proved Wiegold's conjecture for nilpotent groups. For solvable groups the best bound to date is $|G'| \leq n^{(1/2)(5+\log n)}$ obtained by Neumann and Vaughan-Lee [87]. In the same paper they showed that for an arbitrary n-BFC group G we have $|G'| \leq n^{(1/2)(3+5\log n)}$. Using the Classification Theorem of Finite Simple Groups Cartwright [9] improved this bound to $|G'| \leq n^{(1/2)(41+\log n)}$ which was later further sharpened by Segal and Shalev [103]

who obtained $|G'| \leq n^{(1/2)(13+\log n)}$. Applying Theorem 1.23 at the bottom of [103, Page 511] we arrive at a further improvement of the general bound on the order of the derived subgroup of an n-BFC group.

Theorem 1.24 (Guralnick, Maróti; [39]). *Let G be an n-BFC group with $n > 1$. Then we have $|G'| < n^{(1/2)(7+\log n)}$.*

A word ω is an element of a free group of finite rank. If the expression for ω involves k different indeterminates, then for every group G, we obtain a function from G^k to G by substituting group elements for the indeterminates. Thus we can consider the set G_ω of all values taken by this function. The subgroup generated by G_ω is called the verbal subgroup of ω in G and is denoted by $\omega(G)$. An outer commutator word is a word obtained by nesting commutators but using always different indeterminates. In [23] Fernández-Alcober and Morigi proved that if ω is an outer commutator word and G is any group with $|G_\omega| = m$ for some positive integer m then $|\omega(G)| \leq (m-1)^{m-1}$. They suspect that this bound can be improved to a bound close to one obtainable for the commutator word $\omega = [x_1, x_2]$. By noticing that every conjugacy class of a group G has size at most the number of commutators of G we see that Theorem 1.24 yields

Corollary 1.25 (Guralnick, Maróti; [39]). *Let G be a group with m commutators for some positive integer m at least 2. Then $|G'| < m^{(1/2)(7+\log m)}$.*

Segal and Shalev [103] showed that if G is an n-BFC group with no non-trivial Abelian normal subgroup then $|G| < n^4$. We improve and generalize this result in Theorem 1.26. As before, for a finite group X, let $k(X)$ denote the number of conjugacy classes of X.

Theorem 1.26 (Guralnick, Maróti; [39]). *Let G be an n-BFC group with $n > 1$. If the Fitting subgroup $F(G)$ of G is finite, then $|G| < n^2 k(F(G))$. In particular, if G has no non-trivial Abelian normal subgroup then $|G| < n^2$.*

Since $F(G)$ has finite index in G, the hypotheses of Theorem 1.26 imply that G is finite. Note that even more is true than Theorem 1.26; if G is a finite group then $|G| \leq a^2 k(F(G))$ where $a = |G|/k(G)$ is the (arithmetic) average size of a conjugacy class in G (this is [41, Theorem 10 (i)]). If b denotes the maximal size of a set of pairwise non-commuting elements in G then, by Turán's theorem [108] applied to the complement of the commuting graph of G, we have $a < b + 1$. Thus if G is a finite group with no non-trivial Abelian normal subgroup then $|G| < (b+1)^2$. This should be compared with the bound $|G| < c^{(\log b)^3}$ holding for some universal constant c with $c \geq 2^{20}$ which implicitly follows from [93, Lemma 3.3 (ii)] and should also be compared with the remark in [93, Page 294] that for a non-Abelian finite simple group G we have $|G| \leq 27 \cdot b^3$.

The final main result concerns n-BFC groups with a given number of generators. Segal and Shalev [103] proved that in such groups the order of the commutator subgroup is bounded by a polynomial function of n. In particular they obtained the bound $|G'| \leq n^{5d+4}$ for an arbitrary n-BFC group G that can be generated by d elements. By applying Theorem 1.23 to [103, Page 515] we may improve this result.

Corollary 1.27 (Guralnick, Maróti; [39]). *Let G be an n-BFC group that can be generated by d elements. Then $|G'| \leq n^{3d+2}$.*

Finally, the following immediate consequence of Corollary 1.27 sharpens [103, Corollary 1.5].

Corollary 1.28 (Guralnick, Maróti; [39]). *Let G be a d-generator group. Then*

$$|\{[x, y] : x, y \in G\}| \geq |G'|^{1/(3d+2)}.$$

We remark here that every non-Abelian finite simple group G can be generated by 2 elements (see [2]) and, by the recent solution [71] of Ore's conjecture, every element of G is a commutator.

The example $T_m(p)$ [87, Page 213] shows that Theorem 1.24, Corollary 1.25, Corollary 1.27, and Corollary 1.28 are close to best possible.

We point out that Theorem 1.16 for p odd requires only the Feit-Thompson Odd Order Theorem [22]. However, most of the results above depend on the Classification Theorem of Finite Simple Groups as the results in [103] and [57] do (for groups of even order).

Acknowledgement

The author would like to thank his university teacher, Ágnes Szendrei for introducing algebra to him through the many well organized lectures she delivered. He would also like to thank Péter Pál Pálfy for the stimulating group theory courses he held in Szeged. The author thanks László Pyber for the many interesting mathematical problems and for the first discussions about research. The candidate thanks Geoffrey R. Robinson for introducing representation theory to the author.

The author thanks László Pyber, Geoffrey R. Robinson and Robert M. Guralnick for the large number of fruitful discussions about mathematics over the years, and Ágnes Szendrei, Péter Pál Pálfy, László Pyber, Geoffrey R. Robinson, Robert M. Guralnick and Gunter Malle for the constant support and encouragement throughout the years. He also thanks Miklós Abért for support during the time this thesis was prepared.

Last but not least the author thanks the coauthors of those of his papers which are contained in this thesis: Martino Garonzi, Robert M. Guralnick, Zoltán Halasi, and László Pyber.

2 A lower bound for the number of classes

Let p be a prime divisor of the order of G. In a work of Brauer, Pyber noticed that $k(G)$ could perhaps be bounded from below only in terms of p. Héthelyi and Külshammer confirmed this speculation for solvable G. In this chapter we give such an explicit bound, namely $k(G) \geq 2\sqrt{p-1}$, holding for any finite group G. More specifically, we will establish Theorem 1.3. This is related to Brauer's problem 21 which may be viewed as a block version of Brauer's problem 3.

2.1 A reduction to linear groups

Let G be a minimal counterexample to the statement of Theorem 1.3. By [48] (and the equality by [47, Theorem 2.1]) we know that G is not solvable. Also, by [47, Theorem 3.1], we may assume that G is a p-solvable group (whose order is divisible by p). Now we may proceed as in [47, Page 428]. Let V be a minimal normal subgroup in G. If $|G/V|$ is divisible by p then, by the minimality of G, we have $k(G) > k(G/V) \geq 2\sqrt{p-1}$, a contradiction. So p divides $|V|$, and since G is p-solvable, we see that V is an elementary Abelian p-group. By this argument we see that V is the unique minimal normal subgroup of G. By the Schur-Zassenhaus theorem, there is a complement H of V in G. So G has the form HV where V is a coprime, faithful and irreducible H-module.

In the papers [112] and [113] all non-nilpotent finite groups are classified with at most 14 conjugacy classes. By going through these lists of groups we see that no group G of the form described in the previous paragraph is a counterexample to Theorem 1.3. So we have $k(G) \geq 15$. This means that we can assume that $2\sqrt{p-1} \geq 15$ is true. In other words, that $p \geq 59$.

There is a well-known expression for $k(G) = k(HV)$ which is a consequence of the so-called Clifford-Gallagher formula. Let $n(H,V)$ denote the number of H-orbits on V and let $v_1, \ldots, v_{n(H,V)}$ be representatives of these orbits. [100, Proposition 3.1b] says that $k(HV) = \sum_{i=1}^{n(H,V)} k(C_H(v_i))$. This is at least $k(H) + n(H,V) - 1$.

Theorem 1.3 is then a consequence of the following result (with the roles of H and G interchanged).

Theorem 2.1. *Let V be an irreducible and faithful FG-module for some finite group G and finite field F of characteristic p at least 59. Suppose that p does not divide $|G|$. Then we have $k(G) + n(G,V) - 1 \geq 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $|V| = |F| = p$ and $|G| = \sqrt{p-1}$.*

Theorem 2.1 has implicitly been proved in [48] in case G is solvable, without a consideration of when equality can occur.

2.2 Basic results, notation and assumptions

In the rest of the chapter we are going to prove Theorem 2.1. For this purpose let us fix some notation and assumptions.

Let V be an irreducible and faithful FG-module for some finite group G and finite field F of characteristic p. Suppose that p does not divide $|G|$ and it is at least 59. The size of the field F will be denoted by q, the dimension of V over F by n, and the center of $\mathrm{GL}_n(q)$ by Z. We denote the number of orbits of G on V by $n(G,V)$. We will use the following trivial observation throughout the chapter.

Lemma 2.2. *With the notation and assumptions above,* $|V|/|G| \leq n(G,V)$.

However we will also need a more sophisticated lower bound for $n(G,V)$. For this we must introduce some more notation (which will also be valid for the rest of the chapter).

Suppose that G transitively permutes a set $\{V_1,\ldots,V_t\}$ of subspaces of V with t an integer with $1 \leq t \leq n$ as large as possible with the property that $V = V_1 \oplus \cdots \oplus V_t$. Let B be the kernel of this action of G on the set of subspaces. Note that G/B is a transitive permutation group of degree t. The subgroup B is isomorphic to a subdirect product of t copies of a finite group T. In other words B is isomorphic to a subgroup of $T_1 \times \cdots \times T_t$ where for each i with $1 \leq i \leq t$ the vector space V_i is a faithful T_i-module and $T_i \cong T$. Let H_1 be the stabilizer of V_1 in G. Let k be the number of orbits of H_1 on V_1. Then the following is true.

Lemma 2.3. *With the above notation and assumptions,*

$$\max\{t+1,k\} \leq \binom{t+k-1}{k-1} \leq n(G,V).$$

Proof. This is [24, Lemma 2.6]. □

When G is solvable we will also use the following consequence of a result of Seager [102, Theorem 1].

Proposition 2.4. *Let V be a faithful primitive FG-module for a finite solvable group G not contained in $\Gamma L(1,p^n)$ where F is a field of prime order $p \geq 59$ and $|V| = p^n$. Then $p^{n/2}/12n < n(G,V)$.*

As is suggested by Lemma 2.2, in various situations it will be useful to bound the size of G from above. A useful tool in doing so is the following result of Pálfy and Pyber [91, Proposition 4].

Proposition 2.5. *Let X be any subgroup of the symmetric group S_m whose order is coprime to a prime p. If $m > 1$ then $|X| < p^{m-1}$.*

A third means to attack Theorem 2.1 is to bound $k(G)$.

Lemma 2.6. *If G has an Abelian subgroup of index at most $|V|^{1/2}/(2\sqrt{p-1})$ and $n(G,V) \leq 2\sqrt{p-1}$, then $2\sqrt{p-1} \leq k(G)$.*

Proof. If G has an Abelian subgroup A with $|G:A| \leq |V|^{1/2}/(2\sqrt{p-1})$, then

$$|G|(2\sqrt{p-1})/|V|^{1/2} \leq |A|.$$

Now $|A|/|G:A| \leq k(G)$, by a result of Ernest [21, page 502] saying that whenever Y is a subgroup of a finite group X then we have $k(Y)/|X:Y| \leq k(X)$. This gives $(4(p-1)|G|)/|V| \leq k(G)$. Then, by Lemma 2.2, we obtain $2\sqrt{p-1} \leq k(G)$. □

2.3 A special class of linear groups

Our first aim in proving Theorem 2.1 is to describe (as much as possible) the possibilities for G and V with the condition that $n(G,V) < 2\sqrt{q-1}$ where q is the size of the underlying field F. For this we need to introduce a class of pairs (G,V) which we denote by $\mathcal{C}_q$.

In this paragraph we define a class of pairs (G,V) where V is an FG-module. Let W be a not necessarily faithful but coprime QH-module for some finite field extension Q of F and some finite group H. We write $\mathrm{Stab}^Q_{Q_1}(H,W)$ for the class of pairs (H_1,W_1) with the property that W_1 is a Q_1H_1-module with $F \leq Q_1 \leq Q$ where W_1 is just W viewed as a Q_1-vector space and H_1 is some group with the following property. If $\varphi : H_1 \longrightarrow GL(W_1)$ and $\psi : H \longrightarrow GL(W)$ denote the natural, not necessarily injective homomorphisms, then $\varphi(H_1) \cap GL(W) = \psi(H)$. We write $\mathrm{Ind}(H,W)$ for the class of pairs (H_1,W_1) with the property that $W_1 = \mathrm{Ind}^{H_1}_H(W)$ for some group H_1 with $H \leq H_1$. Finally, let $\mathcal{C}_q$ be the class of all pairs (G,V) with the property that V is a finite, faithful, coprime and irreducible FG-module so that (G,V) can be obtained by repeated applications of $\mathrm{Stab}^{Q_2}_{Q_1}$ and Ind starting with (H,W) where W is a 1-dimensional QH-module with Q a field extension of F.

If $(G,V) \in \mathcal{C}_q$ then there exist a sequence of field extensions

$$F_{q_m} \geq F_{q_{m-1}} \geq \ldots \geq F_{q_0} = F,$$

a normal series $1 < N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_{2m-1} = G$, and integers $n_1, \ldots, n_m, n_{m+1} = 1$ so that the following hold. The normal subgroup N_0 of G is a subgroup of the direct product of $\log|V|/\log q_m$ copies of a cyclic group of order $q_m - 1$. For each i with $1 \leq i \leq m$ the factor group N_{2i-1}/N_{2i} is a subgroup of the direct product of $n_i \leq \log|V|/\log q_{m-i+1}$

copies of a cyclic group of order $\log q_{m-i+1}/\log q_{m-i}$ and the factor group N_{2i}/N_{2i-1} is a subgroup of a permutation group on n_i points which is a direct power of n_{i+1} copies of a permutation group on n_i/n_{i+1} points.

The main results of this section are Lemmas 2.7 and 2.8.

Lemma 2.7. *Let $(G,V) \in \mathcal{C}_q$ and $n(G,V) < 2\sqrt{q-1}$. If $q \geq 59$, then $|G| < |V|^{3/2}$.*

Proof. Fix an F_{q_0}-vector space V of dimension n where $q_0 = q$. Suppose that $(G,V) \in \mathcal{C}_q$ with $n(G,V) < 2\sqrt{q-1}$ and G of maximal possible size. Then there exists a sequence of field extensions $F_{q_m} \geq F_{q_{m-1}} \geq \ldots \geq F_{q_0}$ so that

$$|G| \leq (q_m - 1)^{\log|V|/\log q_m} \cdot \Big(\prod_{i=1}^{m} (\log q_i/\log q_{i-1})^{\log|V|/\log q_i} \Big) \cdot p^{\log|V|/\log q_m - 1}$$

where the first factor is equal to the size of the direct product of $\log|V|/\log q_m$ copies of a cyclic group of order $q_m - 1$, the second factor is an upper bound for the product of all the factors with which the sizes of the relevant groups increase by taking normalizers when viewing the linear groups over smaller fields, and the third factor is the product of the sizes of all factor groups (viewed as permutation groups) which arise after inducing smaller modules (this product is at most the size of a p'-subgroup of the symmetric group on $\log|V|/\log q_m$ points which we can bound using Proposition 2.5).

We now proceed to bound the three factors in the product above. The first factor is clearly less than $|V|$. Let us consider the second factor. Define the positive integers $k_1, \ldots, k_m, k_{m+1}$ so that $q_1 = q^{k_1}$, $q_2 = q^{k_1 k_2}, \ldots, q_m = q^{k_1 k_2 \cdots k_m}$, and $|V| = q^{k_1 k_2 \cdots k_m k_{m+1}}$. We may assume that all the k_i's are at least 2 for $1 \leq i \leq m$ (while we allow k_{m+1} to be 1). Then we can write the second factor as

$$\prod_{i=1}^{m} {k_i}^{k_{i+1}\cdots k_{m+1}} \leq \prod_{i=1}^{m} {k_i}^{n/(k_1\cdots k_i)}$$

where $n = \log|V|/\log q$. But by taking logarithms it is easy to see that

$$\prod_{i=1}^{\infty} {n_i}^{1/(n_1\cdots n_i)} \leq 3^{2/3}$$

for any sequence $n_1, n_2, \ldots$ of integers at least 2. Thus the second factor is at most $3^{2n/3} < |V|^{0.18}$ since $q \geq 59$.

Suppose first that $q_m \geq q^4$. Then we can show that $|G| < |V|^{1.39}$. This is clear for $q_m \geq q^{10}$ since the second factor considered above is less than $|V|^{0.18}$ while the third factor is less than $|V|^{1/10}$. By bounding the second factor more carefully in cases $q_m = q^i$ $(4 \leq i \leq 9)$, we see that it is less than $|V|^{0.39-1/i}$.

Thus we may assume that $q_m = q^3, q^2$ or q. In the first two cases $m = 1$ while in the third, $m = 0$.

Suppose that the first case holds. Then we can bound the second factor by $3^{n/3} < |V|^{0.09}$. By Lemma 2.3 and by using the fact that $n(G,V) < 2\sqrt{q-1}$, we certainly have $n/3 < \ell := 2\sqrt{q-1}$. So the third factor is at most

$$(n/3)! < \ell^{n/3} < (4 \cdot q)^{n/6} < |V|^{1/4}$$

since $q \geq 59$. So we get $|G| < |V|^{1.34}$.

Suppose that the second case holds. Then we can bound the second factor by $2^{n/2} < |V|^{0.09}$. By Lemma 2.3 and by using the fact that $n(G,V) < 2\sqrt{q-1}$, we certainly have $n/2 < \ell := 2\sqrt{q-1}$. So the third factor is at most

$$(n/2)! < \ell^{n/2} < (4 \cdot q)^{n/4} < |V|^{0.34}.$$

So we get $|G| < |V|^{1.43}$.

Suppose that the third case holds. Then the second factor is 1. Also, by Lemma 2.3, we can replace the third factor by $n!$ where $n < 2\sqrt{q-1}$. Here $2\sqrt{q-1} \geq 15$. This gives $n! < (\sqrt{q-1})^n < q^{n/2} = |V|^{1/2}$. We get $|G| < |V|^{3/2}$. □

The following can be considered as a refined version of Lemma 2.7.

Lemma 2.8. *Let $(G,V) \in \mathcal{C}_q$ and $n(G,V) < 2\sqrt{q-1}$. If $p \geq 59$, then at least one of the following holds.*

1. *G has an Abelian subgroup of index at most $|V|^{1/2}/(2\sqrt{p-1})$.*
2. *$|F| = p$, the module V is induced from a 1-dimensional module, and G has a factor group isomorphic to A_n or S_n where $n = \dim_F(V)$. In this case we either have $n = 1$, or $15 \leq n \leq 180$ and $p < 8192$.*

Proof. If $G \leq \Gamma L(1, q^n)$, then the result is clear, since $n \leq |V|^{1/2}/(2\sqrt{p-1})$ ((1) is satisfied).

Let us consider the proof (and the notation) of Lemma 2.7. Clearly, an upper bound for the index of an Abelian (subnormal) subgroup of G is the product of the second and third factors. For $q_m \geq q^4$ this was $|V|^{0.39}$, for $q_m = q^3$ this was $|V|^{0.34}$, and for $q_m = q^2$ this was $|V|^{0.43}$. These are at most $|V|^{1/2}/(2\sqrt{p-1})$ unless $n \leq 6$ (in the first case), $n = 3$ (in the second case), and $n \leq 8$ (in the third case). In all these exceptional cases we have $G \leq \Gamma L(1, q^n)$ (the case treated in the previous paragraph) unless $q_m = q^2$ and $n = 4$, 6, or 8. But in all these exceptional cases there exists an Abelian (subnormal) subgroup of index at most $2^n(n/2)! < q^{n/2}/(2\sqrt{p-1})$ where this latter inequality follows from $q \geq p \geq 59$ and $n \leq 8$. Thus (1) is satisfied in all these cases, and we may assume that $q_m = q$ in case $(G,V) \in \mathcal{C}_q$.

Now let t and B be defined for G as in Section 2.2. By Lemma 2.3, we may assume that $t < 2\sqrt{p-1} - 1$. Put ℓ to be the integer part of $2\sqrt{p-1} - 1$. Then it is easy to see that $|G/B| \leq \ell!^{t/\ell} < (\ell/2.2549)^t$ since $p \geq 59$. This gives $|G/B| < 0.89^t \cdot p^{t/2}$.

Suppose that $t = n$. Then G contains an Abelian (normal) subgroup of index less than $0.89^n \cdot p^{n/2} \leq q^{n/2}/(2\sqrt{p-1})$ unless $1.27^n < 4(p-1)$ (in which case this previous inequality fails). By taking logarithms of both sides we get $n < 10 \log p$. But then $|G/B| < ((10/2.2549) \log p)^n < (4.5 \log p)^n$.

Suppose for a contradiction that part (1) fails. Then

$$q^{n/2}/(2\sqrt{p-1}) < |G/B| < (4.5 \log p)^n.$$

This gives $(\sqrt{q}/(4.5 \log p))^n < 2\sqrt{p-1}$. But on the other hand we also have $|G/B| \leq n!$ which, together with our assumption, gives the inequality $p^{n-1} < 4(n!)^2$. Since $p \geq 59$, we certainly have $59^{n-1} < 4(n!)^2$. From this we get $n \geq 15$. Then $(\sqrt{q}/(4.5 \log p))^{15} < 2\sqrt{p-1}$, which forces $q = p < 8192$ and thus $n = t \leq 180$.

It is easy to see that a transitive subgroup of S_n not containing A_n has index at least $3n$ for $n \geq 15$. (This is clear for a primitive subgroup by the bound of Praeger and Saxl [92], while for imprimitive groups a more direct calculation is necessary.) So if G/B does not contain the alternating group A_n, then we can refine our upper bound above for $|G/B|$ by multiplying the result by $1/3n$. But then $9 \cdot n^2 \cdot 1.27^n < 4(p-1)$ follows. However since $n \geq 15$ we also get $73026 < n^2 \cdot 1.27^n < 4(p-1)$ which forces $18257 \leq p$. But this is a contradiction because we already deduced that $p < 8192$. This proves the result in case $t = n$. □

2.4 Some absolutely irreducible representations

As mentioned earlier we will be interested in pairs (G, V) for which $n(G, V) < 2\sqrt{q-1}$. In this section we consider two special cases, the case when G is a central product of an almost quasisimple group H and Z and the case when G is the normalizer of a group of symplectic type. We will also make some more assumptions on the FG-module V.

Proposition 2.9. *Suppose that p is a prime at least 59. Let H be a finite subgroup of $\mathrm{GL}_n(q)$ with generalized Fitting subgroup a quasisimple group where q is a power of p. Put $G = Z \circ H$ where Z is the multiplicative group of F. Furthermore suppose that V is an absolutely irreducible FT-module for every non-central normal subgroup T of G. Suppose also that $|G|$ is not divisible by p. Then $n(G, V) \geq 2\sqrt{q-1}$ unless possibly if $n = 2$, q is in the range $59 \leq q \leq 14389$, it is congruent to ± 1 modulo 10, and $G = Z \circ 2.A_5$.*

Proof. First suppose that H cannot be realized over a proper subfield of F.

In this paragraph suppose also that (n, H) is different from the pairs $(2, 2.A_5)$, $(3, 3.A_6)$, $(3, L_2(7))$, or $(4, 2.S_4(3))$. Let $P(V)$ denote the set of 1-dimensional subspaces of V. Since $|H|$ is not divisible by p and $p \geq 59$, we see by [77, Satz 3.4], that all orbits of G on $P(V)$ have lengths less than $(q^{n-1} - 1)/(q - 1)$. As a result, the number of orbits of G on $P(V)$ is larger than $(q^n - 1)/(q^{n-1} - 1)$. But then $n(G, V)$ is larger than $(q^n - 1)/(q^{n-1} - 1) \geq 2\sqrt{q-1}$.

Suppose that $n = 2$ and $G = Z \circ 2.A_5$. We may assume that $n(G, V) < 2\sqrt{q-1}$. From this we get $|V|/|G| < 2\sqrt{q-1}$. It readily follows that $q < 14400$. Since q must be a prime power, we must have $59 \leq q \leq 14389$. According to Dickson's theorem [54, Kapitel II, 8.27] q must be congruent to ± 1 modulo 10. This accounts for the exception in the statement of the proposition.

Suppose that $n = 3$ and $G = Z \circ 3.A_6$. From the inequality $|V|/|G| < 2\sqrt{q-1}$ it follows that $q \leq 80$. Since q is a prime power, we must have $59 \leq q \leq 79$. However only $p = 61$ is to be considered since $\sqrt{-3}$ and also $\sqrt{5}$ must lie in F. In this case a direct computation shows that there are $21 > 2\sqrt{60}$ orbits of G on $P(V)$.

Suppose that $n = 3$ and $G = Z \times L_2(7)$. From the inequality $|V|/|G| < 2\sqrt{q-1}$ it follows that $q \leq 48$. A contradiction.

Suppose that $n = 4$ and $G = Z \circ 2.S_4(3)$. From the inequality $|V|/|G| < 2\sqrt{q-1}$ it follows that $q \leq 76$. Since q is a prime power, we must have $59 \leq q \leq 73$. However only the cases $p = 61$, 67, and 73 are to be considered since $\sqrt{-3}$ must lie in F. In these cases there are 30, 33, and 43 orbits of G on $P(V)$, respectively. These are all greater than $2\sqrt{72}$.

Now suppose that H can be realized over a proper subfield of F. Then clearly $q \geq 59^2$. Let S be the generalized Fitting subgroup of H which by assumption is quasisimple. We now discuss the possibilities for S according to the classification.

If $n = 2$ then, by Dickson's theorem [54, Kapitel II, 8.27], S is a covering group of A_5 and $H = S$. This is an exception in the statement of the proposition since as before we get $q \leq 14389$ and $q \equiv \pm 1 \pmod{10}$. From now on assume that $n \geq 3$.

Since $q \geq 59^2$, it can easily be checked, just by order considerations and using the fact that $|G|$ is coprime to p, that none of the (generic examples of) groups G with S appearing in Table 2 of [50] have fewer than $2\sqrt{q-1}$ orbits on V. Then, using Table 3 of [51] together with the condition that $q \geq 59^2$, one can check, essentially just by comparing $\log_{10}(q^{n-2})$ and $\log_{10}(|G|)$, that no group G has fewer than $2\sqrt{q-1}$ orbits on V with $n \leq 250$.

So assume that $n > 250$. We can rule out S being a covering group of a sporadic simple group since $|G|$ is much smaller than 59^{498}. For a similar reason as when considering Table 2 of [50], we see that S cannot be a covering group of an alternating group A_m (for we can assume that $m \geq 9$ and so $n \geq m - 2$ by [62, Proposition 5.3.7 (i)]).

Suppose that S is a covering group of a classical group $Cl(d, r)$ where r is a prime power and d is chosen as small as possible (here d is the dimension of the vector space naturally associated to the classical group). If $d \geq 6$ then

$$n \geq \max\{251, (r^{d/2} - 1)/2\}$$

by [62, Corollary 5.3.10 (iv)] and by $n > 250$. But then $q^{n-3} > r^{d^2}$ follows by using the fact that $q \geq 59^2$. This implies that we must have $d \leq 5$.

So suppose that $d \leq 5$. Then [62, Table 5.3.A] shows that $n \geq \max\{251, (r-1)/2\}$.

But then $q^{n-3} > r^{d^2}$ certainly follows for $r \geq 32$. So suppose that $r < 32$. Then $q^{n-3} \geq 59^{496} > 32^{25} \geq r^{d^2}$. This finishes the treatment of the case when S is a covering group of a classical group.

Suppose that S is a covering group of an exceptional simple group of Lie type. Then [62, Tables 5.1.B and 5.3.A] can be used to show that G must have at least $2\sqrt{q-1}$ orbits on V. □

Let us now turn to our second important case of an absolutely irreducible FG-module V. Suppose that the group G has a unique normal subgroup R which is minimal subject to being non-central. Suppose that R is an r-group of symplectic type for some prime r (this is an r-group all of whose characteristic Abelian subgroups are cyclic). Suppose that V is an absolutely irreducible FR-module. Let $|R/Z(R)| = r^{2a}$ for some positive integer a. Then the dimension of the module is $n = r^a$. Suppose that $Z \leq G$. The group $G/(RZ)$ can be considered as a subgroup of the symplectic group $\mathrm{Sp}_{2a}(r)$. As always, we assume that $q \geq p \geq 59$.

Proposition 2.10. *Suppose that V and G satisfy the assumptions of the previous paragraph. If $n(G,V) < 2\sqrt{q-1}$, then $n = 2$, $59 \leq q = p \leq 2297$, and $|G/Z| \leq 24$.*

Proof. Suppose that V and G satisfy the assumptions of the paragraph preceding the statement of the proposition. Then $|V|/|G| < 2\sqrt{q-1}$.

Suppose first that (r,a) is different from any of the pairs $(2,1)$, $(3,1)$, and $(2,2)$. Then $|G| < q \cdot r^{2a} \cdot |\mathrm{Sp}_{2a}(r)| < q \cdot r^{2a^2+3a}$. We wish to show that this is less than $q^{r^a-1} \leq |V|/(2\sqrt{q-1})$. By taking logarithms of both sides, it is sufficient to see the inequality $(2a^2+3a)\log r < (r^a-2)\log q$. But this is true by using the assumption that $q \geq p \geq 59$. This is a contradiction to the fact that $|V|/|G| < 2\sqrt{q-1}$.

If $(r,a) = (2,2)$ then a more careful but similar computation as in the previous paragraph yields a contradiction. For $(r,a) = (3,1)$ we do the same and get a contradiction whenever $q \geq 61$. Also, q cannot be 59 in this case since 3 does not divide 58.

So only $(r,a) = (2,1)$ can occur. In this case we must have $n = 2$, $|G/Z| \leq 24$, and thus q is in the range $59 \leq q = p \leq 2297$. □

2.5 Bounding the number of orbits

The purpose of this section is to describe as much as possible pairs (G,V) for which $n(G,V) < 2\sqrt{q-1}$.

Theorem 2.11. *Let V be a finite, faithful, coprime and irreducible FG-module. Suppose that the characteristic p of the underlying field F is at least 59. Put $q = |F|$ and $|V| = q^n$. Let the center of $\mathrm{GL}_n(q)$ be Z. Then $n(G,V) \geq 2\sqrt{q-1}$ unless possibly if one of the following cases holds.*

1. $(G, V) \in \mathcal{C}_q$;
2. $V = \mathrm{Ind}_H^G(W)$ *for some* 2*-dimensional* FH*-module* W *where* H *is as* G *in Proposition 2.9 or Proposition 2.10 satisfying one of the following.*
   a) $59 \leq q \leq 14389$, $q \equiv \pm 1 \pmod{10}$, *and* $2.A_5 \leq H/C_H(W) \leq Z \circ 2.A_5$;
   b) $59 \leq q = p \leq 2297$ *and* $|(H/C_H(W))/Z(H/C_H(W))| \leq 24$.

In order to prove Theorem 2.11 we need a bound on the orders of groups among the exceptions in the statement of the theorem. The following extends Lemma 2.7.

Lemma 2.12. *Let* (G, V) *be a pair among the exceptions in Theorem 2.11, satisfying* $n(G, V) < 2\sqrt{q-1}$. *Then* $|G| < |V|^{3/2}$.

Proof. If (G, V) is of type (1) then Lemma 2.7 gives the result. If (G, V) is of type (2/a) or (2/b) then it is easy to see that $|G| < |V|^{3/2}$ by using Proposition 2.5 and the fact that $p \geq 59$. □

We can now turn to the proof of Theorem 2.11. In this we follow the reduction argument found in [45, Section 6].

Let G be a counterexample to Theorem 2.11 with n minimal.

Suppose that V is an imprimitive FG-module which is induced from a primitive FH-module W for some proper subgroup H of G. If $n(H, W) \geq 2\sqrt{q-1}$ then $n(G, V) \geq 2\sqrt{q-1}$, by Lemma 2.3. So assume that $n(H, W) < 2\sqrt{q-1}$. By the minimality of n, the pair $(H/C_H(W), W)$ must be of type (1) or (2) of the statement of the theorem. But then (G, V) is also of type (1) or (2). A contradiction.

So we may assume that V is a primitive FG-module.

We first claim that we can assume that every irreducible FN-submodule of V is absolutely irreducible for any normal subgroup N of G. For this purpose let N be a normal subgroup of G. Then V is a homogeneous FN-module, so $V = V_1 \oplus \cdots \oplus V_m$, where the V_i's are isomorphic irreducible FN-modules. Let $K \simeq \mathrm{End}_{FN}(V_1)$. Assuming that the V_i's are not absolutely irreducible, K is a proper field extension of F, and $C_{GL(V)}(N) = \mathrm{End}_{FN}(V) \cap GL(V) \simeq \mathrm{GL}_r(K)$ for some r. Furthermore, $L = Z(C_{GL(V)}(N)) \simeq Z(\mathrm{GL}_r(K)) \simeq K^\times$. Now, by using L, we can extend V to a K-vector space of dimension $\ell := \dim_K V < n$. As $G \leq N_{GL(V)}(L)$, in this way we get an inclusion $G \leq \Gamma L(\ell, K)$. Now G contains the normal subgroup $H = G \cap \mathrm{GL}_\ell(K)$ of index at most n. Clearly V is a homogeneous and faithful KH-module. Let W be a simple KH-submodule of V. Then, by the minimality of n, we get $n(H, V) \geq n(H, W) \geq 2\sqrt{|K|-1}$ unless (H, W) is one of the examples listed in the statement of the theorem. If H is none of the possibilities listed in the statement of the theorem, then $n(G, V) \geq n(H, V)/n \geq 2\sqrt{q-1}$, a contradiction, since we are assuming $p \geq 59$. If (H, W) is of possibility (1) then so is (G, V) of possibility (1) unless $W < V$. If $W < V$ and W is not of dimension 1 over K then Lemma 2.7 shows that $n(H, V) \geq |V|/|H| \geq 2\sqrt{|K|-1}$, and so

$n(G,V) \geq n(H,V)/n \geq 2\sqrt{q-1}$, as before. If W is of dimension 1 over K then a more careful consideration is necessary to obtain the same conclusion. If H is of possibility (2) of the statement of the theorem, then H is of index 2 in G and so $|G| \leq 120(q^2-1)$. But then $n(G,V) > |V|/|G| > q^2/120 \geq 2\sqrt{q-1}$ since $q \geq 59$. This shows the claim.

Let N be a normal subgroup of G and let $V = V_1 \oplus \cdots \oplus V_r$ be a direct sum decomposition of V into isomorphic absolutely irreducible FN-modules. By choosing a suitable basis in $V_1, V_2, \ldots, V_r$, we can assume that $G \leq \mathrm{GL}_n(F)$ such that any element of N is of the form $A \otimes I_r$ for some $A \in N_{V_1} \leq \mathrm{GL}_{n/r}(F)$. By using [62, Lemma 4.4.3(ii)] we get

$$N_{\mathrm{GL}_n(F)}(N) = \{B \otimes C \mid B \in N_{\mathrm{GL}_{n/r}(F)}(N_{V_1}),\ C \in \mathrm{GL}_r(F)\}.$$

Let

$$G_1 = \{g_1 \in \mathrm{GL}_{n/r}(F) \mid \exists g \in G, g_2 \in \mathrm{GL}_r(F) \text{ such that } g = g_1 \otimes g_2\}.$$

We define $G_2 \leq \mathrm{GL}_r(F)$ in an analogous way. Then $G \leq G_1 \otimes G_2$. Here G_1 and G_2 are not homomorphic images of G, since $g = g_1 \otimes g_2 = \lambda g_1 \otimes \lambda^{-1} g_2$ for any $\lambda \in F^\times$, so the map $g = g_1 \otimes g_2 \mapsto g_1$ is not well-defined. However, they both have orders coprime to p. Since $G_1 \otimes G_2$ preserves a tensor product structure $V = W_1 \otimes W_2$, so does G.

We claim that G does not preserve a proper tensor product structure. For a proof suppose that G preserves a tensor product structure $V = W_1 \otimes W_2$ with $r_1 = \dim W_1 > 1$ and $r_2 = \dim W_2 > 1$. Without loss of generality assume that $r_1 \leq r_2$ and $n = r_1 r_2$. Then $G \leq G_1 \otimes G_2$ for some groups G_1 and G_2 acting on W_1 and W_2 respectively. Assume also that these groups have orders coprime to p. We also assume that G acts primitively and irreducibly on V and $Z \leq G$. Notice that the G_i's act irreducibly on the W_i's (for if $0 < U_1 < W_1$ would be a G_1-submodule then $U_1 \otimes W_2$ would be a $G_1 \otimes G_2$-submodule). Also, the G_i's act primitively on the V_i's. (For if G_1 would act imprimitively on W_1, say, then there would be a proper subspace U_1 in W_1 whose stabilizer has index $|W_1|/|U_1|$. But then $U_1 \otimes W_2$ would be a subspace of V whose stabilizer in $G_1 \otimes G_2$ has the same index. But then, by [105, Theorem 3, page 105], we see that $G_1 \otimes G_2$, and in particular G, acts imprimitively on V, a contradiction.) If $n(G_i, W_i) \geq 2\sqrt{q-1}$ for any of the i's, then we are done. (For if $n(G_1, W_1) \geq 2\sqrt{q-1}$, say, and $v_1, \ldots, v_f$ are representatives of f orbits of G_1 on W_1 with $f \geq 2\sqrt{q-1}$, then $v_1 \otimes w, \ldots, v_f \otimes w$ will be representatives of f orbits of G on V where w is a non-zero vector in W_2.) So by the minimality of n we know that both G_1 and G_2 are exceptions in the statement of the theorem. If G is solvable, then Proposition 2.4 gives a contradiction (since $n \geq 4$). So we may assume that G is non-solvable. Notice that $|G| \leq (|G_1| \cdot |G_2|)/(q-1)$.

Let $r_1 = 2$. Then $|G| < 2 \cdot q^{(3/2)r_2+1}$ by Lemma 2.12. But then if $r_2 \geq 5$ then $|V|/|G| > 2\sqrt{q-1}$, a contradiction. We get the same conclusion when $r_1 \geq 3$ and $r_2 \geq 5$ (apply Lemma 2.12). So we conclude that $2 \leq r_1 \leq r_2 \leq 4$. In fact, since G is non-solvable, this forces $r_1 = 2$ and G_1 of type (2/a).

Let $r_2 = 2$. To maximize $|G|$ we may assume that G_2 is of type (1) or (2/a). But then we again have $2\sqrt{q-1} < |V|/|G|$, a contradiction. So $r_2 = 3$ or 4. But then G_2 is of type (1). In both cases G_2 must be solvable. Let $r_2 = 4$. If G_2 is not a semilinear

group of order dividing $4(q^4-1)$, then Proposition 2.4 gives what we want. Otherwise $2\sqrt{q-1} \leq q^8/|G|$. So let $r_2 = 3$. Then $|G_2| \leq 3(q^3-1)$ (since G_2 is primitive) and so $2\sqrt{q-1} \leq q^6/|G|$.

We conclude that G does not preserve a proper tensor product structure.

From now on assume that N is a normal subgroup of G which is minimal with respect to being non-central. Then $N/Z(N)$ is a direct product of isomorphic simple groups.

If N is Abelian then it is central in G. A contradiction.

If $N/Z(N)$ is elementary Abelian of rank at least 2, then G is of symplectic type and Proposition 2.10 gives us a contradiction.

Now let $N/Z(N)$ be a direct product of $m \geq 2$ isomorphic non-Abelian simple groups. Then $N = L_1 \star L_2 \star \cdots \star L_m$ is a central product of isomorphic groups such that for every $1 \leq i \leq m$ we have $Z \leq L_i,\ L_i/Z$ is simple. Furthermore, conjugation by elements of G permutes the subgroups $L_1, L_2, \ldots, L_m$ in a transitive way. By choosing an irreducible FL_1-module $V_1 \leq V$, and a set of coset representatives $g_1 = 1, g_2, \ldots, g_m \in G$ of $G_1 = N_G(V_1)$ such that $L_i = g_i L_1 g_i^{-1}$, we get that $V_i := g_i V_1$ is an absolutely irreducible FL_i-module for each $1 \leq i \leq m$. Now, $V \simeq V_1 \otimes V_2 \otimes \cdots \otimes V_m$ and G permutes the factors of this tensor product. It follows that G is embedded into the central wreath product $G_1 \wr_c S_m$ and that G_1 is non-solvable. Now G_1 acts irreducibly on V_1 for otherwise there are proper G_1-submodules W_i of V_i for each i with $1 \leq i \leq m$, so that $W = W_1 \otimes \cdots \otimes W_m$ is a proper G-submodule of V. If $n(G_1, V_1) \geq 2\sqrt{q-1}$, then so is $n(G, V) \geq 2\sqrt{q-1}$. (For let $v_1, \ldots, v_r$ be members of $n(G_1, V_1) - 2$ non-trivial orbits of G_1 on V_1. Clearly $r > 2$ and these vectors are non-zero and pairwise not multiples of each other. Let v_{r+1} be a fixed non-zero vector not in an orbit of any of the vectors listed above. Then the vectors $w_i = v_i \otimes v_{r+1} \otimes \ldots \otimes v_{r+1}$ for $1 \leq i \leq r+1$ are all non-zero and are all in different G-orbits.) So G_1 is a group among the exceptions in Theorem 2.11. So we have $|G_1| \leq |V_1|^{3/2}$ by Lemma 2.12. Using this we can show that $|V|/|G| > 2\sqrt{q-1}$ provided that $\dim V_1 \geq 4$. So assume that $\dim V_1 = 2$ or 3. Since G_1 is non-solvable, we must then have $\dim V_1 = 2$ and $G_1 = Z \circ 2.A_5$. But then $|G| \leq (q-1)60^m p^{m-1}$ where the last factor follows from Proposition 2.5 and $n = 2^m$. However when $m = 2$ then by using just a factor of 2 in place of p^{m-1}, we get $2\sqrt{q-1} \leq |V|/|G|$. We get the same conclusion in case $m \geq 3$, by Proposition 2.5.

The remaining case is when $N/Z(N)$ is a non-Abelian finite simple group. But then the generalized Fitting subgroup of G is a central product of the center of G with a quasisimple group (by the above reductions) and Proposition 2.9 yields a contradiction.

This proves Theorem 2.11.

2.6 Bounding the number of classes of a linear group

In order to prove Theorem 2.1 we now also have to take $k(G)$ into account.

Theorem 2.13. *Let V be an irreducible and faithful FG-module for some finite group G and finite field F of characteristic p at least 59. Suppose that p does not divide $|G|$. Then we have at least one of the following.*

1. $n(G,V) \geq 2\sqrt{p-1}$.
2. $k(G) \geq 2\sqrt{p-1}$.
3. $\sqrt{p-1}$ *is an integer,* $|V| = |F| = p$ *and* $|G| = \sqrt{p-1}$.
4. *Case (2/a) of Theorem 2.11 holds with* $p = 59$ *and* $1 < t \leq 14$, *or* $p = 61$ *and* $t = 1$, *or* $61 \leq p \leq 119$ *and* $2 \leq t \leq 4$.
5. *Case (2/b) of Theorem 2.11 holds with* $t \leq 4$.

Proof. Let V be an irreducible and faithful FG-module as in the statement of the theorem. Suppose that $n(G,V) < 2\sqrt{p-1}$. Suppose also that case (3) is not satisfied. More in general, suppose that $|V| = |F| = p$ is not satisfied.

We are then in one of the two exceptional cases of Theorem 2.11. First suppose that $(G,V) \in \mathcal{C}_q$. Then case (1) or case (2) of Lemma 2.8 holds. In case (1) we may apply Lemma 2.6. So suppose that case (2) of Lemma 2.8 holds.

Suppose that G/B contains A_n. Then

$$k(G) \geq k(G/B) \geq k(S_n)/2 \geq 385/2 > 2\sqrt{p-1},$$

for $n \geq 18$ and $p < 8192$. So we must have $n = 15$, 16, or 17.

Since $k(G) \geq k(G/B) \geq k(A_{15}) = 94$, we may assume that $94 < 2\sqrt{p-1}$, that is, $2210 < p$. We may assume that $p^{n-1} < 4(n!)^2$ (otherwise we are in case (1) of Lemma 2.8). By the fact that $2210 < p$, we get $2210^{n-1} < 4(n!)^2$. But this is a contradiction for $n = 15$, 16, or 17.

We are now in case (2) of Theorem 2.11.

First we consider case (2/a) of Theorem 2.11.

Let us first assume that V is a primitive FG-module. Let C be the center of G. Then G contains at least $(|C|/2) \cdot k(A_5) = (5/2)|C|$ conjugacy classes. Thus we may assume that $|C| < (4/5)\sqrt{p-1}$. But we also have $|V|/(2\sqrt{p-1}|G/C|) < |C|$. From this we have $|V| < (8/5)(p-1) \cdot 60$, that is $q^2 < 96(p-1)$. Thus we certainly have $p \leq 96$ but also $q = p$. Thus we are left with the cases $q = p = 59$, 71, 79, and 89 (note that we are excluding 61 here).

Let $q = 59$. Then $|C| \leq 6$ by the previous paragraph. But since $|C|$ must divide $q - 1 = 58$ and is even, we have $|C| = 2$. So G has at least (if not exactly) 29 non-trivial orbits on V, which is larger than $2\sqrt{58}$.

Let $q = 71$. Then $|C| \leq 6$. But since $|C|$ must divide $q - 1 = 70$ and is even, we have $|C| = 2$. So G has at least 42 non-trivial orbits on V, which is larger than $2\sqrt{70}$.

Let $q = 79$. Then $|C| \leq 7$. But since $|C|$ must divide $q - 1 = 78$, we have $|C| \leq 6$. So G has at least 18 non-trivial orbits on V, which is larger than $2\sqrt{78}$.

Let $q = 89$. Then $|C| \leq 7$. But since $|C|$ must divide $q - 1 = 88$, we have $|C| \leq 4$. So G has at least 33 non-trivial orbits on V, which is larger than $2\sqrt{88}$.

Now assume that V is an imprimitive FG-module. Let T, t, n, B, V_1, H_1 and k be as above. So $n \geq 4$ and $t \geq 2$.

Suppose that $p > 1000$. Then the number of orbits of H_1 on V_1 is at least 3 (since $H_1/C_{H_1}(V_1)$ cannot be a transitive linear group by Hering's theorem (see [55, Chapter XII])). But then $n(G, V) \geq \binom{t+2}{2}$ by Lemma 2.3. So we may assume that $2\sqrt{p-1} > \binom{t+2}{2}$, which forces $2p^{1/4} > t$. From this we get $|G/B| < 2^t p^{t/4}$. Since $t = n/2$, we have $|G/B| < 2^{n/2} p^{n/8} < p^{0.176n}$ (for $p > 1000$). There exists a central subgroup $A = Z(B)$ in B of index at most $60^{n/2}$. So

$$k(G) \geq k(B)/|G : B| \geq |A|/|G : B| > |A|/p^{0.176n}.$$

We have $|G| > |V|/(2\sqrt{p-1})$ from which

$$|A| \geq |G|/(60^{n/2} p^{0.176n}) > |V|/(60^{n/2} \cdot p^{0.176n} \cdot 2\sqrt{p-1}).$$

This gives $k(G) \geq |V|/(60^{n/2} \cdot p^{0.352n} \cdot 2\sqrt{p-1})$. But this is larger than $2\sqrt{p-1}$ for $n \geq 4$.

Now let $121 < p < 1000$. Then it is easy to see that $n(H_1, V_1) \geq 4$. So we have $n(G, V) \geq \binom{t+3}{3}$ by Lemma 2.3. So we may assume that $2\sqrt{p-1} > \binom{t+3}{3} > t^3/6$. From this $12^{1/3} p^{1/6} > t$. Since $p < 1000$, we get $t \leq 7$. In fact by looking more closely at the bound using the binomial coefficient, we get $t \leq 5$. We claim that $H_1/C_{H_1}(V_1)$ has center of order at most $(q-1)/4$. Otherwise $k(H_1) \geq ((q-1)/4) \cdot k(A_5) > q - 1$. But then

$$k(G) \geq k(H_1)/5 > (q-1)/5 > 2\sqrt{q-1}$$

since $q > 121$. But then going back to the place where we calculated orbits, we see that $n(H_1, V_1) \geq 10$. So $n(G, V) \geq \binom{t+9}{9} \geq \binom{12}{9} = 220 > 64 > 2\sqrt{p-1}$ (for $t \geq 3$ and $p < 1000$), by Lemma 2.3. So $t = 2$. We claim that $H_1/C_{H_1}(V_1)$ has center of order at most $(q-1)/8$. Otherwise $k(G) \geq k(H_1)/2 \geq ((q-1)/8 \cdot k(A_5))/2 \geq 2\sqrt{p-1}$. But then going back to the place where we calculated orbits, we see that $n(H_1, V_1) \geq 18$. So $n(G, V) \geq \binom{19}{2} = 171 > 64 > 2\sqrt{p-1}$ (for $p < 1000$), by Lemma 2.3.

So the only remaining cases are: $t \geq 2$, and $p = 59$, 61, 71, 79, 89, 91, 101, 109, or 119. If $p = 59$ then it can happen that $n(H_1, V_1) = 2$, so in this case we can only say that $t \leq 14$. In all other cases $n(H_1, V_1) \geq 3$, so $t \leq 4$.

Finally we consider (2/b) of Theorem 2.11.

Let $H_1/C_{H_1}(V_1) \leq \mathrm{GL}_2(p)$ be as above. This group is solvable, primitive and its center has index at most 24. We may assume that $t \geq 5$. But then, by Lemma 2.3, $n(G, V) \geq \binom{k+4}{5}$. Thus we can assume that $\binom{k+4}{5} \leq n(G, V) < 2\sqrt{p-1}$. Since we may

also assume that $k \geq 3$ by order considerations, from this previous inequality we get $113 \leq p$. But then, by Proposition 2.4, we have $k \geq p/24$. However, since $113 \leq p$, we also have $k \geq \max\{5, p/24\}$. Just by using the bound $k \geq 5$ we can conclude that $p \geq 3970$. This is a contradiction. □

2.7 Bounding $n(G, V)$ and $k(G)$

We prove Theorems 2.1 (and so 1.3) by going through the cases of Theorem 2.13.

Since both $k(G)$ and $n(G, V)$ are at least 2, there is nothing to do in cases (1) and (2). Groups in cases (3) and (5) are solvable, so the argument of [48] applies. Let us assume then that case (4) of Theorem 2.13 is satisfied.

Let t, V_1, H_1, and k be as above. Let C denote the center of $H_1/C_{H_1}(V_1)$.

Suppose first that $p = 59$ and t is an integer with $2 \leq t \leq 14$. In this case we need $k(G) + n(G, V) - 1 \geq 16$. If C has size 58 then $k(H) > 29 \cdot 5 = 145$. So $k(G) > 145/t$. But $n(G, V) \geq t+1$, so $k(G)+n(G, V)-1 > 145/t+t > 16$. (This also works for $t = 1$.) So we know that H_1 has at least 3 orbits on V_1 by Hering's theorem (see [55, Chapter XII]). But then $n(G, V) \geq \binom{t+2}{2}$ by Lemma 2.3. This is at least 16 unless $t \leq 4$.

Let $t = 4$. Then $n(G, V) \geq 15$ by Lemma 2.3. The result follows from $k(G) \geq 2$.

Let $t = 3$. Then $n(G, V) \geq 10$ by Lemma 2.3. So we would need $k(G) \geq 7$. Then $k(G) \geq (k(A_5)|C|)/2t = (5/2)|C|/3$. If $|C| \geq 9$ then we are finished. Otherwise $n(H_1, V_1) \geq 9$. So $n(G, V) \geq \binom{11}{3} > 22$ by Lemma 2.3.

Let $t = 2$. Then $n(G, V) \geq 6$ by Lemma 2.3. So we would need $k(G) \geq 11$. Then $k(G) \geq (k(A_5)|C|)/2t = (5/2)|C|/2$. If $|C| \geq 9$ then we are finished. Otherwise $n(H_1, V_1) \geq 9$. So $n(G, V)$ is at least $\binom{10}{2} = 45 > 11$ by Lemma 2.3.

Let $q = 61$ and $t = 1$. Then $|C| \leq 6$. So G has at least 11 non-trivial orbits on V. So $n(G, V) + k(G) - 1 \geq 11 + k(G) \geq 16 > 2\sqrt{60}$, a contradiction.

Suppose that $61 \leq p \leq 119$ and $2 \leq t \leq 4$. Then $k \geq 3$ by Hering's theorem (see [55, Chapter XII]).

Let $t = 4$. Then $n(G, V) \geq 15$ by Lemma 2.3. So we would need $k(G) \geq 8$ (since $2\sqrt{118}$ is a bit smaller than 22). Then $k(G) \geq (k(A_5)|C|)/2t = (5/2)|C|/4$. If $|C| \geq 13$ then we are finished. Otherwise $n(H_1, V_1) \geq 6$. So $n(G, V) \geq \binom{9}{4} > 22$ by Lemma 2.3.

Let $t = 3$. Then $n(G, V) \geq 10$ by Lemma 2.3. So we would need $k(G) \geq 13$. Then $k(G) \geq (k(A_5)|C|)/2t = (5/2)|C|/3$. If $|C| \geq 16$ then we are finished. Otherwise $n(H_1, V_1) \geq 5$. So $n(G, V)$ is at least $\binom{7}{3} = 35 > 22$ by Lemma 2.3.

Let $t = 2$. Then $n(G, V) \geq 6$ by Lemma 2.3. So we would need $k(G) \geq 17$. Then $k(G) \geq (k(A_5)|C|)/2t = (5/2)|C|/2$. If $|C| \geq 14$ then we are finished. Otherwise $n(H_1, V_1) \geq 6$. So $n(G, V)$ is at least $\binom{7}{2} = 21$ by Lemma 2.3. But $k(G) \geq 2$.

3 Conjugacy classes in permutation groups

In many situations it is useful to have upper bounds for the number of conjugacy classes of a permutation group. For example, such bounds are needed in the proof of the $k(GV)$ theorem and they are applied to the non-coprime $k(GV)$ problem (which is to bound $k(GV)$ for the semidirect product GV where V is a completely reducible faithful G-module).

Let G be a permutation group of degree n. Kovács and Robinson [65] proved that $k(G) \leq 5^{n-1}$ and reduced the proposed bound of $k(G) \leq 2^{n-1}$ to the case when G is an almost simple group. This latter bound was later proved by Liebeck and Pyber [72] for arbitrary finite groups G. Kovács and Robinson [65] also proved that $k(G) \leq 3^{(n-1)/2}$ for G a solvable permutation group of degree $n \geq 3$. Later Riese and Schmid [97] proved the same bound for $3'$, $5'$ and $7'$-groups, and in [81] Maróti obtained the bound $k(G) \leq 3^{(n-1)/2}$ for an arbitrary finite permutation group G of degree $n \geq 3$. In this chapter we prove the even stronger Theorem 1.5.

3.1 Preliminaries

The following lemma collects basic information on the number of conjugacy classes in a subgroup and in a normal subgroup of a finite group.

Lemma 3.1. *Let H be a subgroup and N be a normal subgroup of a finite group G. Then*

1. $k(H)/|G:H| \leq k(G) \leq k(H) \cdot |G:H|$;
2. $k(H) \leq \sqrt{|G|k(G)}$; *and*
3. $k(G) \leq k(N) \cdot k(G/N)$.

Proof. Statements (1) and (3) can be found in [26] (see also [84]). Statement (2) follows from (1). □

In special cases we will need a straightforward consequence of the Clifford-Gallagher formula [100, Page 18]. The second statement of the following lemma follows from [100, Proposition 8.5d].

Lemma 3.2. *Let* $\mathrm{Irr}(N)$ *denote the set of complex irreducible characters of a normal subgroup N of a finite group G. Then $S = G/N$ acts on* $\mathrm{Irr}(N)$ *in a natural way and let*

$I_S(\theta)$ denote the stabilizer of a character θ in $\mathrm{Irr}(N)$. Then we have

$$k(G) \leq \sum_{\theta \in \mathrm{Irr}(N)} k(I_S(\theta))/|S : I_S(\theta)|.$$

Moreover if N is a full direct power of a finite group T and S permutes the factors of N transitively and faithfully, then $k(G) \leq k(T \wr S)$.

For a non-negative integer n let the number of partitions of n be denoted by $p(n)$. This is the number of conjugacy classes of the symmetric group S_n. In 1918 Hardy and Ramanujan [46] and independently but later Uspensky [109] proved the following asymptotic formula.

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}.$$

In 1937 Rademacher [96] gave a convergent series expression for $p(n)$, however here we will only need the following lower and upper bounds.

Lemma 3.3. *Let $n \geq 1$ be an integer. Then $e^{2.5\sqrt{n}}/13n < p(n) < e^{\pi\sqrt{2n/3}}$.*

Proof. For the upper bound see [19] and for the lower bound see [81]. □

3.2 Conjugacy classes in primitive permutation groups

A transitive permutation group G is called primitive if the stabilizer of any point is a maximal subgroup in G. This is equivalent to saying that the only blocks of imprimitivity for G are the singleton sets and the whole set on which G acts. The symmetric and alternating groups, S_n and A_n, are examples of primitive permutation groups. In this section we will extend Corollary 2.15 (i) of [72] and [82, Theorem 1.3 (i)] to prove Theorem 3.4. This result heavily depends on [80, Theorem 1.1] and also on [27].

Theorem 3.4. *Let G be a primitive permutation group of degree n different from A_n and S_n. Then we have $k(H) \leq p(n)$ for every subgroup H of G.*

Proof. Let G be a primitive permutation group of degree n. If $H \leq G$ are subgroups of $S_m \wr S_r$ in its product action on $n = \binom{m}{k}^r$ points where $m \geq 5$ and S_m acts on k-subsets for some k with $1 \leq k < n$, then $k(H) \leq 2^{mr-1}$ by [72, Theorem 2]. But for $(k, r) \neq (1, 1)$ we have

$$2^{mr-1} < \frac{e^{2.5\sqrt{n}}}{13n} < p(n),$$

where the second inequality follows from Lemma 3.3. Thus we may exclude these cases from the discussion.

By [80, Theorem 1.1], we then know that $|G| < n^{1+[\log_2(n)]}$ or G is one of the Mathieu groups in their 4-transitive action.

Again by Lemma 3.3, we see that $|G| < n^{1+[\log_2(n)]} < p(n)$ for $n \geq 1500$. Furthermore, by using the exact values of $p(n)$ available in [27], $|G| < p(n)$ is true even for $n \geq 1133$.

If $120 \leq n < 1133$ then $p(n) < |G| < n^{1+[\log_2(n)]}$ holds only if $n = 1024$ and $G = \mathrm{AGL}_{10}(2)$, $n = 512$ and $G = \mathrm{AGL}_9(2)$, $n = 256$ and $G = \mathrm{AGL}_8(2)$, or $n = 511$, 255, 190, 171, 153, 144, 136, 128, 127, 121, or 120 (this was also obtained by [27]).

If G is any of these exceptional cases (with $n \geq 120$) and is not a subgroup of $S_m \wr S_r$ in its product action discussed above, then $k(G)|G| < p(n)^2$, which forces $k(H) < p(n)$ for any subgroup H of G (by (2) of Lemma 3.1). Furthermore if $n \leq 119$ then we again have $k(G)|G| < p(n)^2$, unless $n = 64$ and $G = \mathrm{AGL}_6(2)$, or $n \leq 32$ and G is almost simple or of affine type. Both these statements were derived by [27].

For almost simple primitive groups G of degrees n at most 32 (including the 4-transitive Mathieu groups but excluding A_n and S_n) we can compute the subgroup lattice of G by [27] and so the claim can be checked for all subgroups H of G. Thus we may assume that G is an affine primitive permutation group of degree 64 or at most 32.

We must show that if H is a subgroup of $\mathrm{AGL}_m(p)$ with $n = p^m \leq 64$, then $k(H) \leq p(n)$. If $m = 1$ then it is easy to see that $k(H) \leq p = n \leq p(n)$. If $m = 2$ and $p = 5$ or 7, or if $p^m = 27$, then $|\mathrm{AGL}_2(p)|k(\mathrm{AGL}_2(p)) < p(n)^2$ and we may apply (2) of Lemma 3.1. Thus we may assume that $p = 2$ or 3. The full subgroup lattice of $\mathrm{AGL}_m(p)$ can be computed by [27] for all remaining cases except $(m, p) = (5, 2)$ and $(m, p) = (6, 2)$, and thus the validity of the inequality $k(H) \leq p(n)$ can be checked directly.

Let $m = 5$ and $p = 2$. Any subgroup of $\mathrm{GL}_5(2)$ has less than 260 conjugacy classes (this can be obtained by [27] by viewing $\mathrm{GL}_5(2)$ as a permutation group on 31 points), and so (3) of Lemma 3.1 gives $k(H) < 260 \cdot 32 < p(32)$ for any subgroup H of $\mathrm{AGL}_5(2)$.

Let $m = 6$ and $p = 2$. Put $N = O_2(H)$. The factor group H/N can be viewed as a completely reducible subgroup on a vector space of size 64 (see [72, Page 554]). We claim that $k(H/N) \leq 63$. For this observe that for irreducible linear subgroups T of $GL(V)$ we have $k(T) < |V|$ whenever V is a vector space of size a power of 2 at most 64. (This can be checked by [27] by going through stabilizers of all affine primitive permutation groups of degrees a power of 2 at most 64.) Then, by using part (3) of Lemma 3.1, induction, and noting that a normal subgroup of a completely reducible linear group also acts completely reducibly on the same vector space (Clifford's theorem), we obtain the claim.

Let S be a Sylow 2-subgroup of $\mathrm{AGL}_6(2)$ containing N. Suppose that $|S : N| \geq 64$. Then (3) of Lemma 3.1 gives $k(H) \leq |N| \cdot k(H/N) \leq 2^{15} \cdot 63 < 2^{21} < p(64)$. Now suppose that $|S : N| \leq 16$. Then $k(N) \leq |S : N| \cdot k(S) \leq 16 \cdot 1430$, by (1) of Lemma 3.1, and so $k(H) \leq k(N) \cdot k(H/N) \leq 16 \cdot 1430 \cdot 63 < p(64)$. So the only case missing is when $|S : N| = 32$. We would like to bound $k(N)$ in this case. Let S_1 be a maximal subgroup of S containing N. By [27] we know that $k(S_1) \leq 1723$ or $k(S_1) = 1768$. In the first case we have $k(N) \leq 16 \cdot 1723$, and so $k(H) \leq 16 \cdot 1723 \cdot 63 < p(64)$. So suppose that the second case holds. Then let S_2 be a maximal subgroup in S_1

containing N. By [27] again, we know that $k(S_2) \leq 2240$, and so $k(N) \leq 8 \cdot 2240$. This gives $k(H) \leq 8 \cdot 2240 \cdot 63 < p(64)$. □

A straightforward consequence of Theorem 3.4 is the following.

Corollary 3.5. *If H is a subnormal subgroup of a primitive permutation group of degree n, then $k(H) \leq p(n)$.*

Proof. If $H = S_n$ then this is clear. If $H = A_n$, then this follows from [82, Lemma 2.3]. Otherwise apply Theorem 3.4. □

3.3 Conjugacy classes in transitive permutation groups

In this section we will give an upper bound in terms of the partition function for $k(G)$ when G is a transitive permutation group. This result depends on Theorem 3.4 and is used in the proof of Theorem 1.3.

Theorem 3.6. *Let G be a transitive permutation group of degree n with point stabilizer H. Consider the chain*

$$H = H_0 < H_1 < \ldots < H_t = G$$

with H_i maximal in H_{i+1} for $i = 0, \ldots, t-1$ and call $a_i := |H_i : H_{i-1}|$ for $i = 1, \ldots, t$, so that $a_1 \cdots a_t = |G : H| = n$. Then

$$k(G) \leq \left(p(a_1)^{1/a_1} p(a_2)^{1/a_1 a_2} \cdots p(a_{t-1})^{1/a_1 \cdots a_{t-1}} p(a_t)^{1/a_1 \cdots a_t}\right)^n.$$

Proof. Let G be a minimal counterexample to the statement of the theorem with a fixed chain of subgroups. By Corollary 3.5, we may assume that $t \geq 2$. We now construct a subnormal filtration as in [99]. Let B_0 be the core of H_1 in G, so that G/B_0 is a transitive permutation group of degree n/a_1. Let N be the core of $H = H_0$ in H_1, so that H_1/N is a primitive permutation group of degree a_1. Let $\{x_i\}_{1 \leq i \leq n/a_1}$ be a set of representatives for the right cosets of H_1 in G, with $x_1 = 1$, and define inductively $B_i := B_{i-1} \cap N^{x_i}$ for $i \geq 1$. Then $B_i = B_{i-1} \cap B_1^{x_i}$ and since N is normal in H_1 and H is core-free,

$$B_{n/a_1} \subseteq \bigcap_{i=1}^{n/a_1} N^{x_i} = \bigcap_{g \in G} N^g \subseteq \bigcap_{g \in G} H^g = \{1\}.$$

We obtain a subnormal filtration (grading) $B = B_0 \rhd B_1 \rhd \cdots \rhd B_{n/a_1} = \{1\}$. Observe that $B_i \trianglelefteq B_0$ for all $0 \leq i \leq n/a_1$, this is easily seen by induction on i: since $B_0 \trianglelefteq G$ we have $B_1^{x_i} \trianglelefteq B_0^{x_i} = B_0$ and hence $B_i = B_{i-1} \cap B_1^{x_i} \trianglelefteq B_0$. Let $L := B_0 \cap N$. We have

$$B_i/B_{i+1} = B_i/B_i \cap B_1^{x_{i+1}} = B_i/B_i \cap L^{x_{i+1}} \cong B_i L^{x_{i+1}}/L^{x_{i+1}} \trianglelefteq B_0/L^{x_{i+1}} \cong B_0/L.$$

Since $B_0/L \cong B_0 N/N \trianglelefteq H_1/N$, each B_i/B_{i+1} is isomorphic to a subnormal subgroup of the primitive group H_1/N of degree a_1. By Corollary 3.5, $k(B_i/B_{i+1}) \leq p(a_1)$ for

all i. Now consider the chain $H_1/B < H_2/B < \ldots < H_{t-1}/B < H_t/B = G/B$. Each subgroup of the chain is maximal in the following one hence by minimality of G the theorem holds for G/B relative to this chain and hence

$$\begin{aligned} k(G) \leq k(B)k(G/B) &\leq \Big(\prod_{i=0}^{n/a_1-1} k(B_i/B_{i+1}) \Big) \cdot k(G/B) \\ &\leq p(a_1)^{n/a_1} \cdot (p(a_2)^{(n/a_1)/a_2} \cdots p(a_t)^{(n/a_1)/(a_2 \cdots a_t)}) \\ &= p(a_1)^{n/a_1} p(a_2)^{n/a_1 a_2} \cdots p(a_{t-1})^{n/a_1 \cdots a_{t-1}} p(a_t). \end{aligned}$$

The proof is complete. □

3.4 Arbitrary permutation groups

In this section we will prove Theorem 1.5. The first lemma enables us to deal with cases when n is relatively small.

Lemma 3.7. *If G is a permutation group of degree n all of whose orbits have lengths at most 23 then $k(G) \leq 5^{n/4}$.*

Proof. By induction on n, as in Lemma 3.1 of [82], we may assume that G is transitive. For transitive groups the claim can be checked by [27]. □

By [53] all transitive permutation groups of degree at most 30 are known therefore the 23 in Lemma 3.7 could perhaps be replaced by 30 (or even 31) but it is not clear to what extent this possible improvement could be of help.

Now we proceed to the proof of Theorem 1.3. Many of the computations below have been performed by [27], but we will not point this out in all cases.

Let G be as in the statement of the theorem. It acts faithfully on a set Ω of size n.

We proceed by induction on n. By Lemma 3.7 we can assume that $n \geq 24$. Suppose G is intransitive and let O be a nontrivial orbit of G of size $1 < r < n$. Let N be the kernel of the action of G on O. Then N acts faithfully on $n - r$ points and G/N acts faithfully on r points hence if $r, n - r \geq 4$ then

$$k(G) \leq k(N) \cdot k(G/N) \leq 5^{(n-r-1)/3} \cdot 5^{(r-1)/3} < 5^{(n-1)/3}.$$

If $r \leq 3$ then $k(G/N) \leq r$, and if $n - r \leq 3$ then $k(N) \leq n - r$, from which the result follows likewise. Hence we may assume that G is transitive.

Let H be the stabilizer of $\alpha \in \Omega$ in G. If H is maximal in G then G is a primitive permutation group and thus by Theorem 3.6 and Lemma 3.3 we have $k(G) \leq p(n) \leq e^{\pi\sqrt{2n/3}}$ and this is at most $5^{(n-1)/3}$ for $n \geq 25$.

Assume that H is not maximal in G and let K be such that $H < K < G$. Let $a := |K : H|$ and $b := |G : K|$. Notice that the K-orbit Δ containing α is a block of imprimitivity for the action of G. Let B be the kernel of the action of G on the block system Σ associated to Δ, in other words, B is the normal core of K in G. G/B is a transitive permutation group of degree b. By taking subsequent kernels on the blocks (i.e. arguing as in the proof of Theorem 3.6) we find a subnormal sequence $B_0 = B \trianglerighteq B_1 \trianglerighteq \ldots \trianglerighteq B_b = \{1\}$ such that each factor group B_i/B_{i+1} can be considered as a permutation group of degree a.

If a and b are both at least 4 then we may apply induction to find

$$k(G) \leq k(B) \cdot k(G/B) \leq (5^{(a-1)/3})^b \cdot 5^{(b-1)/3} = 5^{(n-1)/3}.$$

So we may assume that whenever $H < L < G$ either $|G : L| \leq 3$ or $|L : H| \leq 3$.

If both a and b are at most 3 then $n \leq 9$ and the result follows from Lemma 3.7. Assume that $4 \leq a \leq 23$ and $b \leq 3$. Then $k(G/B) \leq 3$ hence since the orbits of B all have size at most 23 by Lemma 3.7 we have $k(G) \leq k(B)k(G/B) \leq 5^{n/4} \cdot 3$ which is at most $5^{(n-1)/3}$ since $n \geq 24$.

We are in one of the following cases.

1. H is maximal in K and $b = |G : K| \in \{2, 3\}$, $a \geq 24$ (consider the block system associated to K).
2. K is maximal in G and $a = |K : H| \in \{2, 3\}$.
3. There exists a subgroup $L < G$ such that $H < K < L < G$ with K maximal in L, $a = |K : H| \in \{2, 3\}$, $c = |G : L| \in \{2, 3\}$, and $q = |L : K| \geq 24/a$ (consider the block system associated to L).

We consider the cases separately. In the following "filtration argument" refers to the argument used in the proof of Theorem 3.6. If $B \leq A$ are subgroups of G, by "filtration associated to A and B" we mean the filtration of the kernel of the action of A on the system of blocks associated to B obtained as in the proof of Theorem 3.6.

Case 1. By Theorem 3.6, since $p(b) \leq b$ we have $k(G) \leq p(a)^b b$. Thus it is sufficient to show that $p(a)^b b \leq 5^{(ab-1)/3}$, i.e. $p(a) \leq ((5^{(ab-1)/3})/b)^{1/b}$. For this it is sufficient to show that $p(a) \leq ((5^{(2a-1)/3})/3)^{1/3}$ for $a \geq 24$. If $a \geq 55$ this follows from the bound $p(a) \leq e^{\pi\sqrt{2n/3}}$ (Lemma 3.3), and if $24 \leq a \leq 54$ it follows by inspection.

Case 2. In this case G/B is a primitive group of degree b. Applying the filtration argument used in the proof of Theorem 3.6, since $p(a) \leq a$ we find $k(G) \leq a^b k(G/B)$ and it is enough to prove that $a^b k(G/B) \leq 5^{(ab-1)/3}$, i.e. (*) $k(G/B) \leq ((5^{(ab-1)/3})/a^b) = (5^{(a-1/b)/3}/a)^b$. Recall that $ab = n \geq 24$. If $a = 3$ then $b \geq 8$, now $p(b) \leq (5^{(3-1/8)/3}/3)^b$ follows from the bound $p(b) \leq e^{\pi\sqrt{2b/3}}$ (Lemma 3.3) if $b \geq 34$ and by inspection if $8 \leq b \leq 33$. Suppose now $a = 2$, so that $b \geq 12$. If $b = 12$ let S be a block stabilizer, then $|G : S| = b$ and S is a permutation group on 24 points having at least 2 orbits hence by Lemma 3.7 we have $k(G) \leq 12 \cdot k(S) \leq 12 \cdot 5^6$ and this is less than $5^{23/3}$.

Let $b \in \{13, 14, 15\}$. Then using the fact that any primitive group of degree b different from S_b has at most $k(A_b)$ conjugacy classes we see that (*) holds unless $G/B \cong S_b$. If B is not elementary Abelian of rank b then the filtration argument implies $k(G) \leq a^{b-1}k(G/B) \leq 5^{(ab-1)/3}$. So assume that $B \cong C_2^b$ and $G/B \cong S_b$. Then by the Clifford-Gallagher formula (Lemma 3.2) $k(G) \leq k(C_2 \wr S_b)$ which is at most $5^{(n-1)/3}$ by [27]. If $16 \leq b \leq 55$ then (*) holds by inspection using $k(G/B) \leq p(b)$, and if $b \geq 56$ it follows from the bound $p(b) \leq e^{\pi\sqrt{2b/3}}$ (Lemma 3.3).

Case 3. By Theorem 3.6, since $p(a) \leq a$ and $p(c) \leq c$ we have $k(G) \leq a^b p(q)^c c$ where $b = qc$. We want to prove that $k(G) \leq 5^{(n-1)/3}$ where $n = ab = aqc$. If $a = 3$ then it is sufficient to prove that $3^b p(q)^c c \leq 5^{(aqc-1)/3}$ for $q \geq 8$. Raising both sides to the power $1/c$ and rearranging, using the fact that $c^{1/c} \leq 1.5$ we see that it is sufficient to prove that $p(q) \leq \frac{1}{1.5}(5^{\frac{1}{3}(3-1/16)}/3)^q$ for $q \geq 8$. If $q \geq 31$ this follows from the bound $p(q) \leq e^{\pi\sqrt{2q/3}}$ (Lemma 3.3), and the case $8 \leq q \leq 30$ is checked by inspection.

Now assume that $a = 2$ and $q \geq 16$. We prove that (**) $2^{cq} \cdot p(q)^c \cdot c \leq 5^{(2cq-1)/3}$. Raising both sides of (**) to the power $1/c$ and rearranging we see that it is enough to prove that $p(q) \leq \frac{1}{1.5}(5^{\frac{1}{3}(2-1/32)}/2)^q$, and for this it is enough to prove that $p(q) \leq \frac{1}{1.5}(1.43)^q$. If $q \geq 60$ this follows from the bound $p(q) \leq e^{\pi\sqrt{2q/3}}$ (Lemma 3.3), and if $16 \leq q \leq 59$ inequality (**) can be checked by inspection.

Now assume that $a = 2$ and either $13 \leq q \leq 15$ or $(q, c) = (12, 3)$. Every nontrivial subnormal subgroup of any primitive group of degree q is a primitive group of degree q, a primitive group of degree q which is not the full symmetric group S_q has at most $k(A_q)$ conjugacy classes, and we have $k(A_{12}) = 43$, $k(A_{13}) = 55$, $k(A_{14}) = 72$, $k(A_{15}) = 94$. Moreover, the ratio $5^{(n-1)/3}/(2^{cq} \cdot p(q)^c \cdot c)$ is less than 2. Thus we may assume that the kernel of the action of G on the system of blocks associated to the primitive group K/H_K is a direct product $C_2^{cq} = C_2^b$, indeed if this is not the case then using the filtration argument we see that $k(G) \leq 2^{cq-1} \cdot p(q)^c \cdot c \leq 5^{(n-1)/3}$. Consider the filtration $\mathcal{F}_1$ associated to L and K. The two factors of this filtration are isomorphic to subnormal subgroups of the primitive group L/K_L of degree q. Consider the filtration $\mathcal{F}_2$ associated to L and H. By the Clifford-Gallagher formula (Lemma 3.2) a fixed factor of $\mathcal{F}_2$ has at most $k(S_2 \wr A)$ conjugacy classes, where A is a permutation group of degree q isomorphic to a factor of $\mathcal{F}_1$. If no factor of $\mathcal{F}_1$ is isomorphic to S_q then it is enough to show that $c \cdot k(A_q)^c \cdot 2^{cq} \leq 5^{(n-1)/3}$ which is true, and if there is a factor of $\mathcal{F}_1$ isomorphic to S_q then since $k(S_2 \wr S_{13}) = 1770$, $k(S_2 \wr S_{14}) = 2665$ and $k(S_2 \wr S_{15}) = 3956$ by the Clifford-Gallagher formula (Lemma 3.2) it is enough to show that $c \cdot k(S_2 \wr S_q) \cdot 2^{q(c-1)} \cdot p(q)^{c-1} \leq 5^{(n-1)/3}$ which is true.

Now assume that $(a, q, c) = (2, 12, 2)$. K is the stabilizer of a block of size 2 (there are 24 such blocks). It acts on the 24 points of a block system consisting of 12 blocks of size 2 intransitively, hence if N denotes the kernel of this action we deduce $k(K/N) \leq 5^{24/4} = 5^6$. Now look at the (faithful) action of N on the remaining 24 points. If this action is intransitive then $k(N) \leq 5^{24/4}$ by Lemma 3.7. If it is transitive then there is an induced transitive action of N on the second block system of twelve blocks of size

2. Since any transitive group of degree 12 has at most $p(12) = 77$ conjugacy classes (by [27]), by Theorem 3.6 we deduce $k(N) \leq 2^{12} \cdot 77$ and even $k(N) \leq 2^{11} \cdot 77$, in which case $k(G) \leq |G : K| \cdot k(K/N) \cdot k(N) \leq 24 \cdot 5^6 \cdot 2^{11} \cdot 77 \leq 5^{47/3}$, unless the kernel of the action of N on the 12 blocks of size 2 is a full direct product C_2^{12}. Suppose this is the case. Let R be the kernel of the transitive action of N on the twelve blocks of size 2 of the second block system. If $k(N/R) \notin \{65, 77\}$ then $k(N/R) \leq 55$ and $k(G) \leq |G : K| \cdot k(K/N) \cdot k(N) \leq 24 \cdot 5^6 \cdot 2^{12} \cdot 55 \leq 5^{47/3}$, so now assume $k(N/R) \in \{65, 77\}$. It can be checked by [27] that $k(S_2 \wr N/R) \in \{1165, 1265, 1960, 2210\}$. By the Clifford-Gallagher formula (Lemma 3.2), $k(N) \leq k(S_2 \wr N/R) \leq 2210$ hence we have that $k(G) \leq |G : K| \cdot k(K/N) \cdot k(N) \leq 24 \cdot 5^6 \cdot 2210 \leq 5^{47/3}$.

4 The minimal base size of a linear group

The solution of the $k(GV)$ problem has consequences on the minimal base size of a linear group. In this chapter we will see such an application. Let V be a finite vector space over a finite field of order q and of characteristic p. Let $G \leq GL(V)$ be a p-solvable completely reducible linear group. Theorem 1.6 states that there exists a base for G on V of size at most 2 unless $q \leq 4$ in which case there exists a base of size at most 3. This extends a recent result of Halasi and Podoski and generalizes a theorem of Seress. In this chapter we will also establish Theorem 1.7. This result will be used in the next chapter.

4.1 Preliminaries

Throughout this chapter let $\mathbb{F}_q$ be a finite field of characteristic p and let V be an n-dimensional vector space over $\mathbb{F}_q$. Furthermore, let $G \leq GL(V)$ be a linear group acting on V in the natural way, let $b(G)$ denote its minimal base size, and let $b^*(G)$ denote its minimal strong base size (both notions defined in Chapter 1).

If the vector space V is fixed, then the group of scalar transformations of V (the center of $GL(V)$) will be denoted by Z. Thus $Z \simeq \mathbb{F}_q^\times$, the multiplicative group of the base field. As $G \leq GL(V)$ is p-solvable if and only if GZ is p-solvable, we can (and we will) always assume, in the proofs of Theorems 1.6 and 1.7, that G contains Z. After choosing a basis $\{v_1, \ldots, v_n\} \subseteq V$, we will always identify the group $GL(V)$ with the group $\mathrm{GL}_n(q)$.

Put $t(q) = 3$ for $q \leq 4$ and $t(q) = 2$ for $q \geq 5$.

Finally, if $G \leq GL(V)$ and $X \subseteq V$, then $C_G(X) = \{g \in G \mid g(x) = x \ \forall\, x \in X\}$ and $N_G(X) = \{g \in G \mid g(x) \in X \ \forall\, x \in X\}$ will denote the pointwise and setwise stabilizer of X in G, respectively.

4.2 Special bases in linear groups

In this section we will show that there exist bases of special kinds for certain linear groups. As a consequence (Corollary 4.3), we derive that it is sufficient to establish the required bounds in Theorem 1.6 for $b(G)$ rather than for $b^*(G)$.

Theorem 4.1. *Let V be an n-dimensional vector space over $\mathbb{F}_q$, a field of characteristic p and let $Z \leq G \leq GL(V)$ be a p-solvable linear group.*

1. *If $n = 2$ and $q \geq 5$, then at least one of the following holds.*
   a) *There is a basis $x, y \in V$ such that $N_G(\langle x \rangle) \subseteq N_G(\langle y \rangle)$.*
   b) *$p = 2$ and there is a basis $x, y \in V$ such that $N_G(\langle x \rangle) = Z \times C_2$ and the involution g in $N_G(\langle x \rangle)$ satisfies $g(x) = x$ and $g(y) = y + x$.*
2. *If $n = 3$ and $q = 3$ or 4, then at least one of the following holds.*
   a) *There is a basis $x, y, z \in V$ such that $N_G(\langle x \rangle) \cap N_G(\langle y \rangle) \subseteq N_G(\langle z \rangle)$.*
   b) *There is a basis $x, y, z \in V$ such that $N_G(\langle y, z \rangle) = G$.*

Proof. If $G \leq GL(V)$ leaves invariant a 1-dimensional subspace of V, then 1/(a) or 2/(a) is satisfied. If $n = 3$ and G leaves invariant a 2-dimensional subspace of V then 2/(b) is satisfied. Thus we may assume that G acts irreducibly on V.

If G acts imprimitively on V then it embeds in $C_{q-1} \wr S_n$ where the base group acts on $\langle x \rangle \oplus \langle y \rangle$ if $n = 2$ and on $\langle x \rangle \oplus \langle y \rangle \oplus \langle z \rangle$ if $n = 3$, for some vectors x, y, $z \in V$. In the first case $N_G(\langle x \rangle)$ is diagonalizable and thus 1/(a) is satisfied, while in the second case $N_G(\langle x \rangle) \cap N_G(\langle y \rangle)$ is diagonalizable and thus 2/(a) is satisfied. We may thus assume that G acts primitively (and irreducibly) on V.

Since G is p-solvable by assumption, we see that G does not contain $SL(V)$.

First consider statement (1). By considering the action of G on the set S of 1-dimensional subspaces of V, we may assume that the number of Sylow p-subgroups of G is equal to $|S| = q + 1$. For otherwise there exists $\langle x \rangle \in S$ whose stabilizer in G is a p'-group and thus Maschke's theorem gives 1/(a). For $q = p$ any subgroup of $GL(V)$ with $q + 1$ Sylow p-subgroups contains $SL(V)$, so in this case we are done. So assume that $q > p$.

Since G acts transitively on the set of Sylow p-subgroups of G and every Sylow p-subgroup stabilizes a unique subspace in S, it follows that G acts transitively on S. Moreover since $Z \leq G$ it also follows that G acts transitively on the set of non-zero vectors of V.

By Hering's theorem (see [55, Chapter XII, Remark 7.5 (a)]) we see that if q is odd (and not a prime by assumption) then q must be 9 and G has a normal subgroup isomorphic to $\mathrm{SL}_2(5)$ (case (5)). But then G is not 3-solvable and so we can rule out this possibility. Similarly, if q is even, then the only possibility is that $G \geq Z$ normalizes a Singer cycle $\mathrm{GL}_1(q^2)$ (case (1)). The only such group not satisfying 1/(a) is the full semilinear group $\Gamma(1, q^2) \simeq \mathrm{GL}_1(q^2).2$. In this case taking x to be any non-zero vector in V we have $N_G(\langle x \rangle) = Z \times C_2$ and the involution g in $N_G(\langle x \rangle)$ satisfies $g(x) = x$ and $g(y) = y + x$ for some $y \in V$.

Finally, statement (2) has been checked with [27] by using the list of all primitive

permutation groups of degrees 27 and 64, respectively. □

As a direct consequence we get the following.

Corollary 4.2. *Let us assume that $Z \leq G \leq GL(V)$ is a p-solvable linear group with $b(G) \leq t(q)$.*

1. *If $q \geq 5$, then one of the following holds.*
   a) *There exists a base $x, y \in V$ such that $N_G(\langle x \rangle) \cap N_G(\langle x, y \rangle) \subseteq N_G(\langle y \rangle)$.*
   b) *$p = 2$ and there exists a base $x, y \in V$ such that any non-identity element of $C_G(x) \cap N_G(\langle x, y \rangle)$ takes y to $y + x$.*
2. *If $q \leq 4$, then at least one of the following holds.*
   a) *There exists a base $x, y, z \in V$ such that*
   $$N_G(\langle x \rangle) \cap N_G(\langle y \rangle) \cap N_G(\langle x, y, z \rangle) \subseteq N_G(\langle z \rangle).$$
   b) *There exists a base $x, y, z \in V$ such that $N_G(\langle x, y, z \rangle) \subseteq N_G(\langle y, z \rangle)$ with $x \notin \langle y, z \rangle$.*

Proof. First, 1/(a) or 2/(a) holds if $\dim(V) < t(q)$ so assume that $\dim(V) \geq t(q)$. Both parts of the corollary can be proved by choosing a subspace $U \leq V$ of dimension $t(q)$ generated by a base for G and by restricting $N_G(U)$ to this subspace. Notice that the image of this restriction is also p-solvable, so Theorem 4.1 can be applied. □

Corollary 4.3. *Let V be a vector space over the field $\mathbb{F}_q$ of characteristic p. Let $Z \leq G \leq GL(V)$ be p-solvable with $b(G) \leq t(q)$. Then $b^*(G) \leq t(q)$.*

Proof. We may assume that $\dim(V) \geq t(q)$ and that $q > 2$. Let us choose a base for G of size $t(q)$ satisfying the property given in Corollary 4.2. For $q \geq 5$, if $x, y \in V$ is such a base, then $x, x + y$ is a strong base for G. Likewise, for $q = 3$ or 4, if $x, y, z \in V$ is a base satisfying (2/a) of Corollary 4.2, then $x, y, x + y + z$ is a strong base for G. Finally, in case $x, y, z \in V$ is a base for G satisfying (2/b) of Corollary 4.2, then $x, y + x, z + x$ is a strong base for G. □

4.3 Further reductions

Let us use induction on the dimension n of V in the proofs of Theorems 1.6 and 1.7. The case $n = 1$ is clear. Let us assume that $n > 1$ and that both Theorems 1.6 and 1.7 are true for dimensions less than n.

First we reduce the proof of both theorems for the case when $G \leq GL(V)$ acts irreducibly on V. For otherwise let $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ be a decomposition of V to irreducible $\mathbb{F}_q G$-modules.

By induction, there exist vectors $x_{i,1}, \ldots, x_{i,t(q)}$ in V_i for $1 \leq i \leq k$ with the property that $C_G(\{x_{i,1}, \ldots, x_{i,t(q)}\})$ is precisely the kernel of the action of G on V_i. Now put $x_j = \sum_{i=1}^{k} x_{i,j}$ for $1 \leq j \leq t(q)$. One can see that $C_G(\{x_1, \ldots, x_{t(q)}\}) = \cap_{i=1}^{k} C_G(V_i) = 1$.

For Theorem 1.7 notice that G is a subgroup of a direct product $\times_{i=1}^{k} H_i$ of p-solvable groups H_i acting irreducibly and faithfully on the V_i's. Hence we have

$$|G| \leq \prod_{i=1}^{k} |H_i| \leq \prod_{i=1}^{k} \left(24^{-1/3}|V_i|^{c_1}\right) = 24^{-k/3}|V|^{c_1}$$

by induction.

So from now on we will assume that $G \leq GL(V)$ acts irreducibly on V.

For Theorem 1.6 we may also assume that $q \neq 2, 4$. Otherwise, G is solvable by the Odd Order Theorem and we can use the result of Seress [104].

For Theorem 1.7 we may assume that $|G| > |V|^2$. If $|G| \leq |V|^2$ then $|V|^2 < 24^{-1/3}|V|^{c_1}$ for $|V| \geq 79$, so we may assume that $|V| \leq 73$. If $|V|$ is a prime or $p = 2$ then G is solvable and the theorem of Pálfy [89] and Wolf [115] can be applied. Hence the cases $|V| = 5^2, 7^2, 3^2$ or 3^3 remain to be examined. But in these cases there is no non-solvable, p-solvable irreducible subgroup of $GL(V)$ (see [27]).

Now, if $b(G) \leq 2$ then $|G| \leq |V|^2$. So, once Theorem 1.1 is proved, it remains to prove Theorem 1.7 only in case $q = 3$ and $b(G) > 2$.

4.4 Imprimitive linear groups

In this section we show that we may assume (for the proofs of Theorems 1.6 and 1.7) that G is a primitive (irreducible) subgroup of $GL(V)$.

We first consider Theorem 1.6.

For $G \leq GL(V)$ an irreducible imprimitive linear group, let $V = V_1 \oplus \cdots \oplus V_k$ be a decomposition of V into subspaces such that G permutes these subspaces in a transitive and primitive way. This action of G defines a homomorphism from G into the symmetric group $\mathrm{Sym}(\Omega)$ for $\Omega = \{V_1, \ldots, V_k\}$ with kernel N.

The factor group $G/N \leq S_k$ is p-solvable, so it does not involve A_q for $q \geq 5$ and it does not involve A_5 for $q = 3$. By using [45, Theorem 2.3] it follows that for $q \geq 5$ there is a vector $a = (a_1, \ldots, a_k) \in \mathbb{F}_q^k$ such that $C_{G/N}(a) = 1$. (Here, G/N acts on $\mathbb{F}_q^k$ by permuting coordinates.) If $q = 3$ then again by [45, Theorem 2.3] we know that there is a 5 (and thus 9) part partition of Ω whose stabilizer in G/N is trivial. This implies that, for $q = 3$, there is a pair of vectors $a = (a_1, \ldots, a_k),\ b = (b_1, \ldots, b_k) \in \mathbb{F}_3^k$ such that $C_{G/N}(a) \cap C_{G/N}(b) = 1$.

In fact for $q \geq 8$ even we can say a bit more. For such a q let S be a subset of $\mathbb{F}_q$ of size $q/2$ with the property that for each $c \in \mathbb{F}_q$ exactly one of c and $c+1$ is contained in

S. By [14, Lemma 1 (c)], there is a $4 \leq q/2$ part partition of Ω whose stabilizer in G is N, so there exists a vector $a = (a_1, \dots, a_k) \in S^k$ such that $C_{G/N}(a) = 1$. (Actually, in our case, this already follows from [29, Theorem 1] by noting that since q is even, $p = 2$, and thus G/N is a solvable primitive permutation group.)

For each $1 \leq i \leq k$ let $H_i = N_G(V_i)$, so $N = \cap_i H_i$. By induction (on the dimension), there is a base in V_1 of size $t(q)$ for $H_1/C_{H_1}(V_1)$.

Now we can use Corollary 4.2. First let $q \geq 5$. Then there is a base $x_1, y_1 \in V_1$ for $K_1 = H_1/C_{H_1}(V_1) \leq GL(V_1)$ such that $N_{K_1}(\langle x_1 \rangle) \cap N_{K_1}(\langle x_1, y_1 \rangle) \subseteq N_{K_1}(\langle y_1 \rangle)$ or that any non-identity element of $C_{K_1}(x_1) \cap N_{K_1}(\langle x_1, y_1 \rangle)$ takes y_1 to $y_1 + x_1$.

Let $\{g_1 = 1, g_2, \dots, g_k\}$ be a set of left coset representatives for H_1 in G and $x_i = g_i x_1,\ y_i = g_i y_1$ for every i. Now let $x = \sum_{i=1}^k x_i$ and $y = \sum_{i=1}^k y_i + a_i x_i$.

In case $q = 3$ let $x_1, y_1, z_1 \in V_1$ be a base for $K_1 = H_1/C_{H_1}(V_1) \leq GL(V_1)$ satisfying (2/a) or (2/b) of Corollary 4.2. Again, let $\{g_1 = 1, g_2, \dots, g_k\}$ be a set of left coset representatives for H_1 in G and $x_i = g_i x_1,\ y_i = g_i y_1,\ z_i = g_i z_1$ for every i. Depending on which part of part (2) of Corollary 4.2 is satisfied for x_1, y_1, z_1 let

$$x = \sum_{i=1}^k x_i, \qquad y = \sum_{i=1}^k y_i \qquad z = \sum_{i=1}^k (z_i + b_i x_i + a_i y_i) \qquad \text{if (2/a) holds,}$$

$$x = \sum_{i=1}^k x_i, \qquad y = \sum_{i=1}^k (y_i + a_i x_i) \qquad z = \sum_{i=1}^k (z_i + b_i x_i) \qquad \text{if (2/b) holds.}$$

In each case, it is easy to see that the given set of vectors is a base for G by using similar arguments as in the proof of [45, Theorem 2.6]. For the convenience of the reader, we present a proof here for the case (2/a).

Let x, y, z given as above and $g \in C_G(x) \cap C_G(y) \cap C_G(z)$. Furthermore, let $\sigma \in S_k$ be the permutation associated to the action of g on $\Omega = \{V_1, \dots, V_k\}$. Then $g(x) = x,\ g(y) = y$ implies that $g(x_i) = x_{\sigma(i)},\ g(y_i) = y_{\sigma(i)}$ for every $1 \leq i \leq k$. Using also that $g(z) = z$ we get that

$$z_{\sigma(i)} + b_{\sigma(i)} x_{\sigma(i)} + a_{\sigma(i)} y_{\sigma(i)} = g(z_i + b_i x_i + a_i y_i) = g(z_i) + b_i x_{\sigma(i)} + a_i y_{\sigma(i)},$$

thus, $g(z_i) = z_{\sigma(i)} + (b_{\sigma(i)} - b_i) x_{\sigma(i)} + (a_{\sigma(i)} - a_i) y_{\sigma(i)}$. Now, $h = g_{\sigma(i)}^{-1} g g_i \in H_1$ satisfies

$$h(x_1) = x_1,\ h(y_1) = y_1,\ h(z_1) = z_1 + (b_{\sigma(i)} - b_i) x_1 + (a_{\sigma(i)} - a_i) y_1.$$

By part (2/a) of Corollary 4.2 we conclude that $b_{\sigma(i)} = b_i$ and $a_{\sigma(i)} = a_i$ for every $1 \leq i \leq k$. In other words, σ fixes both $(a_1, \dots, a_k)$ and $(b_1, \dots, b_k)$. By the defintion of these vectors we get that $\sigma = 1$, i.e. $g \in \cap_i H_i = N$. Furthermore, for every $1 \leq i \leq k$ we also have $g(x_i) = x_i,\ g(y_i) = y_i,\ g(z_i + b_i x_i + a_i y_i) = z_i + b_i x_i + a_i y_i$. Since $x_i, y_i, z_i + b_i x_i + a_i y_i \in V_i$ is a base for $H_i/C_{H_i}(V_i)$, we get that $g = \cap_i C_{H_i}(V_i) = 1$.

Now we turn to the reduction of Theorem 1.7 to primitive groups. Notice that N is a p-solvable group and V is the sum of at least k irreducible $\mathbb{F}_q N$-modules, so we have

$|N| \leq 24^{-k/3}|V|^{c_1}$ by Section 4.3. By the last paragraph of Section 4, we may assume that $q = 3$ (and $p = 3$). In particular, the permutation group $G/N \leq S_k$ is 3-solvable, and so it does not contain any non-Abelian alternating composition factor. Now [80, Corollary 1.5] implies that $|G/N| \leq 24^{(k-1)/3}$. But then $|G| = |N||G/N| \leq 24^{-1/3}|V|^{c_1}$ which is exactly what we wanted.

4.5 Groups of semilinear transformations

In this section we reduce Theorems 1.6 and 1.7 to the case when every irreducible $\mathbb{F}_q N$-submodule of V is absolutely irreducible for any normal subgroup N of G.

For this purpose let $N \lhd G$ be a normal subgroup of G. Then V is a homogeneous $\mathbb{F}_q N$-module, so $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, where the V_i's are isomorphic irreducible $\mathbb{F}_q N$-modules. Let $T := \mathrm{End}_{\mathbb{F}_q N}(V_1)$. Assuming that the V_i's are not absolutely irreducible, T is a proper field extension of $\mathbb{F}_q$, and

$$C_{GL(V)}(N) = \mathrm{End}_{\mathbb{F}_q N}(V) \cap GL(V) \simeq \mathrm{GL}_k(T),$$

since $\mathrm{End}_{\mathbb{F}_q N}(V)$ is isomorphic to the matrix algebra $M_k(T)$ by [18, Theorem 1.7.5]

Furthermore, $L = Z(C_{GL(V)}(N)) \simeq Z(\mathrm{GL}_k(T)) \simeq T^{\times}$. Now, by using L, we can extend V to a T-vector space of dimension $l := \dim_T V < \dim_{\mathbb{F}_q} V$. As $G \leq N_{GL(V)}(L)$, in this way we get an inclusion $G \leq \Gamma\mathrm{L}_l(T)$. We proceed by proving the following theorem.

Theorem 4.4. *For a proper field extension T of $\mathbb{F}_q$ let $G \leq \Gamma\mathrm{L}_l(T)$ be a semilinear group acting on the $\mathbb{F}_q$-space V and let $H = G \cap \mathrm{GL}_l(T)$. Suppose that G is p-solvable and that $b(H) \leq t(|T|)$. Then $b(G) \leq t(|T|)$.*

Proof. We modify the proof of [45, Lemma 6.1] to make it work in this more general setting.

Clearly we may assume that $|T| \geq 8$ is different from a prime. In these cases $t(|T|) = 2$.

Let u_1, u_2 be a base for H. By Corollary 4.2, we may also assume that

$$N_H(\langle u_1 \rangle) \cap N_H(\langle u_1, u_2 \rangle) \subseteq N_H(\langle u_2 \rangle)$$

or that every non-identity element of $C_H(u_1) \cap N_H(\langle u_1, u_2 \rangle)$ takes u_2 to $u_2 + u_1$. (The latter case occurs only if $p = 2$.)

For every $\alpha \in T$ let $H_\alpha = C_G(u_1) \cap C_G(u_2 + \alpha u_1) \leq G$. Our goal is to prove that $H_\alpha = 1$ for some $\alpha \in T$. If $g \in \langle \cup H_\alpha \rangle$, then $g(u_1) = u_1$ and $g(u_2) = u_2 + \delta u_1$ for some $\delta \in T$.

We claim that $|\langle \cup H_\alpha \rangle \cap H| \leq 2$. Let $h \in \langle \cup H_\alpha \rangle \cap H$. On the one hand, the action of h on V is T-linear, since $h \in H$. On the other hand, $h(u_1) = u_1$ and $h(u_2) = u_2 + \delta u_1$

for some $\delta \in T$. By our assumption above, either $h \in N_H(\langle u_2 \rangle)$ and $\delta = 0$, or h is an involution and $\delta = 1$. Thus we obtain the claim since $C_H(u_1) \cap C_H(u_2) = 1$.

Let z be the generator of the group $\langle \cup H_\alpha \rangle \cap H$. This is a central element in $\langle \cup H_\alpha \rangle$. For every $g \in G$ let $\sigma_g \in \mathrm{Gal}(T|\mathbb{F}_q)$ denote the action of g on T.

Let g and h be two elements of $\langle \cup H_\alpha \rangle$. Since G/H is embedded into $\mathrm{Gal}(T|\mathbb{F}_q)$, we get $\sigma_g \neq \sigma_h$ unless $g = h$ or $g = hz$. Furthermore, a routine calculation shows that the subfields of T fixed by σ_g and σ_h are the same if and only if $\langle g \rangle = \langle h \rangle$ or $\langle g \rangle = \langle hz \rangle$.

If $g \in H_\alpha \cap H_\beta$, then $g(u_2) = u_2 + (\alpha - \alpha^{\sigma_g})u_1 = u_2 + (\beta - \beta^{\sigma_g})u_1$, so $\alpha - \beta$ is fixed by σ_g. Let $K_g = \{\alpha \in T \mid g \in H_\alpha\}$. The previous calculation shows that K_g is an additive coset of the subfield fixed by σ_g, so $|K_g| = p^d$ for some $d \mid f = \log_q |T|$. Since for any $d \mid f$ there is a unique p^d-element subfield of T, we get $|K_g| \neq |K_h|$ unless the subfields fixed by σ_g and σ_h are the same. As we have seen, this means that $\langle g \rangle = \langle h \rangle$ or $\langle g \rangle = \langle hz \rangle$. Consequently, $|K_g| \neq |K_h|$ unless $K_g = K_h$ or $K_g = K_{hz}$. Hence we get

$$\Big| \bigcup_{g \in \cup H_\alpha \setminus \{1\}} K_g \Big| \leq 2 \sum_{d|f, d<f} q^d \leq 2 \sum_{d<f} q^d < q^f = |T|.$$

So there is a $\gamma \in T$ which is not contained in K_g for any $g \in \cup H_\alpha \setminus \{1\}$. This exactly means that $H_\gamma = C_G(u_1) \cap C_G(u_2 + \gamma u_1) = 1$. □

Using Theorem 4.4, we can assume that $G \leq \mathrm{GL}_l(T)$. As $l = \dim_T V < \dim_{\mathbb{F}_q}(V)$, we can use induction on the dimension of V, thus $b(G) \leq 2$.

By the last paragraph of Section 4.3, we need not consider Theorem 1.7 here.

Hence in the following we assume that V is a direct sum of isomorphic absolutely irreducible $\mathbb{F}_q N$-modules for any $N \lhd G$.

4.6 Stabilizers of tensor product decompositions

Let $N \lhd G$ and let $V = V_1 \oplus \cdots \oplus V_k$ be a direct decomposition of V into isomorphic absolutely irreducible $\mathbb{F}_q N$-modules. By choosing a suitable basis in $V_1, V_2, \ldots, V_k$, we can assume that $G \leq \mathrm{GL}_n(q)$ such that any element of N is of the form $A \otimes I_k$ for some $A \in N_{V_1} \leq \mathrm{GL}_{n/k}(q)$. By using [62, Lemma 4.4.3(ii)] we get

$$N_{\mathrm{GL}_n(q)}(N) = \{B \otimes C \mid B \in N_{\mathrm{GL}_{n/k}(q)}(N_{V_1}),\ C \in \mathrm{GL}_k(q)\}.$$

Let $G_1 = \{g_1 \in \mathrm{GL}_{n/k}(q) \mid \exists g \in G, g_2 \in \mathrm{GL}_k(q) \text{ such that } g = g_1 \otimes g_2\}$. We define $G_2 \leq \mathrm{GL}_k(q)$ in an analogous way. Then $G \leq G_1 \otimes G_2$. Here $G/Z \simeq (G_1/Z) \times (G_2/Z)$, hence $G_1 \leq \mathrm{GL}_{n/k}(q)$ and $G_2 \leq \mathrm{GL}_k(q)$ are p-solvable irreducible linear groups. If $1 < k < n$, then by using induction for $G_1 \leq \mathrm{GL}_{n/k}(q)$ and $G_2 \leq \mathrm{GL}_k(q)$ we get $b(G_1) \leq t(q)$ and $b(G_2) \leq t(q)$. Furthermore $b^*(G_1) \leq t(q)$ and $b^*(G_2) \leq t(q)$ by

Corollary 4.3. Thus [73, Lemma 3.3 (ii)] gives us $b(G) \leq b(G_1 \otimes G_2) \leq b^*(G_1 \otimes G_2) \leq \max(b^*(G_1), b^*(G_2)) \leq t(q)$.

For the reduction of Theorem 1.7, by using induction on the dimension, we have

$$|G| \leq |G_1| \cdot |G_2| \leq 24^{-1/3} q^{(n/k)c_1} \cdot 24^{-1/3} q^{kc_1} \leq 24^{-1/3} |V|^{c_1}.$$

Thus, from now on we can assume that for every normal subgroup $N \lhd G$ either $N \leq Z$ or V is absolutely irreducible as an $\mathbb{F}_q N$-module.

4.7 Groups of symplectic type

From now on assume that N is a normal subgroup of G containing Z such that N/Z is a minimal normal subgroup of G/Z. Then N/Z is a direct product of isomorphic simple groups. In this section we examine the situation when N/Z is an elementary Abelian group.

If N is Abelian then it is central in G. So assume that N is non-Abelian.

If N/Z is elementary Abelian of rank at least 2, then G is of symplectic type. Such groups were examined in [45, Section 5] (see also Remark 5.20 in [45]) where it was proved that $b(G) \leq 2$ unless $q \in \{3, 4\}$, when $b(G) \leq 3$ holds.

For the reduction of Theorem 1.7, we need only examine the case $q = 3,\ n = 2^k$. For this we can use the fact that G/N can be considered as a subgroup of the symplectic group $\mathrm{Sp}_{2k}(2)$. By the theorem of Pálfy [89] and Wolf [115], we may assume that G is a non-solvable (and 3-solvable) group. Thus we must have a composition factor of G (and thus of G/N) isomorphic to a Suzuki group. Since the smallest Suzuki group Suz(8) has order larger than $|\mathrm{Sp}_4(2)|$, we must have $k \geq 3$. On the other hand, since the second largest Suzuki group Suz(32) has order larger than $|\mathrm{Sp}_6(2)|$ and since Suz(8) is not a section of $\mathrm{Sp}_6(2)$ (since 13 divides the order of the first group but not the order of the second), we see that $k \neq 3$. But for $k \geq 4$ we clearly have $|G| = |N||G/N| < 2^{2k^2+3k+3} < 24^{-1/3}|V|^{c_1}$, by use of the formula for the order of $\mathrm{Sp}_{2k}(2)$.

4.8 Tensor product actions

Now let N/Z be a direct product of $t \geq 2$ isomorphic non-Abelian simple groups. Then $N = L_1 \star L_2 \star \cdots \star L_t$ is a central product of isomorphic groups such that for every $1 \leq i \leq t$ we have $Z \leq L_i,\ L_i/Z$ is simple. Furthermore, conjugation by elements of G permutes the subgroups $L_1, L_2, \ldots, L_t$ in a transitive way. By choosing an irreducible $\mathbb{F}_q L_1$-module $V_1 \leq V$, and a set of coset representatives $g_1 = 1, g_2, \ldots, g_t \in G$ of $G_1 = N_G(V_1)$ such that $L_i = g_i L_1 g_i^{-1}$, we get that $V_i := g_i V_1$ is an absolutely irreducible $\mathbb{F}_q L_i$-module for each $1 \leq i \leq t$. Now, $V \simeq V_1 \otimes V_2 \otimes \cdots \otimes V_t$ and G permutes the factors of this tensor product. It follows that G is embedded into the central wreath product $G_1 \wr_c S_t$ defined to

be a split extension of the base group $\underbrace{G_1 \otimes G_1 \otimes \cdots \otimes G_1}_{t \text{ factors}}$ by S_t. Clearly $G_1 \leq GL(V_1)$ is a p-solvable irreducible linear group. Thus $b(G_1) \leq t(q)$ and $b^*(G_1) \leq t(q)$ by induction on the dimension m of V_1 and by Corollary 4.3.

First let $q \geq 5$. Then $t(q) = 2$. Thus $b(G) \leq 2$ follows from [45, Theorem 3.6] unless $(m,t) = (2,2)$. In case $(m,t) = (2,2)$, that is, $G \leq G_1 \wr_c S_2 \leq \mathrm{GL}_4(q)$ for some p-solvable group $G_1 \leq \mathrm{GL}_2(q)$ let $x_1, y_1 \in V_1$ be a basis of V_1 satisfying either $N_{G_1}(\langle x_1 \rangle) \subseteq N_{G_1}(\langle y_1 \rangle)$ or the property that every non-identity element of $C_{G_1}(x_1)$ takes y_1 to $y_1 + x_1$. (Such a basis exists by Theorem 4.1.) We claim that if $\alpha \in \mathbb{F}_q \setminus \{0,1\}$ then $x_1 \otimes x_1,\ y_1 \otimes (y_1 + \alpha x_1)$ is a base for $G_1 \wr_c S_2 \geq G$. Indeed, let $g = (A \otimes B)\sigma \in G_1 \wr_c S_2$ with $A, B \in G_1,\ \sigma \in S_2$ fixing these two vectors. Then $g(x_1 \otimes x_1) = x_1 \otimes x_1$ implies that $Ax_1 = \lambda x_1,\ Bx_1 = \lambda^{-1} x_1$ for some $\lambda \in \mathbb{F}_q^\times$. If $N_{G_1}(\langle x_1 \rangle) \subseteq N_{G_1}(\langle y_1 \rangle)$, then $Ay_1 = a y_1,\ By_1 = b y_1$ for some $a, b \in \mathbb{F}_q^\times$. Hence

$$y_1 \otimes (y_1 + \alpha x_1) = g(y_1 \otimes (y_1 + \alpha x_1)) = aby_1 \otimes y_1 + \alpha a \lambda^{-1} (y_1 \otimes x_1)^\sigma.$$

Comparing the coefficients of $y_1 \otimes y_1$ and $y_1 \otimes x_1$ in the above equality we get $ab = a\lambda^{-1} = 1$ and $\sigma = 1$. So, $A = \lambda I,\ B = \lambda^{-1} I$ and $g = 1$, as claimed. Similarly, if every non-identity element of $C_{G_1}(x_1)$ takes y_1 to $y_1 + x_1$, then by multiplying A with λ^{-1} and B with λ, we can assume that $\lambda = 1$. Then for some $\varepsilon_a, \varepsilon_b \in \{0,1\}$ we have

$$y_1 \otimes (y_1 + \alpha x_1) = g(y_1 \otimes (y_1 + \alpha x_1)) = \Big((y_1 + \varepsilon_a x_1) \otimes (y_1 + (\alpha + \varepsilon_b) x_1)\Big)^\sigma.$$

Comparing the coefficients of $x_1 \otimes x_1, x_1 \otimes y_1$ and $y_1 \otimes x_1$ we get $\varepsilon_a = \varepsilon_b = 0,\ \sigma = 1$, so $g = 1$ follows.

Now, let $q = 3$. Let $x_1, y_1, z_1 \in V_1$ be a strong base for G_1. Then the stabilizer of $\underbrace{x_1 \otimes x_1 \otimes \cdots \otimes x_1}_{t \text{ factors}} \in V$ is of the form $H = H_1 \wr_c S_t$, where $y_1, z_1 \in V_1$ is a strong base for $H_1 = N_{G_1}(x_1)$, so $b^*(H_1) \leq 2$. If $(m,t) \neq (2,2)$ then $b(H) \leq 2$ by [45, Theorem 3.6], which results in $b(G) \leq 3$. Finally, let $(m,t) = (2,2)$. By choosing a basis $x_1, y_1 \in V_1$, it is easy to see that $x_1 \otimes x_1, y_1 \otimes y_1, x_1 \otimes y_1 \in V$ is a base for $GL(V_1) \wr_c S_2 \geq G$.

As for the order of G notice that $G \leq G_1 \wr_c S$ where $S \leq S_t$ is a 3-solvable group. Thus by induction and by [80, Corollary 1.5] we have

$$|G| \leq |G_1|^t |S| \leq 24^{-t/3} |V_1|^{c_1 t} 24^{(t-1)/3} = 24^{-1/3} |V|^{c_1}.$$

4.9 Almost quasisimple groups

Finally, let $Z \leq N \lhd G$ be such that N/Z is a non-Abelian simple group. Let $N_1 = [N,N] \lhd G$ and let V_1 be an irreducible $\mathbb{F}_p N_1$-submodule of V and $G_1 = \{g \in G \mid g(V_1) = V_1\}$ be the stabilizer of V_1. By using the same argument as in the last paragraph of [45, Page 29] we get that G_1 is included in $GL(V_1)$ and we have a chain of subgroups

$N_1 \lhd G_1 \leq GL(V_1)$ where G_1 is p-solvable, N_1 is quasisimple and V_1 is irreducible as an $\mathbb{F}_p N_1$-module.

Suppose that $b(G_1) \leq 2$ in the action of G_1 on V_1, that is, there exist $x, y \in V_1 \leq V$ such that $C_{G_1}(x) \cap C_{G_1}(y) = 1$. For any element $g \in G$ with $g(x) = x$ we have that $N_1 x = \{nx \,|\, n \in N_1\}$ is a g-invariant subset. As the $\mathbb{F}_p$-subspace generated by $N_1 x$ is exactly V_1, we get that $g \in G_1$. This proves that $C_G(x) \cap C_G(y) = C_{G_1}(x) \cap C_{G_1}(y) = 1$. Thus $b(G) \leq 2$.

Hence if we manage to show that $b(G_1) \leq 2$ then we are finished with the proofs of both Theorems 1.6 and 1.7.

So assume that $G = G_1$, $N = N_1$, and $V = V_1$. By the first three paragraphs of this section, we have that $q = p$. To summarize, $G \leq GL(V)$ is a group having a quasisimple irreducible normal subgroup N and $Z \leq G$.

We can assume that G/Z is almost simple. For this it is sufficient to see that N/Z is the unique minimal normal subgroup of G/Z. For let M/Z be another minimal normal subgroup of G/Z. By Section 4.7, we may assume that M/Z is non-Abelian. Furthermore the group MN is a central product and so $[M, N] = 1$. But this is impossible since the centralizer of N in G must be Abelian.

Lemma 4.5. *If N has a regular orbit on V then $b(G) \leq 2$.*

Proof. Since N is normal in G, a regular N-orbit Δ containing a given vector v is a block of imprimitivity inside the G-orbit containing v. Hence the group $C_G(v)N$ is transitive on Δ and N is regular on Δ. Thus for every $h \in C_G(v)$ the number $|\mathrm{fix}(h)|$ of fixed points of h on Δ is $|C_N(h)|$. To prove that G has a base of size at most 2 on V, it is sufficient to see that there exists a vector w in Δ that is not fixed by any non-trivial element of $C_G(v)$.

First notice that if $N/Z(N)$ is isomorphic to the non-Abelian finite simple group S then $|C_G(v)| \leq |\mathrm{Out}(S)| < m(S)$ where $m(S)$ is the minimal index of a proper subgroup of S. This latter inequality follows from [3, Lemma 2.7 (i)].

But $\sum |\mathrm{fix}(h)| = \sum |C_N(h)| < |C_G(v)| \cdot (|N|/m(S)) < |N|$ where the sums are over all non-identity elements h in $C_G(v)$. This completes the proof of the lemma. □

By Lemma 4.5, in the following we may assume that N does not have a regular orbit on V. Our final theorem finishes the proofs of Theorems 1.6 and 1.7.

Theorem 4.6. *Under the current assumptions G is a p'-group and $b(G) \leq 2$.*

Proof. By using Goodwin's theorem [32, Theorem 1], Köhler and Pahlings [67, Theorem 2.2] gave a complete list of (irreducible) quasisimple p'-groups N such that N does not have a regular orbit on V. In all these exceptional cases, when N/Z is simple, $|\mathrm{Out}(N/Z)|$ is divisible by no prime larger than 3 while p is always at least 5. So G itself is a p'-group. But then G admits a base of size 2 on V by [45, Theorem 4.4]. □

5 Normalizers of primitive permutation groups

Let G be a transitive normal subgroup of a permutation group A of finite degree n. The factor group A/G can be considered as a certain Galois group and one would like to bound its size. One of the results of this chapter is that $|A/G| < n$ if G is primitive unless $n = 3^4$, 5^4, 3^8, 5^8, or 3^{16}. This bound is sharp when n is prime. In fact, when G is primitive, $|\operatorname{Out}(G)| < n$ unless G is a member of a given infinite sequence of primitive groups and n is different from the previously listed integers. In this chapter many other results of this flavor are established not only for permutation groups but also for linear groups.

5.1 Basic results on non-Abelian composition factors

If G is a finite group, define $b(G)$ to be the product of the orders of all the non-Abelian simple composition factors of G in a composition series for G. Two trivial observations that we shall use without comment are:

1. if G is normal in A, then $b(A) = b(A/G)b(G)$; and

2. if $A \leq B$, then $b(A) \leq b(B)$ (choose a normal series for B and intersect A with this series – Abelian quotients stay Abelian and the non-Abelian quotients can only get smaller).

The first lemma of the chapter is not used in later parts of the work, nevertheless it is worth mentioning.

Lemma 5.1. *Let X_1 and X_2 be two finite groups, $A \leq X_1 \times X_2$, and $G \lhd A$. For $i = 1, 2$ let π_i denote the projection into X_i. (We consider $\pi_i(A)$ and $\pi_i(G)$ as subgroups of X_i.) Then*

$$b(A/G) \leq b(\pi_1(A)/\pi_1(G))b(\pi_2(A)/\pi_2(G)).$$

Proof. Let K denote the kernel of π_1 on A. Notice that if $x \in \pi_2(K)$ and $y \in \pi_2(G)$ then $[x, y] \in \pi_2(G \cap K)$. Hence $b((\pi_2(K) \cap \pi_2(G))/\pi_2(K \cap G)) = 1$. From this we get

$$b(K/(K \cap G)) = b(\pi_2(K)/(\pi_2(K \cap G))) = b(\pi_2(K)/(\pi_2(K) \cap \pi_2(G))) =$$

$$= b(\pi_2(K)\pi_2(G)/\pi_2(G)) \leq b(\pi_2(A)/\pi_2(G)).$$

Since $b(A/G) = b(A/GK)b(GK/G) = b(\pi_1(A)/\pi_1(G))b(K/(K \cap G))$, the result follows. □

The next lemma is needed for a technical result (see Theorem 5.3) for dealing with non-Abelian composition factors.

Lemma 5.2. *Let $J \leq Y := X_1 \times \cdots \times X_t$ and assume that $\pi_i(J) = X_i$ for all i (where π_i is the projection onto the ith factor). Then $N_Y(J)/J$ is solvable.*

Proof. Set $N = N_Y(J)$. Let M be the final term in the derived series of N. Let $B_i = \ker \pi_i' \cap J$ where π_i' is the projection of Y onto the direct product of all but the ith term (so $B_i = J \cap X_i$).

Set $R = B_1 \times \cdots \times B_t$. Note that $R \lhd J$ and that R is also normal in Y since $\pi_i(J) = X_i$ for all i, whence we may pass to Y/R. If we prove the result in this case, then $MR/R \leq J/R$, and so $M \leq J$. Hence we may assume from now on that $R = 1$. If we prove the result in this case, then $MR/R \leq J/R$, whence $M \leq J$.

We induct on t. If $t = 1$, the result is clear.

Suppose that $t = 2$. Since $R = 1$, we may identify J as a diagonal subgroup of $X_1 \times X_2$ and the normalizer N is $J(Z \times Z)$ where $Z = Z(J)$, whence the result.

So now assume that $t > 2$. By induction, we have $\pi_i'(M) \leq \pi_i'(J)$, whence $M \leq J(N \cap X_i)$. Note that $[N \cap X_i, X_i] = [N \cap X_i, J] \leq X_i \cap J = 1$. Thus, $M = [M, M] \leq [J(N \cap X_i), J(N \cap X_i)] \leq J$ as claimed. □

Note that the proof shows that the derived length of $N_Y(J)/J$ is at most $t - 1$.

We now come to one of our major tools in studying $b(A/G)$.

Theorem 5.3. *Assume that $G \lhd A \leq B = X \wr \mathrm{S}_t = (X_1 \times \cdots \times X_t).\mathrm{S}_t = Y.\mathrm{S}_t$ and that G acts transitively on $\{X_1, \ldots, X_t\}$ by conjugation. Assume that the projection of $N_A(X_i)$ into X_i is X_i (note that $N_A(X_i) \leq X_i \times X_i'$ for an obvious choice of X_i'). Let $N_i = N_G(X_i)$ and set M_i to be the projection of N_i into X_i. Let K be the subgroup of A normalizing each X_i. Then*

$$b(A/G) \leq b(A/GK)b(X_1/M_1).$$

Proof. We have that $b(A/G) = b(A/GK)b(GK/G)$. So we only need to show that $b(GK/G) \leq b(X_1/M_1)$. Let $M = M_1 \times \cdots \times M_t$. Let $I = J_1 \times \cdots \times J_t$ where J_i is the projection of $J = K \cap G$ into X_i.

Note first that $[K, K \cap M] \leq I$ (since $[K, N_i] \leq [K, G] \leq J$). In particular, $(K \cap M)/(K \cap I)$ is Abelian. By Lemma 5.2, $(K \cap I)/J$ is solvable. Thus, $(K \cap M)/J$ is solvable and in particular, $b((K \cap M)/J) = 1$. Thus,

$$b(GK/G) = b(K/J) = b(K/(K \cap M)) = b(KM/M).$$

Put $H = \{y \in Y : [g, y] \in M \text{ for all } g \in G\}$. Notice that $KM \leq H$. From this $KM/M \leq H/M \leq Y/M$ follows. Since G permutes the t direct factors transitively, we see that H/M (and so KM/M) is contained in a full diagonal subgroup of $Y/M = \prod(X_i/M_i)$. Thus, $b(KM/M) \leq b(X_1/M_1)$ as claimed. □

We will use the following lemma.

Lemma 5.4. *Suppose that $n = m^t$. Then*

$$t^{\log t}(\log m)^{\log\log m} \leq (\log n)^{\log\log n}.$$

Proof. It suffices to prove that $(\log t)^2 + (\log\log m)^2 \leq (\log\log n)^2$. The right-hand side is equal to $(\log t + \log\log m)^2$, whence the result. □

5.2 Some examples

In this section, we consider several examples with $G \lhd A \leq \mathrm{S}_n$ always with A and G transitive. The first example shows that $|A/G| = n - 1$ may hold even with G primitive and that $b(A/G)$ can be on the order of $n^{\log n}$ if we only assume that G is transitive (note that when $n = 2^a$ for an integer a, then it is easy to see that $n^{\frac{1}{2}\log n} < |\mathrm{L}_a(2)| < n^{\log n}$). The third example shows that $b(A/G)$ can be close to $(\log n)^{2\log\log n}$ even when G is primitive.

Example 5.5. *Let p be a prime. Let V be a vector space over $\mathbb{F}_p$ of dimension a. Let $A = \mathrm{AGL}_a(p) = \mathrm{AGL}(V)$ be the full group of affine transformations of V. Let G be the normal subgroup of translations.*

1. *$G \lhd A$, G is transitive on V and A is primitive on V;*
2. *If $a = 1$, then G is primitive on V and $|A/G| = p - 1$;*
3. *If $a > 1$ and $(p, a) \neq (2, 2), (2, 3)$, then $b(A/G) = |\mathrm{L}_a(p)|$.*

Example 5.6. *Let $C \lhd D$ be transitive groups of degree t. Let $A = \mathrm{A}_5 \wr D$ and $G = \mathrm{A}_5 \wr C$. Then $G \lhd A$ and they both act primitively on a set of cardinality 5^t. Then $b(A/G) = b(D/C)$. In particular, considering the previous example yields examples of primitive A and G with $b(A/G) > t^{\frac{1}{2}\log t} > (\frac{1}{3}\log n)^{(\frac{1}{2}\log\log n)-2}$.*

For the third example and for later use the full symplectic group of dimension $2a$ (a and integer) over the prime field of order p is denoted by $\mathrm{Sp}_{2a}(p)$. Its order is $p^{a^2}\prod_{i=1}^{a}(p^{2i}-1)$. The group $\mathrm{Sp}_{2a}(p)$ has a center of size $(2, p-1)$, the greatest common divisor of 2 and $p-1$, and the corresponding factor group is denoted by $\mathrm{PSp}_{2a}(p)$. We will also need the orthogonal groups in this chapter however only for the field of size 2 (apart from Lemma 5.25). We denote the full orthogonal groups of dimension $2a$ (a and integer) over the field of order 2 by $\mathrm{O}^{\epsilon}_{2a}(2)$ where $\epsilon = \pm 1$. Their order is $2 \cdot 2^{a(a-1)}(2^a - \epsilon)\prod_{i=1}^{a-1}(2^{2i} - 1)$. The groups $\mathrm{O}^{\epsilon}_{2a}(2)$ have a subgroup of index 2 which we denote by $\mathrm{SO}^{\epsilon}_{2a}(2)$.

Example 5.7. *Let p be a prime. Let R be a p-group of symplectic type – i.e. $Z(R)$ is cyclic of order p or 4, $R/Z(R)$ is elementary Abelian of order p^{2a} for an integer a and R has exponent p for p odd and exponent 4 for $p = 2$. Let q be a prime power such that $q - 1$ is a multiple of p and a multiple of 4 if $|Z(R)| = 4$. Then R embeds in the group $\mathrm{GL}_{p^a}(q) = \mathrm{GL}(V)$. Let N be the normalizer of R in $\mathrm{GL}(V)$ and Z the group of scalars. Then $N/RZ \cong \mathrm{Sp}_{2a}(p)$ or $N/RZ \cong \mathrm{O}^\epsilon_{2a}(2)$ with the latter possibility occurring when $p = 2$ and $Z(R)$ is cyclic of order 2. In particular (except for some very small cases), $b(N/R) = |\mathrm{PSp}_{2a}(p)|$ or $|\mathrm{SO}^\epsilon_{2a}(2)|$. Let $G = VR$ and $A = VN$. Then A and G are primitive permutation groups on V and $b(A/G) = |\mathrm{PSp}_{2a}(p)|$ or $|\mathrm{SO}^\epsilon_{2a}(2)|$. In particular, when $q = 3$, $p = 2$ we obtain examples where $b(A/G)$ has size approximately $(\log n)^{2 \log \log n}$.*

For the proof of Theorem 1.9 we will need more information about 2-groups of symplectic type. By [1, (23.14)] there are, for each positive integer a, two extraspecial groups of order 2^{2a+1}. These are the central product of a copies of D_8 and the central product of $a - 1$ copies of D_8 with one copy of Q_8. The first can be thought of as an orthogonal space of $+$ type and the other an orthogonal space of $-$ type. The central product of a copies of D_8 with one copy of C_4 can be thought of as a symplectic space.

5.3 Normalizers of irreducible linear groups – Non-Abelian composition factors

In this section, we consider $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$ where V is a vector space of dimension d over the finite field of order q and want to bound $b(A/G)$ when G is irreducible on V. Of course, this is a special case of the problem for general pairs of primitive groups – this is equivalent to the setup for the case of groups acting primitively on an affine space.

Recall that a subgroup A of $\mathrm{GL}(V)$ is called primitive if it preserves no additive decomposition of V (i.e. there is no A-invariant collection of subspaces $V_1, \ldots, V_t$ with $V = \oplus_i V_i$). In particular, this implies that A is irreducible and every normal subgroup of A acts homogeneously on V (i.e. any two simple submodules are isomorphic). Recall also the definition of a p-group of symplectic type (see Example 5.7).

Theorem 5.8. *Let $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$. Set $n = q^d \geq 3$. Assume that G acts irreducibly on V and that A acts primitively on V. Assume that every irreducible J-submodule of V is absolutely irreducible for any normal subgroup J of G. Then $b(A/G) < (\log n)^{2 \log \log n}$.*

Proof. As we have already noted, every normal subgroup of A acts homogeneously on V. In particular, any Abelian normal subgroup acts homogeneously and so is cyclic by Schur's Lemma. By hypothesis, it must be central. There is no harm in assuming that G contains all solvable normal subgroups of A (since that does not affect $b(A/G)$).

We claim that any normal subgroup R of A which is minimal with respect to being non-central is contained in G.

By the first paragraph we may assume that R is not solvable.

So $Z(R) \leq Z(A)$ consists of scalars and $R/Z(R)$ is characteristically simple. So either R is a central product of say t quasisimple groups Q_i (with $Q_i/Z(Q_i)$ all isomorphic) or $R/Z(R)$ is an elementary Abelian r-group for some prime r. In the second case it follows easily that R is of symplectic type with $|R/Z(R)| = r^{2a}$ for some a, however we may exclude this case in the proof of the claim since R must be non-solvable.

So R is perfect. Since G acts irreducibly, $C_A(G) = Z(A)$. In particular, R cannot centralize G. Suppose that R is not contained in G. Then $G \cap R \leq Z(A)$. It follows by the Three Subgroup Lemma [1, Page 26] that $R = [R, R]$ centralizes G, a contradiction.

This proves our claim that every normal subgroup of A which is minimal with respect to being non-central is contained in G.

Let $J_1, \ldots, J_k$ denote the distinct normal subgroups of A that are minimal with respect to being noncentral in A. Let $J = J_1 \cdots J_k$ be the central product of these subgroups. We have shown that $J \leq G$. Then $C_A(J) = Z(A)$ (for otherwise the normal subgroup $C_A(J)$ of A would contain a normal subgroup, say J_1 of A which is minimal with respect to being non-central, then $J_1 \leq Z(J)$ which implies that J_1 is Abelian).

Thus, $A/Z(A)J$ embeds into the direct product of the outer automorphism groups of the normal subgroups of A which are minimal subject to being non-central. If J_i is such a normal subgroup and is perfect with t components, then either $t < 5$ and this outer automorphism group is solvable or $t \geq 5$ and modulo its solvable radical is S_t.

If J_i is of symplectic type with $|J_i/Z(J_i)| = r^{2a}$, then this outer automorphism group has at most one non-solvable composition factor – $\mathrm{PSp}_{2a}(r)$ or $\mathrm{SO}^{\epsilon}_{2a}(2)$.

This gives us our upper bound on $b(A/J)$ and so also on $b(A/G)$. Let W be an irreducible constitutent for J. Since A is primitive on V, it follows that J acts homogeneously on V. It follows by [62, Lemma 5.5.5, page 205 and Lemma 2.10.1, pages 47-48] that $W \cong U_1 \otimes \cdots \otimes U_k$ where U_i is an irreducible J_i-module. In particular, if J_i is the central product of t copies of a non-Abelian simple group, then $\dim U_i \geq 2^t$ and if J_i is of symplectic type with $J_i/Z(J_i)$ of order r^{2a}, then $\dim U_i = r^a$. Moreover, since U_i is absolutely irreducible, $r|(q-1)$.

A straightforward computation shows that $\prod_i b(\mathrm{Out}(J_i)) < (\log n)^{2 \log \log n}$ and this finishes the proof. □

Theorem 5.9. *Let $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$. Set $n = q^d \geq 3$. Assume that G acts irreducibly on V. Then $b(A/G) < (\log n)^{2 \log \log n}$.*

Proof. Consider a counterexample with d minimal. We claim that G acts absolutely irreducibly on V. If not, let $E = \mathrm{End}_G(V)$ and let C be the group of units in the field E. So $|E| = q^e > q$.

There is no harm in replacing G by GC and A by AC and so assume $C \leq G$. Let $A_0 = C_A(C)$. Then A/A_0 is Abelian (since it embeds in the automorphism group of C) and so $b(A/G) = b(A_0/G)$. Also, viewing V as a vector space over E, G (and so A_0) certainly act irreducibly. Since $\dim_E(V) < d$ we obtain a contradiction.

So we assume that G (and so A) acts absolutely irreducibly on V.

Suppose that A preserves a field extension structure on V over $\mathbb{F}_{q^e}$ with $e > 1$. Let $A_0 = A \cap \mathrm{GL}_{d/e}(q^e)$ and $G_0 = G \cap A_0$. Let U denote V considered as a vector space over $\mathbb{F}_{q^e}$ (and as an $\mathbb{F}_{q^e}[A_0]$-module). Then A embeds in $\mathrm{GL}_{d/e}(q^e).e$. Let $W = V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e}$. Now

$$W \cong \oplus_{\sigma \in Gal(\mathbb{F}_{q^e}|\mathbb{F}_q)} U^\sigma$$

as an A_0-module. Then A permutes the U^σ. Moreover, G_0 acts irreducibly on U (or G acts reducibly on W, a contradiction to the fact that V is absolutely irreducible as a G-module). Also, A_0 acts faithfully on U (x trivial on U implies that x is trivial on U^σ for all σ, whence x is trivial on W). Then $b(A/G) = b(A_0/G_0) < (\log n)^{2 \log \log n}$ contradicts the minimality of d (noting that $n = |U|$).

Suppose that A acts imprimitively on V – so $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ and A permutes the V_i. Note that G must permute the V_i transitively as well since G is irreducible. Let K be the subgroup of A fixing each V_i. Let A_i be the action of $N_A(V_i)$ on V_i and define G_i in an analogous way. By Theorem 5.3, we have $b(A/G) \leq b(A/GK) b(A_1/G_1)$. By Theorem 5.10 (see the next section), $b(A/GK) < t^{\log t}$. Now G_1 must act irreducibly on V_1 (otherwise $K \cap G$ and so G would act reducibly on V) and so by minimality, $b(A_1/G_1) < (\log m)^{2 \log \log m}$, where $m = |V_1|$. Note that $n = m^t$. So

$$b(A/G) < t^{\log t} (\log m)^{2 \log \log m}.$$

The desired conclusion follows from Lemma 5.4.

The remaining case is that G is absolutely irreducibly on V, A is primitive on V and preserves no field extension structure on V. Let J be a normal subgroup of A. Then J must act homogeneously on V (by the primitivity hypothesis) and moreover, the irreducible constituents for J must be absolutely irreducible (otherwise the center of $\mathrm{End}_J(V)$ is $\mathbb{F}_{q^e}$ for some $e > 1$ and would be normalized by A, whence A preserves a field extension structure on V). Now the result follows by Theorem 5.8. □

5.4 Normalizers of transitive and primitive groups – Non-Abelian composition factors

We consider the situation $G \lhd A \leq \mathrm{S}_n$. We wish to bound $b(A/G)$ when G is transitive and when G is primitive. It is easy to see that even if one is only interested in the primitive case, one needs an answer in the transitive case as well.

We first consider the case when G is merely transitive. We have already used this result in the previous section.

Theorem 5.10. *Let G and A be nontrivial transitive groups with $G \lhd A \leq \mathrm{S}_n$. Then $b(A/G) < n^{\log n}$.*

Proof. Suppose the theorem is false and consider a counterexample with n minimal. First suppose that A is primitive.

Let $E := F^*(A)$ be the generalized Fitting subgroup of A. By the Aschbacher-O'Nan-Scott theorem, either E is a minimal normal subgroup or $E = E_1 \times E_2$ with $E_1 \cong E_2$ a direct product of t copies of a simple non-Abelian subgroup L of order m.

In the latter case, $n = m^t$, G must contain one of the E_i and by the structure theorem together with Schreier's conjecture, we see that $b(A/G) \leq n(t!)/2 < n^{\log n}$.

In the other cases, G contains E and so we may assume that $G = E$. If E is Abelian, then A/G embeds in $\mathrm{GL}_a(p)$ with $n = p^a$ for an integer a and so $b(A/G) \leq |\mathrm{L}_a(p)| < n^{\log n}$. If E is non-Abelian and is the product of t copies of a non-Abelian simple group L, then either $t \leq 4$ and A/G is solvable or $n \geq 5^t$ and $b(A/G) \leq (t!)/2 < n^{\log n}$.

Suppose that A is not primitive. Let $\{B_1, \ldots, B_t\}$ be an A-invariant partition of the underlying set on which A acts. Let A_i denote the action of the stabilizer of B_i in A on B_i. Then A embeds in $A_i \wr \mathrm{S}_t$ and G permutes transitively the subgroups A_i. Let G_i denote the action of the stabilizer of B_i in G on B_i. We apply Theorem 5.3 and induction to conclude that $b(A/G) \leq t^{\log t} b(A_1/G_1) \leq t^{\log t} s^{\log s}$ where $n = st$. Thus, the result holds. □

The previous and the next theorem imply Theorem 1.11.

Theorem 5.11. *Let G and A be primitive groups with $G \lhd A \leq \mathrm{S}_n$ and $n \geq 3$. Then $b(A/G) < (\log n)^{2 \log \log n}$.*

Proof. We consider the various cases in the Aschbacher-O'Nan-Scott theorem.

In all cases, G contains $E := F^*(A)$. The result follows by Theorem 5.9 if E is Abelian. So we may assume that E is a direct product of t copies of a non-Abelian simple group L of order m. Let K denote the subgroup of A stabilizing all the components of a minimal normal subgroup of A. Clearly K contains E.

Suppose first that $E = E_1 \times E_2$ with $E_1 \cong E_2$ the two minimal normal subgroups of A. In this case $t = 2s$ and $n = |E_1| = m^s$. Then $GK/K \lhd A/K$ are transitive subgroups of S_s and so by Theorem 5.10, $b(A/GK) \leq s^{\log s}$. On the other hand, K/E is solvable (because it is contained in the direct product of copies of the outer automorphism group of L). Thus, $b(A/G) = b(A/GK) \leq s^{\log s} < (\log n)^{\log \log n}$.

In the remaining cases, E is the unique minimal normal subgroup of A, the groups $GK/K \lhd A/K$ are transitive subgroups of S_t and so, as in the previous case, we see that $b(A/G) \leq t^{\log t}$. It follows by the Aschbacher-O'Nan-Scott theorem that $n \geq 5^t$ and so $t^{\log t} < (\log n)^{\log \log n}$. □

5.5 p-solvable composition factors of primitive groups

If G is a finite group, define $a(G)$ to be the product of the orders of all the Abelian (i.e. cyclic) simple composition factors of G in a composition series for G. The bounds we will give in this section for $a(G)$ extend naturally to results about $a_p(G)$ defined to be the product of the orders of all composition factors of G which are either p-groups or p'-groups for a given prime p. Clearly $a(G) \leq a_p(G)$ for any prime p and, by the Odd Order Theorem, $a_2(G) = a(G)$.

It is easy to see that $a_p(G)$ (and $a(G)$) is bounded by the order of some p-solvable (solvable) subgroup $S \leq G$ (e.g., this follows from Theorem 5.15 below). By a theorem of Dixon [12] this implies (see also Dixon-Mortimer [13]) that $a(G)$ is at most $24^{(n-1)/3}$ for any subgroup G of S_n. We state the following more general result.

Proposition 5.12. *Let $G \leq \mathrm{S}_n$. The product of the orders of all composition factors of G which are not isomorphic to alternating groups of degrees larger than $d \geq 4$ is at most $d!^{(n-1)/(d-1)}$. In particular, $a_2(G)$ and $a_3(G)$ are at most $24^{(n-1)/3}$ and $a_p(G) \leq (p-1)!^{(n-1)/(p-2)}$ for $p \geq 5$.*

Proof. The first statement follows from [80, Corollary 1.5] by using the argument implicit in the proof of Theorem 1.13 found in [40]. □

Recall that a subgroup I is *intravariant* in a group G if for all automorphisms α of G, the subgroup I^α is G-conjugate to I.

Lemma 5.13. *Let G be a finite group and let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$ be a normal series with each $G_i \lhd G$. Let $\overline{G_i} = G_{i-1}/G_i$. Let p be a fixed prime. Suppose for each i that I_i is an intravariant p'-subgroup of $\overline{G_i}$. Then G has a p'-subgroup H such that $|H| \geq \prod_{i=1}^r |I_i|$.*

Proof. This is a special case of [106, Theorem 5.3.17]. □

We also need a consequence [72, Lemma 2.9] of the classification theorem of finite simple groups.

Lemma 5.14. *Let G be a non-Abelian finite simple group and p a prime. Then G has a solvable intravariant p'-subgroup I such that $2|\operatorname{Out}(G)|_p \leq |I|$.*

Now we prove a useful reduction result.

Theorem 5.15. *Let G be a finite group and p a prime. Then $a_p(G) \leq |S|$ for some p-solvable subgroup S of G.*

Proof. We may assume that the largest normal p-solvable subgroup of G is trivial.

The socle L of G is a direct product $L = L_1 \times \cdots \times L_t$ of non-Abelian simple groups L_i and G is embedded in $\mathrm{Aut}(L)$. Denote the kernel of the action of G on the set of subgroups L_i by K. Then G/K is a permutation group of degree t and $|G/K|_p \leq 2^t$.

Let $I_1, \ldots, I_t$ be solvable intravariant p'-subgroups of maximal orders in the groups $L_1, \ldots, L_t$. Since K/L is isomorphic to a subgroup of $\prod_{i=1}^{t} \mathrm{Out}(L_i)$, using Lemma 5.14 we see that $|I_1|\,|I_2| \cdots |I_t| \geq 2^t\,|K/L|_p \geq |G/L|_p$.

It is easy to see that the subgroup $I = I_1 I_2 \cdots I_t$ is intravariant in L.

Consider now a normal series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} = L$ such that the groups G_i/L form a chief series of G/L. Every p'-factor G_j/G_{j+1} can be considered as an intravariant p'-subgroup of itself. Applying Lemma 5.13 we see that G has a p'-subgroup S whose order is greater or equal to the product of the orders of these p'-factors and $|G/L|_p$. Therefore we have $|S| \geq a_p(G)$ as required. □

Combining Theorem 5.15 with well-known results of Pálfy [89] and Wolf [115] one obtains sharp bounds for $a(X)$ for irreducible linear groups and primitive permutation groups X. Using Theorem 1.7 we extend these results even further. In the next three results $c_1 = \log_9(48 \cdot 24^{1/3})$ which is close to 2.24399.

Theorem 5.16. *If A is a finite group acting faithfully and completely reducibly on a finite vector space of size n in characteristic p, then $a(A) \leq a_p(A) \leq 24^{-1/3} n^{c_1}$.*

Proof. By Theorem 5.15 we know that there is a p-solvable subgroup S of A such that $a_p(A) \leq |S|$. Moreover, by the construction implicit in the proof of Theorem 5.15, we may assume that $O_p(S) = 1$ (since $O_p(A) = 1$). Thus S can be viewed as a finite group acting faithfully and completely reducibly on a vector space of size n. By [43, Theorem 1.2] we have $|S| \leq 24^{-1/3} n^{c_1}$. □

Corollary 5.17. *Let $1 \neq G \lhd A \leq \mathrm{S}_n$ with A primitive. Let p be a prime dividing n. Then $a(A/G) \leq a_p(A/G) \leq 24^{-1/3} n^{c_1}$.*

Proof. We use the Aschbacher-O'Nan-Scott Theorem. The affine case follows from Theorem 5.16 by noting that $|G|$ may be taken to be n. So assume that $F^*(A)$ is non-Abelian and it is the direct product of t copies of a non-Abelian simple group L. By our choice of p the group L (and thus $F^*(A)$) is not p-solvable.

If $F^*(A)$ is the unique minimal normal subgroup of A, then $n \geq m^t$ for some divisor m of $|L|$ which is at least the minimal degree of a permutation representation for L. In this case $a_p(A) \leq |\,\mathrm{Out}(L)|^t a_p(T)$ where T is a transitive permutation group on t letters. By [3, Lemma 2.7 (i)] we have $|\,\mathrm{Out}(L)| \leq (2/3)m$, and by Proposition 5.12 we have $a_p(T) \leq n$ (since m can be chosen such that $m \geq p$). These give $a_p(A) < (2/3)n^2$. This is less than $24^{-1/3} n^{c_1}$ unless $n \leq 15$ (and thus $t = 1$). If $n \leq 15$, then $a_p(A)$ is at most $|\,\mathrm{Out}(L)| < m = n < 24^{-1/3} n^{c_1}$.

Finally assume that $F^*(A)$ is the direct product of two minimal normal subgroups of A. In this case $n = l^{t/2}$ where $l = |L| \geq 60$. Again by [3, Lemma 2.7 (i)] and Proposition 5.12 we find that $a_p(A) \leq (2/3)n^2 < 24^{-1/3}n^{c_1}$ for $n \geq 60$ (since $l^{1/2} \geq p$). □

This immediately implies the following sharp result (which extends the main result of [89] and [115]).

Corollary 5.18. *If A is a primitive permutation group of degree n and p is a prime divisor of n, then $a(A) \leq a_p(A) \leq 24^{-1/3}n^{1+c_1}$.*

This proves a part of Theorem 1.12.

5.6 Basic results on Abelian composition factors

Our earlier results on non-Abelian composition factors in wreath products do not help in considering Abelian composition factors. We use different methods for studying Abelian composition factors.

The following lemma and its consequences will be crucial in proving Theorem 1.8 on the indices of primitive groups in their normalizers.

If V is a G-module over a field, let $t_G(V)$ denote the smallest number r such that every submodule of V can be generated by r elements.

Lemma 5.19. *Let $H < G$ with $|G : H| = t > 1$. Let W be an H-module over an arbitrary field and let $V = W_H^G$ be the induced module. Then we have the following.*

1) $t_G(V) \leq \frac{1}{2}\dim V$.
2) *If $t \neq 2^n$ for any integer n, then $t_G(V) \leq \frac{1}{3}\dim V$.*
3) *If $H \lhd G$ and $G/H \cong C_2^n$, then $t_G(V) \leq c_n \dim V$ where $c_n = \frac{1}{2^n}\binom{n}{\lfloor n/2 \rfloor}$.*
4) *If $t = 2^n$ for an integer n, then $t_G(V) \leq \frac{3}{8}\dim V$, unless H is normal in G and $G/H \cong C_2$ or C_2^2. Moreover $t_G(V) \leq \frac{5}{16}\dim V$ for $t \geq 32$.*

Proof. First we prove 1) and 2). By extension of scalars, we may assume that the ground field k is algebraically closed. Let p be the largest prime dividing t and let S be a Sylow p-subgroup of G.

Consider the restricted module V_S. By the Mackey decomposition, this is a direct sum of induced modules of the form $(W^g)_{H^g \cap S}^S$ with $g \in G$. Now p divides t, so $H^g \cap S$ is a proper subgroup of S for all $g \in G$. If we manage to show the proposed bounds for $t_S(V_S)$ then we are finished since $t_G(V) \leq t_S(V_S)$. Since t_S is subadditive with respective to a direct sum decomposition of V_S, it is sufficient to bound $t_S((W^g)_{H^g \cap S}^S)$ for a given $g \in G$. But this means that we may assume that $S = G$ and $H^g = H$.

Now let $c \in G$ be an element which does not lie in any conjugate of H and let $C = \langle c \rangle$. Then, as above, $C \cap H^g$ is proper in C for all $g \in G$, so by restricting V to C we may assume that G is a nontrivial cyclic p-group.

We can also assume that W is irreducible. Since H is cyclic, W is 1-dimensional and the induced module V consists of a single Jordan block, thus it can be generated by one element. That is, $t_G(V) = 1 \leq \frac{1}{p} \dim V \leq \frac{1}{2} \dim V$ as required.

Now if $t \neq 2^n$, then $p > 2$ and 2) follows.

Now we turn to the proof of 3) and 4). If $t = 2^n$, then let P be the permutation representation of G on the set of left cosets of H and let T be a Sylow 2-subgroup of G, the image of S in the permutation representation P. Then T is transitive and so the restricted module V_S is simply the induced module $W_{S\cap H}^S$, by the Mackey decomposition.

Instead of V and W, we will consider the restricted modules V_S and $W_{S\cap H}$. If $\mathrm{char}(k) \neq 2$, then V_S is semisimple and $t_G(V) \leq t_S(V) \leq \dim W$ holds. So we can assume that $\mathrm{char}(k) = 2$. Then we can assume that $W_{S\cap H}$ is irreducible, so the action of $S \cap H$ on $W_{S\cap H}$ is trivial, i.e., $W_{S\cap H}$ is the trivial 1-dimensional module. (For this notice that a composition series of $W_{S\cap H}$ corresponds naturally to a series of $\dim W$ submodules of V. For any submodule A of V we can view the intersection of A with the members of the previous series. We obtain the claim after summing dimensions corresponding to factor modules of A and by noticing that c_n can be viewed as a constant.) Then V_S is isomorphic to the regular representation module of C_2^n. Now using [64, 3.2] we see that $t_G(V) \leq t_S(V) \leq c_n \dim V$, as required.

In proving 4), we need the following.

Claim. Let D be the permutational wreath product of a regular elementary Abelian 2-group R and C_2. If g is an element of order 4 in D, then the cycle decomposition of g consists of 4-cycles.

To see this, write g in the form $g = (a, b)\tau$ where (a, b) is an element of the base group $R_1 \times R_2$ (here R_1 and R_2 are naturally identified with R) and τ is the involution in the top group. Then $g^2 = (a, b)\tau(a, b)\tau = (ab, ba)$. Since $g^2 \neq 1$, we see that ab and $ba = (ab)^{-1}$ are both different from the identity, hence they are fixed point free involutions and so is g^2 which implies the claim.

Now we will prove 4).

If T itself is not isomorphic to the regular action of C_2^n, then we prove that $t_S(V) \leq \frac{1}{4} \dim V$ from which 4) follows. We argue by induction. Let B_1, B_2 be a T-invariant partition. Let K be the stabiliser of the partition. Since K has index 2 in T, K acts as a transitive group K_i on B_i so using the inductive hypothesis, we are done unless K_1 (or equivalently, K_2) is isomorphic to the regular action of C_2^{n-1}. Then T embeds into the wreath product $K_1 \wr C_2$. Now T has an element g of order 4, otherwise T would be regular elementary Abelian. By our claim, the cycle decomposition of g consists of 4-cycles. Now using the preimage of g in G we see that $t_G(V) \leq \frac{1}{4} \dim V$.

If T is isomorphic to C_2^n then our claim follows from 3). □

Lemma 5.19 is used in the following result.

Lemma 5.20. *Let $X_1, \ldots, X_t$ be finite groups, X their direct product, and let G be an automorphism group of X which permutes the factors transitively. Let $K \leq X$ be a G-invariant subgroup, such that for each projection π_i of X onto X_i we have $\pi_i(K) \lhd\lhd X_i$. Set $J = [G, K]$ (and note that J is normal in K and G-invariant). Then $a(K/J) \leq (a(X_1))^{t/2}$. If $t \neq 2, 4$ then $a(K/J) \leq (a(X_1))^{3t/8}$ and if $t \geq 17$ then $a(K/J) \leq (a(X_1))^{t/3}$.*

Proof. Let Y_1 be a minimal characteristic subgroup of X_1 and let $Y = Y_1 \times \ldots \times Y_t$ where Y_i are the images of Y_1 under G. Note that

$$a(K/J) = a(K/J(K \cap Y))a((K \cap Y)J/J) = a(KY/JY)a((K \cap Y)/(J \cap Y)).$$

So by induction on the length of a characteristic series in X_1, we might assume that X_i is characteristically simple.

If X_i is elementary Abelian, then X is an induced module and the result follows by Lemma 5.19. Suppose that X_i is a direct product of isomorphic copies of a non-Abelian simple group. Since $\pi_i(K) \lhd\lhd X_i$, the same is true for each $\pi_i(K)$, whence K is also a direct product of copies of a non-Abelian simple group. Since $J \lhd K$, K/J also has the same form, whence $a(K/J) = 1$.

If $t \neq 2, 4$ or $t \geq 17$, the same argument applies (using the stronger conclusions in Lemma 5.19). □

We will use Lemma 5.20 in the above form, however in one case we will need a refined version.

Lemma 5.21. *Use the notations and assumptions of Lemma 5.20. Let $t = 4$ and for each i with $1 \leq i \leq t$ suppose that $X_i = \mathrm{GL}_2(3)$. Then $a(K/J) \leq 16^2 \cdot 3$.*

Proof. In the notation of Lemma 5.19 we have $t_G(V) \leq \frac{1}{2} \dim V$ in general, and $t_G(V) \leq \frac{1}{4} \dim V$ for $t = 4$ and $\mathrm{char}(k) = 3$. Since $|\mathrm{GL}_2(3)| = 16 \cdot 3$, the proof of Lemma 5.20 gives $a(K/J) \leq 16^{t/2} \cdot 3^{t/4} = 16^2 \cdot 3$. □

We will need the following explicit exponential estimate.

Theorem 5.22. *Let $G \lhd A \leq \mathrm{S}_n$ with G transitive. Then $a(A/G) \leq 6^{n/4}$.*

Proof. If A is primitive, then our statement follows from Corollary 5.17 for $n \geq 12$ and from [27] for $n \leq 11$.

If A is not primitive, then choose a non-trivial partition $\{B_1, \dots, B_t\}$ that is A-invariant with $1 < t < n$ maximal. Denote by A_1 the action of the stabilizer of B_1 in A on B_1 and denote by K the stabilizer of the partition in A. Write $n = st$. Then

$$a(A/G) \leq a(A/KG)a(K/G \cap K) \leq a(A/KG)a(K/[G,K]).$$

First suppose that t is different from 2 and 4. Then induction and Lemma 5.20 yield $a(A/G) \leq 6^{t/4} \cdot a(A_1)^{3t/8}$. By Proposition 5.12, $a(A_1) \leq 24^{(s-1)/3}$ and so

$$a(A/G) \leq 6^{t/4} \cdot 24^{(s-1)t/8} < 6^{t/4} \cdot 6^{(s-1)t/4} = 6^{st/4} = 6^{n/4}.$$

Now let $t = 2$ or $t = 4$. Then by [80, Corollary 1.4] we see that $a(A_1) \leq 6^{(s-1)/2}$, unless $s = 4$. This and the previous argument using Lemma 5.20 give the desired conclusion unless the set of prime divisors of $|A|$ is $\{2, 3\}$ and $n = 8$ or $n = 16$. But even in this case [27] gives the result. □

An asymptotically better version of Lemma 5.19 has been obtained by Lucchini, Menegazzo and Morigi [74]. The constant in their result has been evaluated by Tracey [107, Corollary 4.2].

Lemma 5.23. *Let $H < G$ with $|G : H| = t > 1$. Let W be an H-module and let $V = W_H^G$ be the induced module. Then $t_G(V) < 4\frac{t}{\sqrt{\log t}} \dim W$.*

Combining this lemma with other ideas above one can easily prove the following.

Theorem 5.24. *Let G and A be transitive permutation groups of degree $n > 1$ with $G \lhd A$. Then $a(A/G) \leq 4^{n/\sqrt{\log n}}$.*

Proof. We use the bound, the notation and the argument of Theorem 5.22. By the $6^{n/4}$ bound we see that we may assume that $n > 512$. Also, by Corollary 5.17, it is easy to see that we may assume that A is an imprimitive transitive group. Let t and s be as in the proof of Theorem 5.22. By use of Lemma 5.20 and Corollary 5.18, the result follows for $s \geq 32$ as in the proof of Theorem 5.22. If $6 \leq s < 32$, then we obtain the result using the fact that $t > 16$. Finally, if $2 \leq s \leq 5$, then $t > 100$ and the bound follows. □

As pointed out in the Introduction, Theorems 5.24 and 5.10 imply Theorem 1.14.

We will also use various bounds for the orders of outer automorphism groups of simple groups. We state the following from [40] without proof.

Lemma 5.25. *Let S be a non-Abelian finite simple group and suppose that S has a nontrivial permutation representation of degree n. Then $|\operatorname{Out}(S)| \leq 2\log n$ or $S = \mathrm{L}_d(q)$ with $d > 2$ or $S = \mathrm{P}\Omega_8^+(3^e)$ with e an integer, and $|\operatorname{Out}(S)| \leq 3\log n$. In all cases we have $|\operatorname{Out}(S)| \leq 2\sqrt{n}$. Moreover, $|\operatorname{Out}(S)| \leq \sqrt{n}$ unless $S = \mathrm{A}_6$, $\mathrm{L}_2(27)$, $\mathrm{L}_3(4)$ or $\mathrm{L}_3(16)$.*

We remark that Lemma 5.25 may be considered as a sharper version of the observation [3] that if $S \neq \mathrm{A}_6$, then $2|\operatorname{Out}(S)| < n$.

A handy consequence of Lemma 5.25 is that for all non-Abelian finite simple groups S we have $|\operatorname{Out}(S)| \leq \sqrt[4]{|S|}$ unless $S = \mathrm{L}_3(4)$. This follows from the known fact that the minimal degree of a permutation representation of S is less than $\sqrt{|S|}$, when $|\operatorname{Out}(S)| \leq \sqrt{n}$, and directly in the remaining cases.

We end this section with a result about dimensions versus outer automorphism groups for simple groups.

Lemma 5.26. *Let S be a non-Abelian simple section of $\mathrm{SL}_n(p)$ where p is a prime. Then $|\operatorname{Out}(S)| \leq 4n$.*

Proof. For sporadic and alternating groups the result is obvious.

Suppose that S is a group in $\mathrm{Lie}(p')$ over $\mathbb{F}_r$ of (untwisted) rank ℓ. By [72, Lemma 3.1] in this case we have $n \geq \min\{R_p(S), r^\ell\}$ where $R_p(S)$ is the minimal degree of a projective representation of S in characteristic p. Using the lower bounds of Landazuri and Seitz for $R_p(S)$ (slightly corrected in [62, Table 5.3A]) and [62, Table 5.1A], where values of $|\operatorname{Out}(S)|$ are given, the result follows by easy inspection.

Suppose now that S is a group in $\mathrm{Lie}(p)$. If the order of S is divisible by a primitive prime divisor of $p^m - 1$ then clearly $n \geq m$ holds. A list of the largest such numbers m is given in [62, Table 5.2C]. Using this we see that in all cases $4m \geq |\operatorname{Out}(S)|$ holds. This completes the proof. □

5.7 Normalizers of primitive groups – Abelian composition factors

We consider the situation $G \lhd A \leq \mathrm{S}_n$, G primitive and want to bound $a(A/G)$. We first consider the case when the socle of G is Abelian. To deal with this case, we need the following result on primitive linear groups.

Theorem 5.27. *Let V be a finite vector space of order $n = p^b$ defined over a field of prime order p. Let B be a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ which acts primitively (and irreducibly) on V. Let F be a maximal field such that B embeds in $\Gamma L_F(V)$. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Then one of the following holds.*

1. *$d = 1$ and $a(B) \leq (n-1)f \leq (n-1)\log n$; or*
2. *$d > 1$ and $a(B) < n$ for $n > 3^{16}$.*

Furthermore $a(B) < n^2/6^{1/2}$ unless $n = 9$ and $B = \mathrm{GL}_2(3)$.

Proof. Every normal subgroup of a primitive linear subgroup of $\mathrm{GL}(V)$ acts homogeneously on V. In particular, any Abelian subgroup normalized by B acts homogeneously

and so is cyclic by Schur's Lemma. Let C be the subgroup of nonzero elements in F (viewing F as a subring of $\mathrm{End}(V)$). Note that C is normalized by B and, for $d = 1$, contains the centralizer of B. We may replace B by BC and so assume that $C \leq B$.

Let $E = \mathrm{End}_B(V)$ with $q = |E|$. The algebra generated by C is F and $|F| = q^e$ for some integer e.

Let B_0 be the centralizer of C in B. Note that C is the center of B_0. We claim that B_0 acts irreducibly on V considered as a vector space over F. For let U denote V as a B_0-module over F. Then $V' := V \otimes_E F \cong \oplus U^\sigma$, where the sum is over the elements of $\mathrm{Gal}(F \mid E)$. Since B acts absolutely irreducibly on V (over E), B acts irreducibly on V'. Note that B/B_0 acts regularly on the set $\{U^\sigma\}$ and so B_0 must act irreducibly on each U^σ and so, in particular, on U as claimed.

Note that $a(B) = a(B_0)e$ for B/B_0 is cyclic of order e.

Let R be a normal subgroup of B contained in B_0 minimal with respect to not being contained in C. If none exists, then $B_0 = C$, $d = 1$ and B' is cyclic and the first conclusion allowed holds. So assume that this is not the case. Let W be an irreducible $F[R]$-submodule of V, which, as an $F[R]$-module, is a direct sum of copies of W. Let $F' = \mathrm{End}_R(W)$.

We claim that $F' = F$. The center of the centralizer of R in $\mathrm{GL}(V)$ is the group of units of F'. This is normalized by B and so by the choice of C must just be C, whence $F = F'$. Let d_R denote $\dim_F W$.

Notice that R cannot be Abelian. For if R is Abelian, then so is RC. But then RC is cyclic by Schur's Lemma and so $RC = C$ by our choice of C. This is a contradiction since we chose R not to be contained in C. (By this same argument we also see that every characteristic Abelian subgroup of B_0 is central and contained in C.)

So there are two possibilities for R.

1. R is of symplectic type with $R/Z(R)$ of order r^{2a} for some prime r and integer a. Since $Z(R) \leq C$, it follows that $r|q^e - 1$ and $d_R = r^a$. By [75, Lemma 1.7] in this case $R/Z(R)$ is a completely reducible $\mathbb{F}_r B_0$-module under conjugation.

2. R is the central product of t isomorphic quasisimple groups $Q_i, 1 \leq i \leq t$. Since R acts homogeneously on V and since $F' = F$, it follows that W is of the form $W_1 \otimes \cdots \otimes W_t$ where W_i is absolutely irreducible over F (and the tensor product is taken over F). Thus $d_R = (\dim_F W_1)^t$.

Choose a maximal collection of non-cyclic subgroups described above which pairwise commute. Denote these by $J_1, \ldots, J_m$. Let $J = J_1 \cdots J_m$ be the central product of these subgroups.

We next claim that $C_{B_0}(J) = C$. Suppose not. By the maximality condition, any B-normal subgroup of $C_{B_0}(J)$ minimal with respect to not being contained in C is one of the J_i. However, J_i is non-Abelian and so is not contained in $C_{B_0}(J)$.

In particular B_0/C embeds in the direct product of the automorphism groups of the $J_i/Z(J_i)$. Since J is the central product of the J_i, J acts homogeneously and F is a splitting field for the irreducible constituents for each J_i, it follows that $d = \dim_F V \geq \prod d_i$ where $d_i = d_{J_i}$.

Thus, $a(B) \leq f(p^f - 1) \prod e_i$, where the e_i are defined as follows.

If J_i is of symplectic type with $J_i/Z(J_i)$ of order $r_i^{2\ a_i}$, then if B_i denotes the (completely reducible) action of B_0 on $J_i/Z(J_i)$, we have $a(B_i) \leq (r_i^{2a_i})^{2.25}$ by Theorem 5.16. In this case we set $e_i = r_i^{6.5a_i}$.

If $J_i/Z(J_i) = L_1 \times \cdots \times L_t \neq 1$ for non-Abelian simple groups L_i, then if S_i denotes the action of B_0 permuting the L_j, we have $a(S_i) \leq 24^{(t-1)/3}$ by Proposition 5.12. In this case we set $e_i = |\operatorname{Out}(L_1)|^t 24^{(t-1)/3}$. Using Lemma 5.26 we see that

$$e_i \leq 4^t\ d_{J_i} \cdot f^t \cdot 24^{(t-1)/3} \leq (d_{J_i})^{4.53} f^{[\log d_{J_i}]}.$$

Altogether we see that $a(B) \leq p^f \cdot f^{1+[\log d]} \cdot d^{6.5}$. On the other hand $n = p^{fd}$.

From this, by a tedious calculation, it follows that $a(B) < n$ whenever $n \geq 2^{40}$ (for $d > 1$). With more calculations it is possible to show that $a(B) < n$ whenever $n > 3^{16}$ and $d > 1$.

Finally, consider the last statement of the theorem. By similar calculations as before, it follows that $a(B) < n^2/6^{1/2}$ whenever $n \geq 2^{16}$ (even if $d = 1$). So assume that $n < 2^{16}$ and also that $d > 1$.

If $p^f = 2$ then no J_i is a group of symplectic type and so a closer look at our previous estimates yields $a(B) < n^2/6^{1/2}$ and $a(B) < n$ (if $d > 1$).

Let $p^f = 3$. Then $d \leq 10$, a J_i can be a group of symplectic type, but, in this case, we must have $r_i = 2$. Using this observation, a simple calculation gives $a(B) < n^2/6^{1/2}$ whenever $n > 81$.

Let $p^f = 4$. Then $d \leq 7$, a J_i can be a group of symplectic type, but, in this case, we must have $r_i = 3$ and $a_i = 1$. Using the fact that $|\mathrm{Sp}_2(3)| = 24$, the exponent 6.5 in the above estimate can be improved in this special case and we get $a(B) < n^2/6^{1/2}$ whenever $n > 64$. The same bound holds even in case $d = 1$ and $n > 64$.

Let $p^f \geq 5$. Here $d \leq 6$ and a very similar argument yields the desired bound.

Thus we only need to check the last statement of the theorem for $n \leq 81$. This was done by GAP [27]. □

Theorem 5.28. *Let $G \lhd A \leq \mathrm{GL}(V)$ with $|V| = p^f = n$. Assume that G acts irreducibly on V. Then either A is metacyclic and $|A/G| < n$ or $a(A/G) < n$ for $n > 3^{16}$.*

Proof. Consider a counterexample with n minimal.

If A acts primitively on V, then, by Theorem 5.27, either $a(A) < n$, or A' is cyclic, A embeds in $\Gamma\mathrm{L}_1(p^f)$ and $|A| = a(A) < nf$.

Consider the latter case. Since G acts irreducibly on V over the prime field, it follows that $|G| \geq f$ (a group of order less than f will not have an irreducible module of dimension f). Thus $|A/G| < n$.

So we may assume that A acts imprimitively.

So $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ and A permutes the V_i. Note that since G is irreducible, G must permute the V_i transitively as well. We may assume that this is done in such a way that V_1 has minimal dimension over $\mathbb{F}_p$. Set $m = |V_1|$. Since $t > 1$ and since A is irreducible on V, we have $m > 2$.

Let K be the subgroup of A fixing each V_i. Let A_i be the image of $N_A(V_i)$ acting on V_i and define G_i similarly. Since V_1 is minimal, it follows that A_1 acts primitively on V_1.

Now $a(A/G) \leq a(A/GK)a(K/(G \cap K)$. By Theorem 5.22, $a(A/GK) \leq 6^{t/4}$. By Lemma 5.20 and Theorem 5.27, $a(K/(G \cap K) \leq a(A_1)^{t/2} < (m^2/6^{1/2})^{t/2}$ unless m is 9 and $A_1 = \mathrm{GL}_2(3)$. Thus, if $m \neq 9$, we have $a(A/G) < 6^{t/4}(m^2/6^{1/2})^{t/2} = n$.

Assume now that $m = 9$ and $A_1 = \mathrm{GL}_2(3)$.

By the restriction $n > 3^{16}$, we have $t \neq 2, 4$. Then Lemma 5.20 implies that $a(K/(G \cap K)) \leq a(A_1)^{3t/8} = 48^{3t/8}$. Hence $a(A/G) \leq \left(6^{1/4}48^{3/8}\right)^t < m^t = n$. □

Theorem 5.29. *Let G and A be primitive permutation groups of degree n with $G \lhd A$. Then $a(A/G) < n$ for $n > 3^{16}$.*

Proof. We consider the various cases in the Aschbacher-O'Nan-Scott Theorem.

In all cases, G contains $E := F^*(A)$. The result follows by Theorem 5.28 if E is Abelian. So we may assume that E is a direct product of t copies of a non-Abelian simple group L of order l. Let K denote the subgroup of A stabilizing all the components.

Suppose first that $E = E_1 \times E_2$ with $E_1 \cong E_2$ the two minimal normal subgroups of A. In this case $t = 2s$ for some integer s and $n = |E_1| = l^s$. Then the groups $GK/K \lhd A/K$ can be considered as transitive subgroups of S_s and so by Theorem 5.22, $a(A/GK) \leq 6^{s/4}$. By Lemma 5.20, $a(GK/G) = a(K/G \cap K) \leq |\operatorname{Out}(L)|^s$. Hence $a(A/G) \leq n^{1/4} \cdot 6^{s/4}$ unless $L = \mathrm{L}_3(4)$ by a remark after Lemma 5.25. This is certainly less than n since $l \geq 60$. The same follows for $L = \mathrm{L}_3(4)$ by direct computation.

In the remaining cases, E is the unique minimal normal subgroup of A, the groups $GK/K \lhd A/K$ are transitive subgroups of S_t and so as in the previous case, we see that $a(A/GK) \leq 6^{t/4}$. Here $n \geq m^t$ where m is at least the minimal degree of a nontrivial permutation representation of L. By Lemmas 5.20 and 5.25 it follows that $a(GK/G) \leq |\operatorname{Out}(L)|^{t/2} \leq (2\sqrt{m})^{t/2}$. Hence $a(A/G) \leq n^{1/4} \cdot 2^{t/2} \cdot 6^{t/4}$ which is less than n if $m \geq 5$. □

5.8 Normalizers of primitive groups – Sizes

We continue to consider the situation $G \lhd A \leq \mathrm{S}_n$, G primitive and want to bound $|A/G|$. We first consider the case when the socle of G is Abelian. To deal with this case, we need the following result on primitive linear groups.

Theorem 5.30. *Let V be a finite vector space of order $n = p^b$ defined over a field of prime order p. Let A be a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ which acts primitively (and irreducibly) on V. Let F be a maximal field such that A embeds in $\Gamma\mathrm{L}_F(V)$. Let G be a normal subgroup of A which acts irreducibly on V. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Then $a(A)b(A/G) < f \cdot p^f \cdot d^{2\log d+3}$.*

Proof. We use the description of the structure of A found in the proof of Theorem 5.27 (where this group was denoted by B). By the fourth paragraph of the proof of Theorem 5.8 we see that G contains every non-solvable normal subgroup of A which is minimal with respect to being non-central. From this the result easily follows. □

We note here that, with little modification and in case $J \neq 1$, the proof of Theorem 5.8 essentially bounds $|A|/(b(G)|J|) = (a(A)b(A/G))/|J|$, where J is the product of all *solvable* normal subgroups of A (satisfying the conditions of Theorem 5.8) which are minimal with respect to being non-central. We also note that $(\log n)^{2\log\log n}$ is close to $d^{2\log d}$. However the argument in Theorem 5.27 is to be used together with Lemma 5.26 but excluding Theorem 5.16.

We continue with a simple lemma.

Lemma 5.31. *Let us use the notations and assumptions of the statement of Theorem 5.30. Put $A_0 = A \cap \mathrm{GL}_F(V)$. Suppose that A has a unique normal subgroup J contained in A_0 which is minimal subject to being not contained in the multiplicative group C of F viewed as a subset of $\mathrm{End}(V)$. If $|A/G| \geq n$, then $J \leq G$.*

Proof. Let the multiplicative group of the field $K = \mathrm{End}_G(V)$ be L.

We may assume that G is not cyclic. Indeed, otherwise $|A| < |L| \cdot |G| < n \cdot |G|$ since A acts on G by conjugation with kernel contained in L.

By the facts that G is not cyclic and a Singer cycle is self centralizing, we must have $df \geq 2$ and $|K| \leq p^{df/r}$ where r is the smallest prime factor of df.

We may also assume that G is metacyclic. Indeed, $G_0 = G \cap A_0$ is normal in A, is contained in A_0, thus it may be assumed that $G_0 \leq C$ is cyclic and thus G is metacyclic.

By considering the action of A_0 on G, we see that $|A_0| \leq |L| \cdot |G|$ since the kernel of the action is $L \cap A_0$, $G_0 \leq Z(A_0)$, and G/G_0 is cyclic. From this we have $|A/G| \leq f \cdot |L| < f \cdot p^{df/r} \leq p^{df} = n$. □

We next present two useful bounds for $|A/G|$ in terms of n.

Lemma 5.32. *Let n, A and G be as in Theorem 5.30. Then we have the following.*

1. *$|A/G| < n$ for $n > 3^{16}$;*
2. *$a(A)b(A/G) < n^2/6^{1/2}$ unless $n = 9$ and $A = \mathrm{GL}_2(3)$.*

Proof. In case A/G is solvable, this follows from Theorems 5.28 and 5.27. Thus we may assume that A/G is not solvable. An easy computation using Theorem 5.30 shows that $|A/G| < n$ for $n \geq 2^{136}$ and $a(A)b(A/G) < n^2/6^{1/2}$ for $n \geq 2^{34}$. It is easy to see by the structure of a primitive linear group (see Theorem 5.27), that if $p^f = 2$ (where p and f are as in Theorem 5.30) and A/G is not solvable, then $n \geq 2^{243}$. Thus we may also assume that $p^f \geq 3$ (and $d \geq 4$, where d is as in Theorem 5.30).

Now straightforward calculations using Theorem 5.30 give $|A/G| < n$ for $n \geq 3^{54}$ and $a(A)b(A/G) < n^2/6^{1/2}$ for $n \geq 3^{14}$.

Let us adopt the notations and assumptions of the proof of Theorem 5.27 (with B replaced by A and B_0 replaced by A_0).

Assume that $p^f = 3$. Then we may assume that $16 < d \leq 53$ and $d \leq 13$ in the respective cases. A J_i can be a group of symplectic type, but, in this case, we must have $r_i = 2$. As in Example 5.7 the normalizer N_i in $\mathrm{GL}_{2^{a_i}}(3)$ of such a J_i satisfies $N_i/(J_iZ) \cong \mathrm{O}^{\epsilon}_{2a_i}(2)$ where Z is the group of scalars. (This is because $|Z(J_i)|$ must be 2 since it divides $p^f - 1$.) A straightforward computation using the structure of A (and G) gives the result.

We only comment on the bound (1) in case $n = 3^{32}$ and when the product J of all normal subgroups of A contained in A_0 which are not contained in the multiplicative group, C of F viewed as a subset of $\mathrm{End}(V)$, is solvable. When J is itself a normal subgroup of A contained in A_0 which is minimal subject to being not contained in C (a unique such), then $J \leq G$, by Lemma 5.31, and so we find that $|A/G| < n$. Otherwise, if J is a product of more than one J_i, then $|A| < n$ by the fact that the index of a proper subgroup in $\mathrm{O}^{\epsilon}_{10}(2)$, apart from the simple subgroup $\mathrm{SO}^{\epsilon}_{10}(2)$ whose index is 2, is at least 495.

Assume that $p^f = 4$. Then $13 \leq d \leq 42$ and $d \leq 11$ in the respective cases. A J_i can be a group of symplectic type, but, in this case, we must have $r_i = 3$. We are assuming that A/G is not solvable. As a result, for (2), only the case $d = 9$ has to be checked. The bound in (1) is slightly more complicated to establish (but true).

To finish the proof of (2) we may assume that $p^f \geq 5$. Then $4 \leq d \leq 9$. Using this information and Theorem 5.30 we see that $a(A)b(A/G) < f \cdot p^f \cdot d^{2\log d+3} < n^2/6^{1/2}$. Thus from now on we only consider (1).

Let $p^f = 5$. Then we may assume that $11 \leq d \leq 36$. In fact, by use of Theorem 5.30 we may assume that $d \leq 29$. With a computation similar to the ones above it is possible to deduce (1) in this special case.

We only comment on the case $n = 5^{16}$ and when the product J of all normal subgroups

of A contained in A_0 which are minimal subject to being not contained in C is solvable. When J is itself a normal subgroup of A contained in A_0 which is minimal subject to being not contained in C (a unique such), then $J \leq G$, by Lemma 5.31, and so we find that $|A/G| < n$. Otherwise, if J is a product of more than one J_i, then $|A| < n$ by the fact that the subgroups $\mathrm{Sp}_6(2) \times \mathrm{Sp}_2(2)$ and $\mathrm{Sp}_4(2) \times \mathrm{Sp}_4(2)$ of $\mathrm{Sp}_8(2)$ are relatively small.

Let $p^f = 7$. We may assume that $10 \leq d \leq 17$ (by use of Theorem 5.30). A straightforward computation gives the result.

Similarly, if $p^f = 8$, 9 or 11, then we may assume that d satisfies $9 \leq d \leq 16$, $9 \leq d \leq 15$ or $8 \leq d \leq 11$ in the respective cases. Straightforward computations give the result.

Let $p^f = 13$. We may assume that $d = 7$, 8 or 9. A straightforward computation gives the result except when $d = 8$ and A does not contain a non-solvable normal subgroup which is minimal subject to being not contained in C. In this latter case we may proceed as in the case $n = 5^{16}$ described above.

Let $p^f = 16$. We may assume that $d = 7$ or $d = 8$. In this case there is nothing to do since we are assuming that A/G is non-solvable.

Let $p^f = 17$. We may assume that $d = 7$ and so there is nothing to do.

Let $p^f = 19$. We may assume that $d = 6$. However there is nothing to do since A/G is non-solvable.

By $p^f \geq 23$ and Theorem 5.30, we have $d = 4$ or $d = 5$. Both these cases can easily be handled using the assumption that $n > 3^{16}$.

This finishes the proof of the lemma. □

We next state without proof the following result from [40].

Theorem 5.33. *Let $G \lhd A \leq \mathrm{S}_n$. If G is transitive, then $|A : G| \leq 168^{(n-1)/7}$.*

Theorem 5.33 is used in the proof of the following result.

Theorem 5.34. *Let $G \lhd A \leq \mathrm{GL}(V)$ with $|V| = p^d = n$. Assume that G acts irreducibly on V. Then $|A/G| < n$ for $n > 3^{16}$.*

Proof. By Lemma 5.32 we may assume that A acts imprimitively on V. By Theorem 5.28 we may also assume that A/G is not solvable.

We may proceed almost as in the relevant paragraph of Theorem 5.9. We may decompose V in the form $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ maximal such that A permutes the V_i. Note that G must permute the V_i transitively as well since G is irreducible. Let K be the subgroup of A fixing each V_i. Let A_i be the action of $N_A(V_i)$ on V_i and define G_i similarly.

Now G_1 must act irreducibly on V_1 and so by Theorem 5.30 we have the inequality $a(A_1)b(A_1/G_1) < f_1 \cdot p^{f_1} \cdot d_1^{2\log d_1+3}$, where $m = |V_1| = p^{f_1 d_1}$ for certain integers f_1 and d_1. Note that $n = m^t$.

By Theorem 5.3, we have

$$|A/G| = a(A/G)b(A/G) \leq a(A/GK)b(A/GK) \cdot a(K/(G \cap K))b(A_1/G_1).$$

We have $b(A/GK) < t^{\log t}$ by Theorem 5.10. We also have $a(A/GK) \leq 6^{t/4}$ by Theorem 5.22. Thus Lemma 5.20, Theorem 5.27, and Theorem 5.9 give

$$|A/G| \leq 6^{t/4} \cdot t^{\log t} \cdot a(A_1)^{t/2} \cdot b(A_1/G_1) < 6^{t/4} \cdot t^{\log t} \cdot (m^2/6^{1/2})^{t/2} \cdot (\log m)^{2\log\log m},$$

provided that $m \neq 9$. However we can improve this bound by use of the inequality

$$a(A_1)^{t/2} b(A_1/G_1) \leq f(m)^{t/2} (a(A_1)b(A_1/G_1))/f(m),$$

where $f(m)$ is any upper bound for $a(A_1)$. For example if $m \neq 9$ then we get

$$|A/G| < 6^{t/4} \cdot t^{\log t} \cdot (m^2/6^{1/2})^{t/2} \cdot (a(A_1)b(A_1/G_1))/(m^2/6^{1/2}).$$

First it will be convenient to deal with the case when $t = 2$ or $t = 4$. Then $m \neq 9$. Since $b(A/GK) = 1$, the previous inequality shows that we are done unless $b(A_1/G_1) \neq 1$. On the other hand, if $b(A_1/G_1) \neq 1$, then Lemma 5.32 gives

$$a(A_1)b(A_1/G_1) < m^2/6^{1/2},$$

provided that $m \neq 9$.

Now let t be different from 2 and 4 but at most 16.

Assume first that $m \neq 4$. By Lemma 5.20 and Theorem 5.33,

$$|A/G| < 168^{(t-1)/7} \cdot (m^{8/3}/168^{8/21})^{3t/8} \cdot (a(A_1)b(A_1/G_1))/(m^{8/3}/168^{8/21}) <$$

$$< m^t \cdot (a(A_1)b(A_1/G_1))/(m^{8/3}/168^{8/21}) \cdot 168^{-1/7}$$

(since $m^{8/3}/168^{8/21} > m^2/6^{1/2} > a(A_1)$ for $m \geq 5$ (and m different from 9), and $m^{8/3}/168^{8/21} > a(A_1)$ for $m = 3$ and $m = 9$). Again, we are finished if $b(A_1/G_1) = 1$. Assume that $b(A_1/G_1) \neq 1$. If $m = 81$ then we can use GAP [27] to arrive to a conclusion. Otherwise it is easy to see that $m \geq 625$. Since $d_1 \geq 4$, we certainly have

$$a(A_1)b(A_1/G_1) < f_1 \cdot p^{f_1} \cdot d_1^{2\log d_1+3} < m^{8/3}/168^{8/21}$$

for $m \geq 625$, unless possibly if $p^f = 2$ or $p^f = 3$. If $p^f = 2$, then $d_1 \geq 3^5$, by the structure of A_1, and so the previous inequality holds. We also have the previous inequality in case $p^f = 3$ since we may assume by the structure of A_1 that $d_1 \geq 8$.

If $m = 4$ then Lemma 5.20 and Theorem 5.33 give us $|A/G| \leq 168^{(t-1)/7} \cdot 6^{3t/8}$. This is not necessarily less than 4^t, however it is for $t \leq 16$.

Now let $t \geq 17$.

By Lemma 5.20 and Theorem 5.33,

$$|A/G| < 168^{(t-1)/7} \cdot (m^3/168^{3/7})^{t/3} \cdot (a(A_1)b(A_1/G_1))/(m^3/168^{3/7}) <$$

$$< m^t \cdot (a(A_1)b(A_1/G_1))/(m^3/168^{3/7}) \cdot 168^{-1/7}$$

(since $m^3/168^{3/7} > m^2/6^{1/2}$ when $m \geq 4$, and $m^3/168^{3/7} > a(A_1)$ for $m = 3$ and $m = 9$). We may assume that $b(A_1/G_1) \neq 1$. Then $m = 81$ or $m \geq 625$ by the structure of A_1. If $m = 81$ then we have $a(A_1)b(A_1/G_1) < m^3/168^{3/7}$ by use of GAP [27]. If $m \geq 625$ then we arrive to a conclusion by use of three paragraphs up, noting that $m^{8/3}/168^{8/21} < m^3/168^{3/7}$ for $m \geq 3$. □

Theorem 5.35. *Let G and A be permutation groups with $G \lhd A \leq \mathrm{S}_n$. Suppose that G is primitive and $|A/G| \geq n$. Then A and G are affine primitive permutation groups and $n \leq 3^{16}$.*

Proof. If A is an affine primitive permutation group then the result follows from Theorem 5.34. Otherwise we may mimic the proof of Theorem 5.29 by noting that we must replace $6^{s/4}$ by $168^{s/7}$ and $6^{t/4}$ by $168^{t/7}$ in the respective cases (due to Schreier's conjecture and Theorem 5.33). □

5.9 Small linear groups

In this section we will finish the proof of the first half of Theorem 1.8.

Let G and A be permutation groups with $G \lhd A \leq \mathrm{S}_n$. Suppose that G is primitive and $|A/G| \geq n$. We must show that the pair $(n, A/G)$ is one of the eleven exceptions in Theorem 1.8.

By Theorem 5.35 it is sufficient to consider affine primitive permutation groups of degrees at most 3^{16}.

Let V be a finite vector space of size n with $n \leq 3^{16}$. Opposed to the notation of the statement of the theorem, let G and A be groups such that $G \lhd A \leq \mathrm{GL}(V)$. Assume that G (and thus A) acts irreducibly on V. We must classify all possibilities for which $|A/G| \geq n$.

Let us first assume that A acts primitively on V. We use the notations and assumptions of Theorem 5.27 and its proof (with B replaced by A and B_0 replaced by A_0). We put $n = p^b$ for a prime p and integer b with the property that A is a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ acting primitively (and irreducibly) on V. Let F be a maximal field

such that A embeds in $\Gamma L_F(V)$. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Let the multiplicative group of F, viewed as a subset of $\mathrm{End}(V)$, be denoted by C.

If $d = 1$ then Theorem 5.28 gives $|A/G| < n$. Thus assume that $d > 1$.

As in the proof of Theorem 5.27, let J be the product of all normal subgroups of A contained in A_0 which are minimal subject to not being contained in C.

Assume that d is a prime. Then, by the proof of Theorem 5.27, J itself is a normal subgroup of A contained in A_0 which is minimal subject to not being contained in C. Moreover J is either a quasisimple group or is a group of symplectic type with $|J/Z(J)| = d^2$. In both of these cases we must have $J \leq G$, by Lemma 5.31.

Assume that J is a quasisimple group. By Lemma 5.26 (and the proof of Theorem 5.27), we have $|A/G| \leq 4(p^f - 1)df^2$. This is less than p^{df} for $d \geq 5$. Assume that $d = 2$. If A_5 is a factor group of J, then $|A/G| \leq 2f(p^f - 1) < p^{2f}$. Otherwise, by Dickson's theorem on subgroups of $\mathrm{GL}_2(p^f)$, we have $|A/G| \leq 2f^2(p^f - 1) < p^{2f}$ if p is odd, and $|A/G| \leq f^2(p^f - 1) < p^{2f}$ if $p = 2$. Now assume that $d = 3$. Then, by information from [62], we find that $|A/G| \leq 6f^2(p^f - 1)$. This is smaller than p^{3f} unless $p = f = 2$. If $d = 3$ and $p = f = 2$, then, by [27], we get the desired estimate $|A/G| \leq 4f(p^f - 1) = 24 < 64 = n$.

Let J be a group of symplectic type with $|J/Z(J)| = d^2$ where d is a prime. Then $|A/G| \leq |\mathrm{Sp}_2(d)|f(p^f - 1) < d^3 f(p^f - 1) < n$ for $d \geq 5$, and also for $d = 3$ and $p^f > 4$. If $d = 3$ and $p^f = 4$, then $|A/G| \leq d^3 f = 54 < 64$. Let $d = 2$. It is then easy to see that $|A/G| \leq 6f((p^f - 1)/2) < p^{2f}$ since $p > 2$.

From now on we assume that d is not a prime and larger than 1.

In this paragraph let $p^f = 2$. By the structure of A described in the proof of Theorem 5.27 we know that all normal subgroups of A contained in A_0 and minimal with respect to being not contained in C are non-solvable. Moreover J has at most two non-Abelian simple composition factors, since $d \leq 25$. By this, we immediately see, as in the proof of Theorem 5.27, that $|A/G| \leq 32d$. This is less than 2^d unless $d \leq 8$. If $d = 6$ or 8, then $|A/G| \leq 4d < 2^d$. For $d = 4$ the result follows by [27].

From now on we assume that $p^f > 2$.

In this paragraph we deal with the cases when $d = 6$, 10, 14, or 15. In these cases d is a product of two primes r_1 and r_2. First suppose that J is not solvable. If A has no solvable normal subgroup contained in A_0 which is minimal with respect to being noncentral, then it is easy to see that $|A/G| \leq f(p^f - 1) \cdot 4^2 f^2 d < p^{fd}$ since $p^f > 2$. Otherwise we get $|A/G| \leq f^2(p^f - 1) \cdot 4{r_1} \cdot {r_2}^5$ (for a certain choice of r_1 and r_2). This is always less than p^{df} unless $d = 6$ and $p^f = 3$ or 4. If $d = 6$ and $p^f = 3$, then in the previous bound we must have $r_2 = 2$ and thus $|A/G| < n$. If $d = 6$ and $p^f = 4$, then we must have $r_1 = 2$ and $r_2 = 3$. In this special case we can modify our bound to $|A/G| \leq f(p^f - 1) \cdot 2 \cdot 3^5 = 12 \cdot 3^5 < 4^6 = n$. Thus we may assume that J is solvable. In this case d divides $p^f - 1$, and since $n \leq 3^{16}$, we are left to consider only the case $d = 6$

and $p^f = 7$ or 13 when $|A| < n$.

We are left to consider the cases when $d = 4$, 8, 9, 12, or 16.

Let $d = 4$.

First assume that J is solvable and it is the unique normal subgroup of A contained in A_0 which is minimal subject to being not contained in C. By Lemma 5.31 we may assume that $J \leq G$. For $p^f \geq 7$ we can bound $|A/G|$ by $f((q^f-1)/2)|\mathrm{Sp}_4(2)| = 360f(q^f-1) < p^{4f}$. We are left to consider the cases when $p^f = 3$ and $p^f = 5$. If $p^f = 3$, $d = 4$ and $|A/G| \geq 81$, then $(n, A/G) = (3^4, \mathrm{O}_4^-(2))$, while if $p^f = 5$, $d = 4$ and $|A/G| \geq 625$, then $(n, A/G) = (5^4, \mathrm{Sp}_4(2))$. Now assume that J is solvable and it is the product of two normal subgroups, say J_1 and J_2 of A contained in A_0 which are minimal subject to being not contained in C. If $f = 1$ then G contains one (if not both) of these normal subgroups, say J_1. Furthermore, since J_1 is not irreducible on V, the irreducible group G properly contains J_1. Thus $|A/G| \leq 4 \cdot 36 \cdot ((p^f-1)/2) \cdot (1/2) = 36(p-1) < p^4$. We may now assume that $f \geq 2$ (and also that p is odd). In this case we only use the fact that $|G| \geq 4$ to conclude that $|A/G| \leq f(p^f-1)16 \cdot 36 \cdot (1/4) = 144f(p^f-1)$. We already know from the same paragraph that this is less than p^{4f} for $p^f \geq 9$.

Secondly assume that A has no solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. In this case J has at most two non-Abelian composition factors and so $|A/G| \leq f^3(p^f-1) \cdot 4^3 \cdot 2 = 128f^3(p^f-1)$, by the second half of the proof of Theorem 5.27. From this we get $|A/G| < p^{4f}$ unless possibly if $p^f = 3$, 4, 8, 9 or 16. When J has a unique non-Abelian composition factor, then we may sharpen our bound to $|A/G| \leq 16f^2(p^f-1)$, and this is smaller than p^{4f} for the remaining five values of p^f. Thus J has exactly two non-Abelian composition factors. In this case we can apply Dickson's theorem on subgroups of $\mathrm{GL}_2(p^f)$ to refine our bound on $|A/G|$ even further. This is $8f^3(p^f-1)$ which is smaller than p^{4f} for the remaining five values of p^f.

Thirdly there are two normal subgroups of A contained in A_0 which are minimal subject to not being contained in C. One is J_1, a symplectic 2-group, and one is J_2, a quasisimple group. In this case we have $|A/G| \leq f(p^f-1) \cdot 2f \cdot 24 = 48f^2(p^f-1)$. This is less than p^{4f} where $p > 2$, unless $p^f = 3$. But $p^f = 3$ cannot occur in this case since $J_2 \leq \mathrm{GL}_2(3)$ is solvable.

From now on let d be 8, 9, 12 or 16.

In this paragraph suppose that A has no solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. In this case the number, say r of non-Abelian composition factors of J is at most 4. If $r = 4$ then $d = 16$ and so $p^f = 3$. In this case it is easy to see that $|A/G| \leq 98304f^5(p^f-1) < 3^{16}$. Let $r = 3$. Then $d = 8$ or $d \geq 12$. In the first case we can use Dickson's theorem to conclude that a quasisimple subgroup Q of $\mathrm{GL}_2(p^f)$ satisfies $|\mathrm{Out}(S/Z(S))| \leq 2f$. This implies that $|A/G| \leq 48f^4(p^f-1) < p^{8f}$. In case $d \geq 12$ we can use our usual bound $|A/G| \leq f^4(p^f-1) \cdot 4^3 \cdot 16 \cdot 6 = 6144f^4(p^f-1) < p^{12f}$. Finally let $r \leq 2$. Then

$|A/G| \leq 512f^3(p^f-1)$. This is less than p^{fd} for $d \geq 8$ (and $p^f > 2$).

In the remaining cases A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. This implies that the greatest common divisor of d and p^f-1 is larger than 1. This, the above, and the fact that $n \leq 3^{16}$ imply that the only cases to deal with are the following: $d = 8$ and $p^f = 3$, 5, 7, 9; $d = 9$ and $p^f = 4$, 7; $d = 12$ and $p^f = 3$, 4; and $d = 16$ and $p^f = 3$.

Let $d = 8$. We may assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. First suppose that J is not solvable. Then J has one or two non-Abelian composition factors. Such a composition factor can be considered as a subgroup of $\mathrm{L}_2(p^f)$ or of $\mathrm{L}_4(p^f)$. In the first case we must have $p^f \geq 5$. Suppose J has exactly one non-Abelian composition factor. If this is a subgroup of $\mathrm{L}_2(p^f)$, then, by Dickson's theorem, we have the estimate $|A/G| \leq f(p^f-1)\cdot 2f\cdot|\mathrm{Sp}_4(2)|\cdot 2^4 < p^{8f}$ for $p^f \geq 5$. If this is considered as a subgroups of $\mathrm{L}_4(p^f)$, then $|A/G| \leq f(p^f-1)\cdot 16f\cdot|\mathrm{Sp}_2(2)|\cdot 4 < p^{8f}$. Finally, if J has exactly two non-Abelian composition factors, then these must be subgroups of $\mathrm{L}_2(p^f)$, and we have $|A/G| \leq f(p^f-1)\cdot(2f)^2\cdot 2\cdot|\mathrm{Sp}_2(2)|\cdot 4 < p^{8f}$ for $p^f \geq 5$. Thus we may assume that J is solvable. First assume that $p^f = 9$. If A has more than one normal subgroup contained in A_0 which is minimal subject to not being contained in C, then $|A| \leq 2\cdot 8\cdot|\mathrm{Sp}_4(2)||\mathrm{Sp}_2(2)|\cdot 2^6 < 9^8$. Otherwise we may assume that $J \leq G$, by Lemma 5.31, and so $|A/G| \leq 2\cdot 8\cdot|\mathrm{Sp}_6(2)| < 9^8$. We may now assume that $p^f = 3$, 5, or 7. In all of these cases $A_0 = A$. First suppose that A has more than one normal subgroup which is minimal subject to not being contained in C. If $p^f \neq 3$, then $|A/G| \leq 16\cdot 3\cdot|\mathrm{Sp}_4(2)||\mathrm{Sp}_2(2)| < p^{8f}$. Let $p^f = 3$. If $|G| \geq 16$, then $|A/G| \leq 8\cdot|\mathrm{O}_4^-(2)||\mathrm{O}_2^-(2)| < 3^8$. Otherwise $|G\cap J| = 8$ and in fact $|G| = 8$. But such a group G cannot act irreducibly on V. We conclude that J is the unique normal subgroup of A which is minimal subject to not being contained in C. Thus $J \leq G$. If $p^f = 7$, then $|A/G| \leq |\mathrm{O}_6^-(2)| < 7^8$. Let $p^f = 5$. Assume that A is the full normalizer of J in $\mathrm{GL}(V)$. If $G = J$, then $(n, A/G) = (5^8, \mathrm{Sp}_6(2))$. Otherwise, since $A/J \cong \mathrm{Sp}_6(2)$ is simple, $G = A$. Thus we may assume that A/J is a proper subgroup of $\mathrm{Sp}_6(2)$. By [13, pp. 319], we have $|A/G| \leq |A/J| \leq |\mathrm{Sp}_6(2)|/28 < 5^8$. We remain with the case $p^f = 3$. If $G = J$ and $J \leq A$ has index at most 2 in the full normalizer of J in $\mathrm{GL}(V)$, then $|A/G| > n$ and $(n, A/G) = (3^8, \mathrm{O}_6^-(2))$, $(3^8, \mathrm{SO}_6^-(2))$, $(3^8, \mathrm{O}_6^+(2))$ or $(3^8, \mathrm{SO}_6^+(2))$. Suppose now that $J \leq A$ has index larger than 2 in the full normalizer of J in $\mathrm{GL}(V)$. Since $\mathrm{SO}_6^+(2) \cong \mathrm{A}_8$ and $\mathrm{SO}_6^-(2) \cong \mathrm{U}_4(2)$ are simple groups with minimal index of a proper subgroup 8 and 27 respectively (for the latter see [13, pp. 317]), we immediately get $|A/G| \leq |A/J| < 3^8$ in the remaining cases.

Let $d = 9$. We may assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. If J is non-solvable, then, by the structure of A (and G), $|A/G| \leq f(p^f-1)\cdot 4\cdot 3f\cdot 3^2\cdot|\mathrm{Sp}_2(3)| < p^{9f}$. Thus J is solvable. If $p^f = 7$ then an easy computation yields $|A| \leq 6\cdot 81\cdot|\mathrm{Sp}_4(3)| < 7^9$. We assume that $p^f = 4$. Now J is the product of one or two normal subgroups of A not contained in C. If one, then we may assume by Lemma 5.31 that $J \leq G$. In this case we get $|A/G| \leq 2\cdot|\mathrm{Sp}_4(3)| < 4^9$. In the other case we get $|A| \leq 6\cdot 81\cdot|\mathrm{Sp}_2(3)|^2$. Since

$|G| > 2$, we see that $|A/G| < 4^9$.

Let $d = 12$. We may again assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. We may also assume that J is not solvable since p^f is 3 or 4. If J has one non-Abelian composition factor, then $|A/G| \leq f(p^f - 1) \cdot 4 \cdot 6f \cdot 16 \cdot |\mathrm{O}_4^-(2)| = f^2(p^f - 1) \cdot 46080 < p^{12f}$ for both $p^f = 3$ and $p^f = 4$. Finally, if J has two non-Abelian composition factors, then $|A/G| \leq f(p^f - 1) \cdot 4^2 \cdot 4 \cdot f^2 \cdot 2 \cdot 9 \cdot |\mathrm{Sp}_2(3)| = f^3(p^f - 1) \cdot 27648 < p^{12f}$ for both $p^f = 3$ and $p^f = 4$.

Let $d = 16$. Then $p^f = 3$ and $A_0 = A$. From the above we may assume that A has a solvable normal subgroup which is minimal subject to not being contained in C. Assume first that J is not solvable. Since $\mathrm{GL}_2(3)$ is solvable and 3 does not divide 16, we know that J has a unique non-Abelian composition factor and this can be considered as a subgroup of $\mathrm{L}_4(3)$. From this we arrive to a conclusion by $|A/G| \leq f(p^f - 1) \cdot 4 \cdot (4f) \cdot |\mathrm{O}_4^-(2)| \cdot 2^4 < 3^{16}$. Thus we may assume that J is solvable. First assume that A contains more than one normal subgroup which is minimal subject to not being contained in C. In this case $|A/G|$ is at most $2^6 \cdot |\mathrm{O}_6^-(2)||\mathrm{O}_2^-(2)| < 3^{16}$. Thus we may assume that J is the unique normal subgroup of A which is minimal subject to not being contained in C. This implies that $J \leq G$. If $G = J$ and $J \leq A$ has index at most 2 in the full normalizer of J in $\mathrm{GL}(V)$, then $|A/G| > n$ and $(n, A/G)$ is $(3^{16}, \mathrm{O}_8^-(2))$, $(3^{16}, \mathrm{SO}_8^-(2))$, $(3^{16}, \mathrm{O}_8^+(2))$ or $(3^{16}, \mathrm{SO}_8^+(2))$. Now $\mathrm{SO}_8^\epsilon(2)$ are simple groups with the property that every proper subgroup has index at least 119 (see [13, pp. 319–320]). This implies that if $J \leq A$ has index larger than 2 in the full normalizer of J in $\mathrm{GL}(V)$, then $|A/G| \leq |A/J| < 3^{16}$.

We may now assume that A acts imprimitively on V. By the proofs of Theorems 5.28 and 5.34 we see that we may assume, in the notations of these proofs, that $m = 9$ and $t = 2$ or $t = 4$. In these cases $n = 3^4$ or $n = 3^8$. If $n = 3^4$, then [27] gives $|A/G| < n$. So assume that the second case holds. The group A is clearly solvable and so by Lemmas 5.21 and 5.22 we have $|A/G| \leq 6 \cdot 16^2 \cdot 3$. This is less than 3^8.

This completes the proof of the first half of Theorem 1.8.

5.10 Normalizers and outer automorphism groups of primitive groups

In this section we prove Theorem 1.9.

Let G be a primitive permutation group of degree n. Assume first that the generalized Fitting subgroup $E = F^*(G)$ of G is non-Abelian. Now $\mathrm{Aut}(G)$ has a natural embedding into $\mathrm{Aut}(E)$ and it acts transitively on the components of E (this is also true if G has two minimal normal subgroups). The bound follows as in the proof of the bound for $|A/G|$.

So suppose that $F^*(G) = V$ is Abelian. If V is central, then n is a prime, G is cyclic

and $\mathrm{Out}(G)$ is cyclic of order $n-1$. So assume that $Z(G) = 1$. In this case the centralizer of G in S_n is 1.

Lemma 5.36. *Let G be a primitive affine permutation group of degree n and H a point stabilizer. Let $V = F(G) = F^*(G)$. Then $|\mathrm{Aut}(G) : N_{\mathrm{S}_n}(G)| = |H^1(H, V)|$.*

Proof. Let N be the normalizer of G in S_n, then N embeds into $A = \mathrm{Aut}(G)$. Moreover an element $\varphi \in A$ is in N exactly when the image of a point stabilizer H of G under φ is also a point stabilizer [13, 4.2B].

It is easy to see that A acts transitively on the complements of V hence it acts transitively on the G-conjugacy classes of such complements. It follows that $|A : N|$ equals the number of G-conjugacy classes of complements, that is, $\left|H^1(H, V)\right|$. □

In particular, if $H^1(H, V) = 0$, our previous estimates apply. So now we consider the case with $H^1(H, V) \neq 0$. So $G = VH$ with H acting faithfully and irreducibly on V. We first point out the following result in [2, 2.7 (c)]. See also [33].

Lemma 5.37. *Suppose that H is a finite group acting irreducibly and faithfully on V with $H^1(H, V) \neq 0$. Then H has a unique minimal normal subgroup N of the form $L_1 \times \cdots \times L_t$ with $L_i \cong L$ a non-Abelian simple group. Set $L_{i'} = C_N(L_i)$ (the product of all the other L_j). Moreover, $V = \oplus_i V_i$ where $V_i = [L_i, V] = C_V(L_{i'})$ and $|H^1(H, V)| \leq |H^1(L_1, W)|$, where W is any nontrivial irreducible L_i-submodule of V_1.*

Now we obtain bounds on the size of outer automorphism groups for such groups.

First an example. Let $q = 2^e, e > 1$ and $H = \mathrm{L}_2(q)$. Let V be the natural module for H (i.e. 2-dimensional over F_q). Consider $G = V.\mathrm{L}_2(q)$ acting on V. Then G is primitive and $|\mathrm{Out}(G)| = |H^1(H, V)||N_{\mathrm{S}_n}(G) : G| = q(q-1)e < (n \log n)/2$ but $|\mathrm{Out}(G)| > n$ and indeed has order roughly $(n \log n)/2$. We now show that this is the only example with $|\mathrm{Out}(G)| \geq n$, completing the proof of Theorem 1.9..

Theorem 5.38. *Let G be a primitive affine permutation group of degree n. Let $V = F(G) = F^*(G)$ and $H \neq 1$ a point stabilizer. Assume that $H^1(H, V) \neq 0$. Then either $|\mathrm{Out}(G)| < n$ or $n = q^2$ with $q = 2^e, e > 1$ and $H = \mathrm{L}_2(q)$.*

Proof. We use the lemma above and write $V = \oplus V_i$ where $V_i = [L_i, V]$. Let N be the normalizer of L_1. Then N preserves V_1 and indeed N is precisely the stabilizer of V_1. Since H is irreducible on V, N is irreducible on V_1. Let $E = \mathrm{End}_H(V)$. So E is a field of size q. By Frobenius reciprocity, $E \cong \mathrm{End}_N(V_1)$. Let $d = \dim_E V_1$ and $h_1 = |H^1(H, V)|$.

So $H^1(H, V)$ embeds in $H^1(L_1, U_1)$ where U_1 is an L_1-submodule of V_1. Now we know that $|\mathrm{Out}(G)| \leq (q-1)h_1|N_J(H)/H|$ where $J = \mathrm{Aut}(L) \wr \mathrm{S}_t$.

Suppose that $t = 1$. Then $F^*(H) = L$ and $|\mathrm{Out}(G)| \leq (q-1)h_1|\mathrm{Out}(L)|$. We first consider some special cases.

If $d = 2$, then (since we are assuming that $h_1 > 1$), $h_1 = q$. This implies (see [35]) that $L = \mathrm{L}_2(q)$ with $q = 2^e > 2$. Moreover, the equality on h_1 implies that $H = L$ and we are as in the example above.

Suppose that $d = 3$. Then also by the main result in [35], it follows that $h_1 = q$. So $|\operatorname{Out}(G)| < q(q-1)\sqrt{(q^3-1)/(q-1)} < q^3$ unless possibly $L = \mathrm{A}_6$, $\mathrm{L}_2(27)$, $\mathrm{L}_3(4)$ or $\mathrm{L}_3(16)$ (see Lemma 5.25). In these exceptional cases $|\operatorname{Out}(L)|$ has order $4, 6, 12$ or 24 respectively and the result holds unless possibly $q < |\operatorname{Out}(L)|$. This easily rules out the first two cases (there are no 3-dimensional representations over a field of size $q < |\operatorname{Out}(L)|$ cf. [59]). For the latter two groups, there are no 3-dimensional representations (only projective representations).

So assume that $d \geq 4$.

Suppose that $|H^1(H, V)| < |V|^{1/2}$. Since (by construction), V is an irreducible $\mathbb{F}_q[H]$-module, $|H^1(H, V)| \leq q^{(d/2)-1}$ if d is even and $|H^1(H, V)| \leq q^{(d-1)/2}$ if d is odd.

In this case, the same argument as above applies. We only need to deal with the four groups as above and only for representations where $|\operatorname{Out}(L)| > \sqrt{(q^d-1)/(q-1)}$. From [59] we see that the only possibility is that $L = \mathrm{A}_6$ and $q = 2$, $d = 4$. In that case, $|H^1(H, V)| \leq 2$ and we still have the result.

The remaining case is when $|H^1(H, V)| = |V|^{1/2}$. This can only occur for $d = 2$ except if $H = \mathrm{A}_6$, $q = 3$ and $d = 4$ [35]. So $n = 81$. In that case, we see that $|\operatorname{Out}(G)| \leq 9 \cdot 2 \cdot 4 = 72$ and the result still holds.

Now suppose that $t > 1$ and $n = q^{dt}$ where $d = \dim_E V_1$. Then we have $|N_J(H)/H| \leq |\operatorname{Out}(L)|^{t/2} b_t$ where b_t is the analogous bound for transitive groups of degree t. Thus by [35], $|\operatorname{Out}(G)| \leq (q-1)q^{d/2}|\operatorname{Out}(L)|^{t/2} b_t$. By Theorem 5.10 and Theorem 5.22, we have $b_t \leq 2^t \cdot t^{\log t}$ and it is easy to see that if $t \leq 7$ then in fact $b_t \leq 2^t$ holds. Unless $L = \mathrm{A}_6$ (which we assume) we have $|\operatorname{Out}(L)| < q^d/(2(q-1))$ by [3, Lemma 2.7].

Assuming first that $q \neq 2$ we see that $|\operatorname{Out}(G)| < q^{d((t/2)+1)} t^{\log t}$. It is also clear that (since $\mathrm{L}_2(3)$ is solvable) in this case we have $q^d \geq 16$ and $|\operatorname{Out}(G)| < q^{dt}$ follows for $t \geq 8$ (and even for $t \leq 7$ by the observation a few lines above).

Finally let $q = 2$. Then we see that $|\operatorname{Out}(G)| \leq 2^{(d+t+dt)/2} \cdot t^{\log t}$. If $d \geq 4$ and $t \geq 8$, then this is less than 2^{dt}. Otherwise $L = \mathrm{L}_3(2)$ and in this case for $t \geq 8$ we have $|\operatorname{Out}(G)| \leq 2 \cdot 2^{t/2} \cdot 2^t \cdot t^{\log t} < 2^{3t}$. If $t \leq 7$, then $|\operatorname{Out}(G)| < 2^{dt}$ follows, using $b_t \leq 2^t$ and Lemma 5.25, in all cases, except when $L = \mathrm{A}_6 = \mathrm{L}_2(9)$. Finally, if $L = \mathrm{A}_6 = \mathrm{L}_2(9)$, then $d \geq 6$ and $|\operatorname{Out}(G)| < 2^{dt}$ follows easily. □

5.11 p-solvable composition factors and outer automorphism groups

The purpose of this section is to complete the proof of Theorem 1.12.

Fix a prime p. Throughout this section we put c to be $24^{1/3}$ if $p \leq 3$ and $(p-1)!^{1/(p-2)}$ if $p \geq 5$.

The first result concerns transitive permutation groups.

Theorem 5.39. *Let $G \lhd A \leq \mathrm{S}_n$ be transitive permutation groups of degree n. Let p be a prime. Then $a_p(G)|A/G| \leq c^{n-1}$.*

Proof. We prove the result by induction on n.

First let A be a primitive permutation group. If A contains A_n, then the bound is clear. Otherwise we have $|A| \leq 24^{(n-1)/3}$ by [80].

Now let A be an imprimitive permutation group. Let $\{B_1, \ldots, B_t\}$ be an A-invariant partition of the underlying set on which A acts, with $1 < t < n$. Let A_1 denote the action of the stabilizer of B_i in A on B_i. Then A embeds in $A_i \wr \mathrm{S}_t$ and G permutes transitively the subgroups A_i. Let G_i denote the action of the stabilizer of B_i in G on B_i. By Theorem 5.3 we have $b(A/G) \leq b(A/GK)b(A_1/G_1)$ where K denotes the kernel of the action of A on $\{B_1, \ldots, B_t\}$.

In order to bound $a_p(G)$ we first set $s = |B_1|$, that is $n = st$. We have

$$a_p(G) = a_p(G/K \cap G) \cdot a_p(K \cap G) \leq a_p(GK/K) \cdot a_p(K \cap G).$$

Let N be the kernel of the action of K on B_1. We have

$$a_p(K \cap G) \cdot a(K/(K \cap G)) \leq a_p((K \cap G)N) \cdot a(K/(K \cap G)N) =$$

$$= a_p((K \cap G)N/N) \cdot a_p(N) \cdot a(K/(K \cap G)N) \leq a_p(G_1) \cdot a(A_1/G_1) \cdot a_p(N).$$

We are now in position to bound $a_p(G) \cdot |A/G| = a_p(G) \cdot a(A/G) \cdot b(A/G)$. We have

$$a_p(G) \cdot |A/G| \leq a_p(GK/K) \cdot |A/GK| \cdot a_p(K \cap G) \cdot a(K/(K \cap G)) \cdot b(A_1/G_1) \leq$$

$$\leq (a_p(GK/K) \cdot |A/GK|) \cdot (a_p(G_1) \cdot |A_1/G_1|) \cdot a_p(N).$$

By induction (noting that GK/K and G_1 are transitive on $\{B_1, \ldots, B_t\}$ and B_1 respectively), we have $a_p(GK/K) \cdot |A/GK| \leq c^{t-1}$ and $a_p(G_1) \cdot |A_1/G_1| \leq c^{s-1}$. Moreover by repeated use of Proposition 5.12, we see that $a_p(N) \leq c^{(s-1)(t-1)}$. These give $a_p(G)|A/G| \leq c^{t-1}c^{s-1}c^{(s-1)(t-1)} = c^{n-1}$. □

We next need a lemma which depends on the existence of regular orbits under certain coprime actions.

Lemma 5.40. *Let A be a primitive linear subgroup of $\Gamma\mathrm{L}_d(p^f)$ for a prime p and integers f and d with d as small as possible. Put $A_0 = \mathrm{GL}_d(p^f) \cap A$. Let J_0 be the product of all normal subgroups of A contained in A_0 which are nonsolvable, have orders coprime to p, and are minimal with respect to being noncentral in A_0. Then either $p^f = 7$, $d = 4$ or 5, and $b(J_0) = |\mathrm{PSp}_4(3)|$, or $b(J_0) < p^{fd}$.*

Proof. The group J_0 is a central product of quasisimple groups $J_1, \ldots, J_r$ for some r. Since $J_0 \lhd A$ and A is primitive, J_0 acts homogeneously on the underlying vector space. Let W be an irreducible J_0-submodule. As in the proof of Theorem 5.8, we may use [62, Lemma 5.5.5, page 205 and Lemma 2.10.1, pages 47-48] to write W in the form $W_1 \otimes \cdots \otimes W_r$ where for each i the J_i-module W_i (defined over a possibly larger field) is irreducible.

Assume first that $r = 1$. If J_0 has a regular orbit on W, then the result is clear. If J_0 does not have a regular orbit on W, then [100, Theorem 7.2.a] says that (J_0, W) is a permutation pair in the sense of [100, Example 5.1.a] or (J_0, W) is listed in the table on [100, Page 112]. In all these exceptional cases we have $|J_0/Z(J_0)| < |W|$ unless W is a 4 or 5 dimensional module over the field of size 7 and $J_0/Z(J_0) \cong \mathrm{PSp}_4(3)$. Moreover $|J_0/Z(J_0)| < p^{fd}$ or $|W| = p^{fd}$ and one of the previous exceptional cases holds.

Assume that $r > 1$. For each i we have $b(J_i) < |W_i|$ or $|W_i| = 7^4$ or 7^5 and $b(J_i) < |W_i|^{1.31}$. From these it follows that $b(J_0) < |W| \leq p^{fd}$. □

The next lemma may be viewed as a sharper version of Theorem 5.16 under the assumption that $p \geq 7$.

Lemma 5.41. *Let G be a finite group acting faithfully and completely reducibly on a finite vector space V in characteristic p. Then $a_p(G) \leq |V|^{c_1}/c$.*

Proof. By Theorem 5.16, we may assume that $p \geq 5$. By [43, Theorem 1.1], the strong base size of a p-solvable finite group S acting completely reducibly and faithfully on a vector space of size n over a field of characteristic $p \geq 5$ is at most 2. Thus $|S| < n^2/(p-1)$. By the proof of Theorem 5.16 we then have $a_p(G) \leq |V|^2/(p-1) \leq |V|^{c_1}/c$. □

Theorem 5.39 is used in the proof of the following result which could be compared with Theorem 5.16.

Theorem 5.42. *Let $G \lhd A \leq \mathrm{GL}(V)$ be linear groups acting irreducibly on a finite vector space V of size n and characteristic p. Then $a_p(G)|A/G| \leq 24^{-1/3} n^{c_1}$.*

Proof. We prove the result by induction on n.

Assume that A acts primitively on V. If $a_p(G) = a(G)$, then the result follows from part (2) of Lemma 5.32. In fact, in our argument to show Theorem 1.8 we naturally took G to be as small as possible and our calculations actually gave $|A/(G \cap Z(A)J)| < n$ apart from the eleven exceptions listed in Theorem 1.8 (when $a_p(G) = a(G)$). Here, as usual, J denotes the central product of all normal subgroups of A contained in A_0 (where $A_0 = \mathrm{GL}_d(p^f) \cap A$ and d is smallest with $A \leq \Gamma\mathrm{L}_d(p^f)$ and $n = p^f$) subject to being noncentral. Thus we are finished if the product of the orders of the non-Abelian composition factors of J which are p'-groups is at most $24^{-1/3} n^{c_1 - 1}$. Let J_0 be as in Lemma 5.40. By Lemma 5.40 we have $b(J_0) \leq 24^{-1/3} n^{c_1 - 1}$ unless $n \leq 81$ or $p^f = 7$ and $d = 4$ or 5. It can be checked by GAP [27] that the bound holds in case $n \leq 81$.

Thus assume that $p^f = 7$ and $d = 4$ or 5 with $|b(J_0)| = |\mathrm{PSp}_4(3)|$. Then A is a $7'$-group by [100, Theorem 7.2.a] and so $a_7(G)|A/G| = |A| \leq 24^{-1/3}n^{c_1}$ by [43, Theorem 1.2].

Assume that A acts (irreducibly and) imprimitively on V. Let $V = V_1 \oplus \cdots \oplus V_t$ be a direct sum decomposition of the vector space V such that $1 < t$ and A (and so G) acts transitively on the set $\{V_1, \ldots V_t\}$. Set $m = |V_1|$. Let K be the kernel of the action of A on $\{V_1, \ldots V_t\}$ and let A_1 and G_1 be the action of $N_A(V_1)$ and $N_G(V_1)$ on V_1 respectively. As in the proof of Theorem 5.39, we have

$$a_p(G) \cdot |A/G| \leq (a_p(GK/K) \cdot |A/GK|) \cdot (a_p(G_1) \cdot |A_1/G_1|) \cdot a_p(N),$$

where, in this case, N denotes the kernel of the action of K on V_1. Since the groups $GK/K \lhd A/K$ can be viewed as transitive permutation groups acting on t points, Theorem 5.39 gives $a_p(GK/K)|A/GK| \leq c^{t-1}$. In the proof of Theorem 5.9 it was noted that G_1 must act irreducibly on V_1. Thus, by the induction hypothesis, $a_p(G_1)|A_1/G_1| \leq 24^{-1/3}m^{c_1}$. Since N is subnormal in the irreducible group A, it must be completely reducible. By repeated use of Lemma 5.41 we have $a_p(N) \leq m^{c_1(t-1)}/c^{t-1}$. Applying these three estimates to the displayed inequality above, we get $a_p(G) \cdot |A/G| \leq c^{t-1} \cdot (24^{-1/3}m^{c_1}) \cdot (m^{c_1(t-1)}/c^{t-1}) = 24^{-1/3}n^{c_1}$. □

We are now in the position to complete the proof of Theorem 1.12 in the special case that G is an affine primitive permutation group.

Theorem 5.43. *Let G be an affine primitive permutation group of degree n, a power of a prime p. Then $a_p(G)|\mathrm{Out}(G)| \leq 24^{-1/3}n^{1+c_1}$.*

Proof. Let H be a point stabilizer in G. We may assume that $H \neq 1$. Clearly H acts irreducibly and faithfully on a vector space V of size n. If $H^1(H, V) = \{0\}$, then Theorem 5.42 gives the result, by Lemma 5.36. So assume that $H^1(H, V) \neq \{0\}$. By Lemma 5.37, $F^*(H) = L_1 \times \cdots \times L_t$ where $L_i \cong L$ are non-Abelian simple groups viewed as subgroups of $\mathrm{GL}(V_i)$ where the V_i are vector spaces with $V = \oplus_{i=1}^t V_i$. For each i put $|V_i| = p^d$ for a prime p and integer d. (See Lemma 5.37 and the proof of Theorem 5.38.)

If $n = q^2$ with $q = 2^e$ for an integer $e > 1$ and $H = \mathrm{L}_2(q)$, then, by Section 5.10, $a_2(G)|\mathrm{Out}(G)| < (n^2 \log n)/2 < 24^{-1/3}n^{1+c_1}$. Thus, by Theorem 5.38, we may assume that $|\mathrm{Out}(G)| < n$.

Assume first that L is not p-solvable. By Lemma 5.26 and Proposition 5.12, we have the estimate $a_p(H) \leq (4d)^t c^{t-1}$ where c is as in the beginning of this section, depending on p. For $d = 2$ and $p \geq 5$, $d = 3$ and $p \geq 3$, or $d = 4$ and $p \geq 3$, or $d \geq 5$ we have $(4d)^t c^{t-1} \leq 24^{-1/3}p^{dt(c_1-1)}$ giving the desired bound for $a_p(H)$ and thus for $a_p(G)|\mathrm{Out}(G)|$ in these cases. The only exceptions are $d = 3$ and $p = 2$, and $d = 4$ and $p = 2$. However in these cases in the previous two estimates we may replace $4d$, we obtained from Lemma 5.26, by 1 and 4 respectively. Thus we may assume that L is p-solvable (and $p \geq 3$).

Let A be the full normalizer of G in S_n. Assume that $p \geq 5$ and that A/G is not p-solvable. By Schreier's conjecture and the proof of Theorem 5.10 we must then have $t \geq 8$. By the proof of Lemma 5.41 we have $a_p(A) \leq n^3/4$. Thus, by the main result of [35], Lemma 5.37 and Theorem 5.10, we have the estimate $a_p(G)|\operatorname{Out}(G)| \leq (n^3/4) \cdot t^{\log t} \cdot p^{d/2}$. Furthermore, by the proof of Theorem 5.38, we may also assume that $d \geq 3$ as well as $t \geq 8$. Under these conditions it easily follows that $(n^3/4) \cdot t^{\log t} \cdot p^{d/2} < 24^{-1/3} n^{1+c_1}$. Assume now that $p \geq 5$ and A/G is p-solvable. Then we must bound $a_p(A)|H^1(H,V)| \leq (n^3/4) \cdot p^{d/2}$. Using Lemma 5.26 this is smaller than the desired estimate unless $t \leq 2$. Using Lemma 5.40 we can deduce the result if $t \leq 2$ and $d \geq 4$. By the proof of Theorem 5.38 we cannot have $d = 2$ since $H^1(H,V) \neq \{0\}$ and $p \neq 2$. Thus $t \leq 2$ and $d = 3$. We then have by the proof of Lemma 5.41 that $a_p(A)|H^1(H,V)| \leq (n^3/(p-1)) \cdot p$ which is, for $n \geq 343$, less than $24^{-1/3} n^{1+c_1}$. This forces $p = 5$, $d = 3$ and $t = 1$ with $|L|$ not divisible by 5. GAP [27] shows that there is no such possibility.

We are left to consider the case when $p = 3$ and L is 3-solvable, that is, a Suzuki group. In this case $F^*(H)$ has a regular orbit on V by [100, Theorem 7.2.a]. We also have $1 < |H^1(H,V)| \leq n^{1/14}$ by [52, Table 2] and so we may assume by Lemma 5.37 that $d \geq 14$. By these, Proposition 5.12 and a remark after Lemma 5.25, $a_3(A)|H^1(H,V)| < n^3 < 24^{-1/3} n^{1+c_1}$ for $n \geq 3^{14}$. We may thus assume that $a_3(G)|\operatorname{Out}(G)| > a_3(A)|H^1(H,V)|$. Then $t \geq 8$ as in the previous paragraph and so $a_3(G)|\operatorname{Out}(G)| < n^3 \cdot t^{\log t} \cdot p^{d/14} < 24^{-1/3} n^{1+c_1}$ whenever $n \geq 3^{8 \cdot 14}$. □

Finally we finish the proof of Theorem 1.12. By Theorem 5.43 we may assume that G is a primitive permutation group of degree n with non-Abelian socle E which is isomorphic to a direct product of t copies of a non-Abelian simple group L. By Theorem 1.9 we know that $|\operatorname{Out}(G)| < n$ in this case and so it is sufficient to show $a_p(G) \leq 24^{-1/3} n^{c_1}$ for every prime divisor p of n. This follows from the proof of Corollary 5.17.

5.12 Asymptotics

In this section the second half of Theorem 1.8 and Theorem 1.10 are proved.

Let G be a primitive permutation group of degree n and let A be the full normalizer of G in S_n. Assume that A is not an (affine) subgroup of $\mathrm{A\Gamma L}_1(q)$ for a prime power q equal to n. We will show that for $n \geq 2^{14000}$ we have $|A/G| < n^{1/2} \log n$.

Assume first that A is an affine primitive permutation group. Then so is G. In fact we may change notation and assume that A and G are linear groups acting irreducibly on a finite vector space V of size n with $G \lhd A$. First assume that A acts primitively on V. Let us use the notation of Theorem 5.30. By assumption, we have $d \geq 2$. If $d = 2$ then, by the structure of A, we have that $|A/G|$ is at most $(3/2)(\sqrt{n} - 1) \log_3 n < n^{1/2} \log n$ if A is solvable and $|A/G| < n^{1/2} \log n$ if A is nonsolvable (using Dickson's theorem). If

$d \geq 3$, then, by Theorem 5.30,

$$|A/G| < n^{1/3} \cdot (\log n) \cdot d^{2\log d+3} \leq n^{1/3}(\log n)^{2\log\log n+4} < n^{1/2}$$

for $n \geq 2^{8192}$.

Assume now that A acts imprimitively on V and that it preserves a direct sum decomposition $V_1 \oplus \cdots \oplus V_t$ of V where $t > 1$ is as large as possible. Let K denote the kernel of the (transitive) action of A on $\{V_1, \ldots, V_t\}$. As in the proof of Theorem 5.28, let A_1 be the action of $N_A(V_1)$ on V_1. The group A_1 acts primitively and irreducibly on V_1. By Theorem 5.27, we have $a(A_1) < m \log m$ for $m = |V_1| > 3^{16}$. In the notation of Lemma 5.20 for $t \geq 2^{729}$ we have $a(K/J) \leq (a(X_1))^{t/3c_1}$, by use of Lemma 5.23, where c_1 is as in Theorem 1.12. From this and by the proof of Theorem 5.28 together with part (2) of Lemma 5.32 and Theorem 1.14, for $t \geq 2^{729}$ we get

$$|A/G| \leq |A/GK| \cdot (a(A_1)b(A_1/G_1))^{t/3c_1} \leq 16^{t/\sqrt{\log t}} \cdot n^{1/3} < n^{1/2}.$$

Otherwise, if t is bounded (is at most 2^{729}) but $t \neq 2$, 4, then, again by the proof of Theorem 5.28 and by Lemma 5.20 and Theorems 1.14 and 5.9, we have, for $n \geq 2^{8192}$,

$$|A/G| \leq |A/GK| \cdot b(A_1/G_1) \cdot (a(A_1))^{3t/8} \leq 16^{t/\sqrt{\log t}} \cdot (\log m)^{2\log\log m} \cdot n^{7/16} < n^{1/2}.$$

If $t = 2$ and $m \geq 2^{2048}$, then $|A/G| \leq b(A_1/G_1)a(A_1) < m \log m < n^{1/2} \log n$.

Let $t = 4$. Then $|A/G| \leq 6 \cdot b(A_1/G_1) \cdot (a(A_1))^2$. Using the notation d (for A_1) as in Theorem 5.30, by the argument above, we see that for $d \geq 2$ and $m \geq 2^{2048}$ we have $b(A_1/G_1) \cdot a(A_1) < 16 \cdot m^{1/2} \log m$. This gives $|A/G| < n^{1/2} \log n$ for $n \geq 2^{8192}$ under the assumption that $d \geq 2$. Thus assume that $d = 1$. Here we use the observation made in Lemma 5.21. Write $a(A_1) = |A_1|$ in the form $2^\ell r$ where r is odd and ℓ is an integer. Then we have $|A/G| \leq 6 \cdot 2^{2\ell} \cdot r$. From this the result follows if $|A_1| < 6m$. Otherwise, by Zsigmondy's theorem, $2^\ell < m$. Now $|A_1| < m \log_q m$ where q is the size of the field over which A_1 and A are defined. From this $2^{2\ell} \cdot r < m^2 \log_q m$ giving $|A/G| < n^{1/2} \log n$ unless $q = 2$. If $q = 2$, then $2^\ell \leq \log m$, and so $|A/G| < 6 \cdot m(\log m)^2 < n^{1/2} \log n$ for $m \geq 2^{2048}$.

Assume that A is a primitive permutation group which is not of affine type. In this case we use the notation, assumptions and the argument in the last two paragraphs of Section 5.7. However, we use Theorem 1.14. If A has two minimal normal subgroups, then we have $|A/G| = a(A/G)b(A/G) < n^{1/3} \cdot 4^{s/\sqrt{\log s}} \cdot (\log n)^{2\log\log n} < n^{1/2}$ for $n \geq 2^{8192}$, if $s \neq 1$, and also when $s = 1$. Finally assume that A has a unique minimal normal subgroup. We first claim that we may assume that $t \geq 512$. If $|\mathrm{Out}(L)| \leq \sqrt{m}$ and $t \leq 512$, then $|A/G| \leq n^{1/4} \cdot 16^{t/\sqrt{\log t}} < n^{1/2}$. If $|\mathrm{Out}(L)|$ is larger than $\sqrt{m}$, then L is one of the exceptions in Lemma 5.25 and so $t \geq 512$ by use of $n \geq 2^{14000}$. If $t \geq 512$, then, for $n \geq 2^{14000}$, we have $|A/G| \leq |\mathrm{Out}(L)|^{1/3t} \cdot 4^{t/\sqrt{\log t}} \cdot t^{\log t} < n^{1/2} \log n$.

This proves the second half of Theorem 1.8.

So far we showed Theorem 1.10 in case $|\operatorname{Out}(G)| = |A/G|$. In fact by the same calculation as in the previous paragraph we established Theorem 1.10 in case G is not of affine type. Thus assume that G is of affine type and $H^1(H,V) \neq 0$ where V is the minimal normal subgroup of G and $H \neq 1$ is a point stabilizer in G. Let us use the notation and assumptions of the proof of Theorem 5.38.

Let us first assume that $t > 1$ and $|\operatorname{Out}(G)| \leq (q-1)q^{[d/2]}|\operatorname{Out}(L)|^{t/2}b_t$ with $d \geq 2$ where $b_t \leq 4^{t/\sqrt{\log t}} \cdot t^{\log t}$, by Theorem 1.14 and $|\operatorname{Out}(L)| \leq 4(\log n)/t$, by Lemma 5.26. Here $n = q^{dt}$. Thus $|\operatorname{Out}(G)| < q^{[d/2]+1} \cdot (4(\log n)/t)^{t/2} \cdot 4^{t/\sqrt{\log t}} \cdot t^{\log t}$. If $d \geq 3$ or $t \geq 3$, then this is less than $n^{1/2}\log n$ for $n \geq 2^{14000}$. Finally, if $d = 2$ and $t = 2$, then $|\operatorname{Out}(G)| < n^{1/2}\log n$ since $|\operatorname{Out}(L)| \leq \log n$ by use of Dickson's theorem on subgroups L of $\mathrm{GL}_2(q)$.

Finally assume that in the proof of Theorem 5.38 we have $t = 1$, that is, H is an almost simple group with socle L. Then $|\operatorname{Out}(G)| \leq (q-1)|H^1(L,W)||\operatorname{Out}(L)|$ where W is a nontrivial irreducible L-module of size dividing n and defined over a field of size q. By Lemma 5.26, $|\operatorname{Out}(L)| \leq 4\log n$.

By the main result of [35], we have $|\operatorname{Out}(G)| \leq 4(q-1)|W|^{1/2}\log n$. Assume first that $|W| < n$. If $\dim W \geq 3$, then $|\operatorname{Out}(G)| \leq 4 \cdot n^{5/12}\log n$, which is less than $n^{1/2}\log n$ for $n \geq 2^{14000}$. If $\dim W = 2$, then $|\operatorname{Out}(G)| < n^{1/2}|\operatorname{Out}(L)|$ which is less than $n^{1/2}\log n$ by using Dickson's theorem once again. Thus assume that $|W| = n = q^d$. Furthermore, as observed in the proof of Theorem 5.38, we may assume that $d \geq 3$ (otherwise G is a member of the infinite sequence of examples in Theorem 1.9). Then, by [35], it is easy to see that $|\operatorname{Out}(G)| < 2 \cdot n^{3/4}$, at least for $n \geq 2^{14000}$. (In this previous bound the factor 2 comes from the fact that the full normalizer in $\mathrm{GL}_4(q)$ of A_6 acting on the fully deleted permutation module of dimension 4 in characteristic 3 over the field of size q has size $(q-1)|\mathrm{S}_6|$ since the dimension of the fixed point space of a 3-cycle in A_6 is different from the dimension of the fixed point space of an element in A_6 which is the product of two 3-cycles.) This proves the first statement of Theorem 1.10.

If L is an alternating group of degree at least 7, a sporadic simple group or the Tits group, then $\dim(H^1(L,W)) \leq (1/4)\dim(W)$ by [36, Corollary 3] and [35]. Thus in these cases we have $|\operatorname{Out}(G)| < 2 \cdot n^{1/2} \leq n^{1/2}\log n$. If L is a simple group of exceptional type, then $\dim(H^1(L,W)) \leq (1/3)\dim(W)$ by [52], thus if $d \geq 7$ then $|\operatorname{Out}(G)| < 4 \cdot n^{3/7}\log n < n^{1/2}\log n$ for $n \geq 2^{14000}$. Otherwise $d = 6$ and $L = \mathrm{G}_2(r)$ with r even or $4 \leq d \leq 6$ and L is a Suzuki group (by [62, Table 5.3.A] and [62, Table 5.4.C]). However in these cases $\dim(H^1(L,W)) \leq 1$, by [52], and so $|\operatorname{Out}(G)| < n^{1/2}\log n$. We may now assume that L is a classical simple group.

Since we are assuming that the dimension of the natural module for L is at least 7, we see from [62, Table 5.4.C] and [62, Table 5.3.A] that $d \geq 7$. By [52] we also have $\dim(H^1(L,W)) \leq (1/3)\dim(W)$. Thus $|\operatorname{Out}(G)| < 4 \cdot n^{3/7}\log n < n^{1/2}\log n$ for $n \geq 2^{14000}$.

This completes the proof of Theorem 1.10.

6 Fixed point spaces

In this last chapter of the thesis we consider fixed point spaces of elements of linear groups. Let G be a finite group, F a field, and V a finite dimensional FG-module such that G has no trivial composition factor on V. Then the arithmetic average dimension of the fixed point spaces of elements of G on V is at most $(1/p)\dim V$ where p is the smallest prime divisor of the order of G. This answers and generalizes a 1966 conjecture of Neumann [86] which also appeared in a paper of Neumann and Vaughan-Lee [87] and also as a problem in The Kourovka Notebook posted by Vaughan-Lee. Our result also generalizes a recent theorem of Isaacs, Keller, Meierfrankenfeld, and Moretó [57]. We also classify precisely when equality can occur. Various applications are given. For example, another conjecture of Neumann and Vaughan-Lee is proven and some results of Segal and Shalev [103] are improved and/or generalized concerning BFC groups.

6.1 The proofs

Our first lemma sharpens and generalizes [87, Theorem 6.1].

Lemma 6.1. *Let G be a finite group, F a field, and V a finite dimensional FG-module. Let N be an elementary Abelian normal subgroup of G such that $C_V(N) = 0$. Then* $\mathrm{avgdim}(Ng, V) \leq (1/p)\dim V$ *for every $g \in G$ where p is the smallest prime factor of the order of G.*

Proof. We may assume that F is algebraically closed. Let us consider a counterexample with $|G|$ and $\dim V$ minimal. It clearly suffices to assume that $G = \langle g, N\rangle$. We may assume that V is irreducible (since if we have the inequality on each composition factor of V we have it on V). Finally, we may assume that N acts faithfully on V. If N does not act homogeneously on V, then g transitively permutes the components in an orbit of size $t \geq p$ and so every element in Ng has a fixed point space of dimension at most $(1/t)\dim V \leq (1/p)\dim V$. So we may assume that the elementary Abelian group N acts homogeneously on V. This means that it acts as scalars on V. Thus $N \leq Z(G)$ and $G/Z(G)$ is cyclic. It follows that G is Abelian and so $\dim V = 1$. At most 1 element in the coset Ng is the identity and so $\mathrm{avgdim}(Ng, V) \leq (1/|N|)\dim V \leq (1/p)\dim V$. The result follows. □

We first need a result about generation of finite groups. This is an easy consequence of the proof of the main results of [8].

Theorem 6.2. *Let G be a finite group with a minimal normal subgroup $N = L_1 \times \ldots \times L_t$ for some positive integer t with $L_i \cong L$ for all i with $1 \leq i \leq t$ for a non-Abelian simple group L. Assume that $G/N = \langle xN \rangle$ for some $x \in G$. Then there exists an element $s \in L_1 \leq N$ such that $|\{g \in Nx : G = \langle g, s \rangle\}| > (1/2)|N|$.*

Proof. First suppose that $t = 1$. This is an immediate consequence of [8, Theorem 1.4] unless G is one of $\mathrm{Sp}_{2n}(2), n > 2$, S_{2m+1} or $L = \Omega_8^+(2)$ or A_6.

If $G = \mathrm{Sp}_{2n}(2), n > 2$, then the result follows by [8, Proposition 5.8]. If $G = S_{2m+1}$, then apply [8, Proposition 6.8].

Suppose that $L = A_6$. Note that the proper overgroups of s of order 5 in A_6 are two subgroups isomorphic to A_5 (of different conjugacy classes) and the normalizer of the subgroup generated by s. The result follows trivially from this observation.

Finally consider $L = \Omega_8^+(2)$. We take s to be an element of order 15. It follows by the discussion in [8, Section 4.1] that given G, there is an element of order 15 satisfying the result (although it is possible that the choice of s depends on which G occurs).

Now assume that $t > 1$. Write $x = (u_1, \ldots, u_t)\sigma$ where σ just cyclically permutes the coordinates of N (sending L_i to L_{i+1} for $i < t$) and $u_i \in \mathrm{Aut}(L_i)$. By conjugating by an element of the group $\mathrm{Aut}(L_1) \times \ldots \times \mathrm{Aut}(L_t)$ we may assume that $u_2 = \ldots = u_t = 1$ (we do not need to do this but it just makes the computations easier).

Let $f : Nx \to \mathrm{Aut}(L_1)$ be the map sending wx to the projection of $(wx)^t$ in $\mathrm{Aut}(L_1)$. Write $w = (w_1, \ldots, w_t)$ with $w_i \in L_i$. Then $f(wx) = w_t w_{t-1} \ldots w_1 u_1$ is in $L_1 u_1$. Moreover, we see that every fiber of f has the same size. By the case $t = 1$, we know that the probability that $\langle f(wx), s \rangle = \langle L_1, u_1 \rangle$ is greater than $1/2$.

We claim that if $L_1 \leq \langle f(wx), s \rangle$, then $G = \langle wx, s \rangle$. The claim then implies the result. So assume that $L_1 \leq \langle (f(wx), s \rangle$ and set $H = \langle wx, s \rangle$. Let $M \leq N$ be the normal closure of s in $J := \langle (wx)^t, s \rangle$. This projects onto L_1 by assumption, but is also contained in L_1, whence $M = L_1$. So $L_1 \leq H$. Since any element of Nx acts transitively on the L_i, it follows that $N \leq H$ and so $G = H$. □

The next result we need is Scott's Lemma [101].

Lemma 6.3 (Scott's Lemma)**.** *Let G be a subgroup of $\mathrm{GL}_(V))$ with V a finite dimensional vector space. Suppose that $G = \langle g_1, \ldots, g_r \rangle$ with $g_1 \cdots g_r = 1$. Then*

$$\sum_{i=1}^{r} \dim[g_i, V] \geq \dim V + \dim[G, V] - \dim C_V(G).$$

We will apply this in the case $r = 3$. Noting that $\dim V = \dim[x, V] + \dim C_V(x)$ for any x, we can restate this as:

$$\sum_{i=1}^{3} \dim C_V(g_i) \leq \dim V + \dim C_V(G) + \dim V/[G,V].$$

Theorem 6.4. *Let G be a finite group. Assume that G has a normal subgroup E that is a central product of quasisimple groups. Let V be a finite dimensional FG-module for some field F such that E has no trivial composition factor on V. If $g \in G$, then* $\operatorname{avgdim}(gE, V) \leq (1/2)\dim V$.

Proof. Let us consider a counterexample with $|G|$ and $\dim V$ minimal. There is no loss of generality in assuming that F is algebraically closed, $G = \langle E, g\rangle$, and then assuming that V is an irreducible (hence absolutely irreducible) and faithful FG-module. If $Z(E) \neq 1$, the result follows by Lemma 6.1 (by taking $N = Z(E)$ and noting that $Z(E)$ is completely reducible on V with $C_V(Z(E)) = 0$ (since V is a faithful FG-module)). So we may assume that E is a direct product of non-Abelian simple groups. If V is not a homogeneous FE-module, then g transitively permutes the homogeneous components and so any element in gE has fixed point space of dimension at most $(1/2)\dim V$. So we may assume that V is a homogeneous FE-module. Thus $E = L_1 \times \ldots \times L_m$ with the L_i's non-Abelian simple groups. So V is a direct sum of say t copies of $V_1 \otimes \ldots \otimes V_m$ where V_i is an irreducible nontrivial FL_i-module. (Since G/E is cyclic and V is irreducible, it follows that $t = 1$ (by Clifford theory) but we will not use this fact.) We may replace E by a minimal normal subgroup of G contained in E (the hypothesis on the minimal normal subgroup will hold by Clifford's theorem) and so assume that g transitively permutes the isomorphic subgroups $L_1, \ldots, L_m$.

Let $s \in L_1 \leq E$ be chosen so that $Y := \{y \in gE : \langle y, s\rangle = G\}$ has size larger than $(1/2)|E|$. Such an element exists by Theorem 6.2. Set $c = \dim C_V(s)$. If $y \in Y$ then, by Lemma 6.3 (applied to the triple $(y, s, (ys)^{-1})$), we have

$$c + \dim C_V(y) + \dim C_V(ys) \leq \dim V.$$

For any $y \in Y' := gE \setminus Y$, we at least have

$$\dim C_V(y) + \dim C_V(ys) \leq \dim V + c.$$

Thus,

$$2\sum_{y \in gE} \dim C_V(y) = \sum_{y \in gE} \Big(\dim C_V(y) + \dim C_V(ys)\Big)$$

is at most

$$|Y|(\dim V - c) + |Y'|(\dim V + c) < |E| \dim V.$$

This gives $\operatorname{avgdim}(gE) \leq (1/2)\dim V$ as required. □

We now prove Theorem 1.16. As usual, we may assume that F is algebraically closed, V is an irreducible FG-module, and N acts faithfully on V. Let A be a minimal normal

subgroup of G contained in N. Since V is a faithful completely reducible FN-module, A has no trivial composition factor on V. Now apply Lemma 6.1 and Theorem 6.4 to conclude that $\operatorname{avgdim}(Ag, V) \leq (1/p)\dim V$ where p is the smallest prime divisor of $|G|$. Since Ng is the union of cosets of A, the result follows.

We next consider fields of characteristic 0.

Lemma 6.5. *Let G be a finite group, $\mathbb{C}$ the field of complex numbers, and V a finite dimensional $\mathbb{C}G$-module. For an element $g \in G$ and a root of unity $a \in \mathbb{C}$ let a_g denote the multiplicity of a as an eigenvalue of g. Then $\sum_{g\in G} a_g = \sum_{g\in G} b_g$ as long as a and b have the same order in $\mathbb{C}^*$.*

Proof. Let a and b be roots of unity of the same order. Let m be the exponent of G with μ a primitive m-th root of unity. Let σ be an element of the automorphism group of the field $\mathbb{Q}(\mu)$ with $\sigma(a) = b$. Let e be a positive integer such that $\sigma(\mu) = \mu^e$. Then e is relatively prime to m and hence also to $|G|$. Thus, the map $G \to G$ with $g \mapsto g^e$ is a bijection on G and so $\sum_{g\in G} b_g = \sum_{g\in G} b_{g^e} = \sum_{g\in G} a_g$, whence the result. □

The Möbius function $\mu(n)$ of a positive integer n is 0 if n is not square free and is $(-1)^m$ if n is square free and the number of (distinct) prime divisors of n is m. For a positive integer n let $s(n)$ be the sum of primitive nth roots of unity (in $\mathbb{C}$). We recall the following well known result.

Lemma 6.6. *For a positive integer n we have $s(n) = \mu(n)$.*

Proposition 6.7. *Let G be a finite group, let F be a field such that $|G|$ is invertible in F, let V be a finite dimensional FG-module with no trivial FG-composition factor, and let p be the smallest prime divisor of the order of $G/C_G(V)$. Then* $\operatorname{avgdim}(G, V) \leq (1/p)\dim V$ *with equality if and only if the exponent of $G/C_G(V)$ is p.*

Proof. By $\operatorname{avgdim}(G, V) = \operatorname{avgdim}(G/C_G(V), V)$ we see that it is sufficient to assume that $C_G(V) = 1$. Since $|G|$ is invertible, there is no loss in assuming that $\operatorname{char}(F) = 0$.

Let χ be the character of the FG-module V. Then, by hypothesis, $\langle 1_G, \chi\rangle = 0$, that is, $\sum_{g\in G} \chi(g) = 0$. Let $n_1, n_2, \ldots, n_m$ be the possible distinct orders of elements of G with $n_1 = 1$ and $n_2 = p$. Since $\chi(g)$ is the sum of the eigenvalues of the matrix of g acting on V, Lemma 6.5 shows that there exist positive integers $k_1, k_2, \ldots, k_m$ with

$$0 = \sum_{g\in G} \chi(g) = \sum_{i=1}^{m} k_i s(n_i).$$

Letting $\varphi(n)$ denote the Euler function of n, we may write the previous equation as

$$0 = \sum_{i=1}^{m} (k_i\varphi(n_i))(s(n_i)/\varphi(n_i)) \geq k_1 - (|G|\dim V - k_1)(1/(p-1))$$

since $s(n_i)/\varphi(n_i) > (-1)/(p-1)$ for all i with $2 < i \leq m$. This gives $k_1 \leq (1/p)|G|\dim V$ with equality if and only if the exponent of G is p. □

Now we prove Theorem 1.17. By Proposition 6.7, we know that equality always occurs when $G/C_G(V)$ is a group of exponent p. Hence, it remains to show that whenever $\operatorname{avgdim}(G,V) = (1/p)\dim V$, then $G/C_G(V)$ is a group of exponent p.

Choose a minimal counterexample to this latter statement with respect to $|G|$ and $\dim V$. As before, we may assume that $C_G(V) = 1$. By Proposition 6.7, we may also assume that $r := \operatorname{char}(F)$ divides the order of G.

We claim that V is an irreducible FG-module. For suppose not and W is a non-trivial proper submodule of V. By the minimality of $\dim V$ and by the fact that

$$\operatorname{avgdim}(G,V) \leq \operatorname{avgdim}(G,W) + \operatorname{avgdim}(G,V/W) \leq (1/p)\dim W + (1/p)\dim V/W,$$

we have that $G/C_G(W)$ and $G/C_G(V/W)$ are groups of exponent p. Let N be the normal subgroup of G which acts trivially on both W and V/W. Note that N is an r-group. So $G = PN$ where P is a Sylow p-subgroup of G of exponent p. Since G is a counterexample to the above statement, $N \neq 1$. For any element $g \in P$ we have $\operatorname{avgdim}(gN,V) \leq \dim C_V(g)$. (This can be seen by observing that some power of an arbitrary element gn is conjugate to g. Moreover, $\operatorname{avgdim}(N,V) \leq (1/r)\dim V < (1/p)\dim V$. Thus,

$$\operatorname{avgdim}(G,V) = |P|^{-1}\sum_{g\in P}\operatorname{avgdim}(gN,V) < \operatorname{avgdim}(P,N) = (1/p)\dim V,$$

a contradiction.

So we may assume that V is an irreducible FG-module. Let M be a minimal normal subgroup of G. By Theorem 1.16, we have $\operatorname{avgdim}(Mg,V) \leq (1/p)\dim V$ for each coset Mg of M in G, so $\operatorname{avgdim}(Mg,V) = (1/p)\dim V$ must hold for each coset Mg of M in G. In particular, by the minimality of G, the group M is an elementary Abelian p-group. Since G is not a p-group, we can choose $g \in G$ of prime order $s > p$ such that $G = \langle g, M\rangle$ (by the minimality of G). (The module V remains an irreducible FG-module (by the minimality of $\dim V$) and $C_G(V) = 1$ continues to hold since both M and g acts faithfully on V.) If M is central in G, then G is Abelian and $\dim V = 1$. In this case $\operatorname{avgdim}(G,V) = (1/|G|)\dim V < (1/p)\dim V$, a contradiction. If M is not central, then g permutes the eigenspaces of M in an orbit of size $s > p$ (for some divisor t of s) and so $\operatorname{avgdim}(Mg,V) \leq (1/t)\dim V < (1/p)\dim V$, which is again a contradiction. This proves Theorem 1.17.

Let us next prove the first statement of Corollary 1.19. By making the assumptions of the proof of [57, Corollary D], it is sufficient to show that the number of $g \in G$ such that $\dim C_V(g) \leq (1/2)\dim V$ is at least

$$\frac{2|G|}{1+\log_p|G|_p} \leq \frac{2|G|}{2+\dim V}.$$

But this is clear by Theorem 1.16 noting that $\dim V$ is even.

Let us prove the second statement of Corollary 1.19. Use the notations and assumptions of the last part of the proof of [57, Corollary D]. Let H be a Hall p'-subgroup of G. Since V is a completely reducible G-module with $C_V(G) = 0$, the vector space V is also a completely reducible H-module with $C_V(H) = 0$. Hence applying Corollary 1.18 to the H-module V we get that there exists $g \in H$ with $\dim C_V(g) < (1/2)\dim V$. So the last displayed inequality of the proof of [57, Corollary D] becomes

$$\frac{|\mathrm{cl}_G(g)|_p}{p} \geq \chi(1)^{1/3}$$

since $\dim V$ is even. From this we get that $p^3\chi(1) \leq |\mathrm{cl}_G(g)|_p{}^3$.

In the next two paragraphs we prove Theorem 1.20.

Note that Y centralizes M and so there is no loss in working in G/Y and assuming that $X = M$ is a minimal normal subgroup of G. Set $H = \langle M, g\rangle$ and so assume that g acts transitively on the direct factors of M.

We compute the arithmetic mean of the positive integers $|C_M(x)|$ for $x \in gM$. All elements in a given M-conjugacy class in gM have the same centralizer size. If $h \in gM$, then the M-conjugacy class of h has $|M : C_M(h)|$ elements. Thus, we see that the arithmetic mean is precisely the number of M-conjugacy classes in gM. By [25, Lemma 2.1], this is at most $k(M)$, the number of conjugacy classes in M. By [25, Proposition 5.3], this is at most $|M|^{.41}$. Since the geometric mean is bounded above by the arithmetic mean, the result follows.

We end this chapter by proving Theorem 1.21.

Let us fix a chief series for a finite group G. Let $\mathcal{N}$ be the set of non-central chief factors of this series. Let p be the smallest prime factor of the order of $G/F(G)$. If $N \in \mathcal{N}$ is Abelian then, by Theorem 1.16 (noting that $F(G)$ acts trivially on N), we have $\mathrm{geom}(G, N) \leq |N|^{1/p}$. If $N \in \mathcal{N}$ is non-Abelian then, by Theorem 1.20 and the Feit-Thompson Odd Order Theorem [22], we again have $\mathrm{geom}(G, N) \leq |N|^{1/p}$. Notice also that for any $g \in G$ we have the inequality $|C_G(g)| \leq \mathrm{ccf}(G)\prod_{N\in\mathcal{N}} |C_N(g)|$. From these observations Theorem 1.21 already follows since

$$\mathrm{geom}(G,G) = \Big(\prod_{g\in G}|C_G(g)|\Big)^{1/|G|} \leq \mathrm{ccf}(G)\Big(\prod_{g\in G}\prod_{N\in\mathcal{N}}|C_N(g)|\Big)^{1/|G|} =$$

$$= \mathrm{ccf}(G)\Big(\prod_{N\in\mathcal{N}}\prod_{g\in G}|C_N(g)|\Big)^{1/|G|} = \mathrm{ccf}(G)\Big(\prod_{N\in\mathcal{N}}\mathrm{geom}(G,N)\Big) \leq$$

$$\leq \mathrm{ccf}(G)\Big(\prod_{N\in\mathcal{N}}|N|^{1/p}\Big) = \mathrm{ccf}(G)\cdot(\mathrm{ncf}(G))^{1/p}.$$

Bibliography

[1] M. Aschbacher, Finite group theory. Second edition. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 2000.

[2] M. Aschbacher and R. M. Guralnick, Some applications of the first cohomology group. *J. Algebra* **90** (1984), 446–460.

[3] M. Aschbacher and R. M. Guralnick, Abelian quotients of primitive groups. *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

[4] B. Baumeister, A. Maróti, H. P. Tong-Viet, Finite groups have more conjugacy classes. *Forum Math.* **29** (2017), no. 2, 259–275.

[5] R. Brauer, On groups whose order contains a prime number to the first power. I. *Amer. J. Math.* **64**, (1942), 401–420.

[6] R. Brauer, Representations of finite groups. 1963 Lectures on Modern Mathematics, Vol. I pp. 133–175 Wiley, New York.

[7] R. Brauer and W. Feit, On the number of irreducible characters of finite groups in a given block, Proc. Natl. Acad. Sci. USA **45** (1959) 361–365.

[8] T. Breuer, R. M. Guralnick, W. M. Kantor, Probabilistic generation of finite simple groups, II. *J. Algebra* Vol. 320. **2**, (2008), 443–494.

[9] M. Cartwright, The order of the derived group of a BFC group. *J. London Math. Soc.* **30** (1984), 227–243.

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, Wilson, R. A. Atlas of finite groups. *Oxford University Press*, Eynsham, (1985).

[11] J. P. Cossey, Z. Halasi, A. Maróti, H. N. Nguyen, On a conjecture of Gluck. *Math. Z.* **279** (2015), no. 3-4, 1067–1080.

[12] J. D. Dixon, The Fitting subgroup of a linear solvable group. *J. Austral. Math. Soc.* **7** (1967), 417–424.

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

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

[15] S. Dolfi, Intersections of odd order Hall subgroups. *Bull. London Math. Soc.* **37** (2005) 61–66.

[16] S. Dolfi, Large orbits in coprime actions of solvable groups. *Trans. Amer. Math. Soc.* **360** (2008), 135–152.

[17] S. Dolfi and E. Jabara, Large character degrees of solvable groups with Abelian Sylow 2-subgroups. *J. Algebra* **313** (2007), 687–694.

[18] Y. A. Drozd and V. V. Kirichenko, Finite-dimensional algebras. Springer-Verlag, Berlin, 1994.

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

[20] P. Erdős and P. Turán, On some problems of a statistical group-theory. IV. *Acta Math. Acad. Sci. Hungar* **19** (1968), 413–435.

[21] J. A. Ernest, Central intertwining numbers for representations of finite groups. *Trans. Amer. Math. Soc.* **99** (1961), 499–508.

[22] W. Feit and J. G. Thompson, Solvability of groups of odd order. *Pacific J. Math.* **13** (1963), 775-1029.

[23] G. A. Fernández-Alcober and M. Morigi, Outer commutator words are uniformly concise. *J. Lond. Math. Soc.* (2) **82** (2010), no. 3, 581–595.

[24] D. A. Foulser, Solvable primitive permutation groups of low rank. *Trans. Amer. Math. Soc.* **143** (1969), 1–54.

[25] J. Fulman and R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023–3070.

[26] P. X. Gallagher, The number of conjugacy classes in a finite group. *Math. Z.* **118** (1970) 175–179.

[27] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2005, `(http://www.gap-system.org)`.

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

[29] D. Gluck, Trivial set-stabilizers in finite permutation groups. *Canad. J. Math.* **35** (1983), no. 1, 59–67.

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

[31] D. Gluck, K. Magaard, U. Riese, P. Schmid, The solution of the $k(GV)$-problem. *J. Algebra* **279** (2004), no. 2, 694–719.

[32] D. P. M. Goodwin, Regular orbits of linear groups with an application to the $k(GV)$-problem, I,II. *J. Algebra* **227** (2000), 395–432 and 433–473.

[33] R. M. Guralnick, Generation of simple groups. *J. Algebra* **103** (1986), 381–401.

[34] R. M. Guralnick, Cyclic quotients of transitive groups. *J. Algebra* **234** (2000), 507–532.

[35] R. M. Guralnick and C. Hoffman, The first cohomology group and generation of simple groups, in Proc. Conf. Groups and Geometries (Siena, 1996), Trends in Mathematics, Birkhäuser, Basel 1998, pp. 81–89.

[36] R. M. Guralnick and W. Kimmerle, On the cohomology of alternating and symmetric groups and decomposition of relation modules. *J. Pure Appl. Algebra* **69** (1990), no. 2, 135–140.

[37] R. M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.* **25** (2012), no. 1, 77–121.

[38] R. M. Guralnick and A. Maróti, On the non-coprime $k(GV)$-problem. *J. Algebra* **385** (2013), 80–101.

[39] R. M. Guralnick and A. Maróti, Average dimension of fixed point spaces with applications. *Adv. Math.* **226** (2011), no. 1, 298–308.

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

[41] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups. *J. Algebra* Vol. 300, No. 2, (2006), 509–528.

[42] R. M. Guralnick and P. H. Tiep, The non-coprime k(GV) problem. *J. Algebra* **293** (2005), no. 1, 185–242.

[43] Z. Halasi and A. Maróti, The minimal base size for a p-solvable linear group. *Proc. Amer. Math. Soc.* **144** (2016), no. 8, 3231–3242.

[44] Z. Halasi and P. P. Pálfy, The number of conjugacy classes in pattern groups is not a polynomial function. *J. Group Theory* **14** (2011), no. 6, 841–854.

[45] Z. Halasi and K. Podoski, Every coprime linear group admits a base of size two. *Trans. Amer. Math. Soc.* **368** (2016), no. 8, 5857–5887.

[46] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc (2)* **17** (1918), 75–115.

[47] L. Héthelyi, E. Horváth, T. M. Keller, A. Maróti, Groups with few conjugacy classes. *Proc. Edinb. Math. Soc.* (2) **54** (2011), no. 2, 423–430.

[48] L. Héthelyi and B. Külshammer, On the number of conjugacy classes of a finite solvable group. *Bull. London Math. Soc.* **32** (2000), no. 6, 668–672.

[49] L. Héthelyi and B. Külshammer, On the number of conjugacy classes of a finite solvable group. II. *J. Algebra* **270** (2003), no. 2, 660–669.

[50] G. Hiss and G. Malle, Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.* **4** (2001), 22–63.

[51] G. Hiss and G. Malle, Corrigenda: "Low-dimensional representations of quasi-simple groups" [*LMS J. Comput. Math.* **4** (2001), 22–63]. *LMS J. Comput. Math.* **5** (2002), 95–126.

[52] C. Hoffman, On the cohomology of the finite Chevalley groups. *J. Algebra* **226** (2000), no. 2, 649–689.

[53] A. Hulpke, Constructing transitive permutation groups. *J. Symbolic Comput.* **39** (2005), no. 1, 1–30.

[54] B. Huppert, Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.

[55] B. Huppert and N. Blackburn, Finite groups. III. Grundlehren der Mathematischen Wissenschaften, 243. Springer-Verlag, Berlin-New York, 1982.

[56] I. M. Isaacs, Character Theory of Finite Groups. Dover Publications, New York, 1994.

[57] I. M. Isaacs, T. M. Keller, U. Meierfrankenfeld, A. Moretó, Fixed point spaces, primitive character degrees and conjugacy class sizes. *Proc. Am. Math. Soc.* **134** 11, (2006), 3123–3130.

[58] I. M. Isaacs, G. Malle, G. Navarro, A reduction theorem for the McKay conjecture. *Invent. Math.* **170** (2007), 33–101.

[59] C. Jansen, K. Lux, R. Parker and R. Wilson, An Atlas of Brauer characters, Oxford Univ. Press, Oxford 1995.

[60] T. M. Keller, Lower bounds for the number of conjugacy classes of finite groups. *Math. Proc. Cambridge Philos. Soc.* **147** (2009), no. 3, 567–577.

[61] T. M. Keller, Finite groups have even more conjugacy classes. *Israel J. Math.* **181** (2011), 433–444.

[62] P. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[63] L. G. Kovács and C. R. Leedham-Green, Some normally monomial p-groups of maximal class and large derived length. *Quart. J. Math. Oxford Ser.* (2) **37** (1986), no. 145, 49–54.

[64] L. G. Kovács and M. F. Newman, Generating transitive permutation groups. *Quart. J. Math. Oxford* (2), **39** (1988), 361–372.

[65] L. G. Kovács and G. R. Robinson, On the number of conjugacy classes of a finite group. *J. Algebra* **160** (1993), no. 2, 441–460.

[66] The Kourovka Notebook. Unsolved problems in group theory. Sixteenth augmented edition, 2006. Edited by V. D. Mazurov and E. I. Khukhro.

[67] C. Köhler and H. Pahlings, Regular orbits and the $k(GV)$-problem. Groups and computation, III, (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ. 8, de Gruyter, Berlin (2001), 209–228.

[68] Külshammer, B. Landau's theorem for p-blocks of p-solvable groups. *J. Reine Angew. Math.* **404** (1990), 189-191.

[69] Külshammer, B.; Robinson, G. R. Alperin-McKay implies Brauer's problem 21. *J. Algebra* **180** (1996), no. 1, 208-210.

[70] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante. *Math. Ann.* **56** (1903), no. 4, 671–676.

[71] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep, The Ore conjecture. *J. Eur. Math. Soc.* (JEMS) **12** (2010), no. 4, 939–1008.

[72] M. W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), no. 2, 538–562.

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

[74] A. Lucchini, F. Menegazzo and M. Morigi, Asymptotic results for transitive permutation groups. *Bull. Lond. Math. Soc.* **32** (2000), 191–195.

[75] A. Lucchini, F. Menegazzo and M. Morigi, On the number of generators and composition length of finite linear groups. *J. Algebra* **243** (2001), 427–447.

[76] I. D. Macdonald, Some explicit bounds in groups with finite derived groups. *Proc. London Math. Soc.* (3) **11** (1961), 23–56.

[77] G. Malle, Fast-einfache Gruppen mit langen Bahnen in absolut irreduzibler Operation. *J. Algebra* **300** (2006), no. 2, 655–672.

[78] G. Malle and A. Maróti, On the number of p'-degree characters in a finite group. *Int. Math. Res. Not. IMRN* Vol. **2016** No. 20 (2016), 6118–6132.

[79] G. Malle and B. Späth, Characters of odd degree. *Ann. of Math.* (2) **184** (2016), no. 3, 869–908.

[80] A. Maróti, On the orders of primitive groups. *J. Algebra* **258** (2002), no. 2, 631–640.

[81] A. Maróti, On elementary lower bounds for the partition function. *Integers* **3** (2003).

[82] A. Maróti, Bounding the number of conjugacy classes of a permutation group. *J. Group Theory* **8** (2005), no. 3, 273–289.

[83] A. Maróti, A lower bound for the number of conjugacy classes of a finite group. *Adv. Math.* **290** (2016), 1062–1078.

[84] H. Nagao, On a conjecture of Brauer for p-solvable groups. *J. Math. Osaka City*

Univ. **13** (1962) 35–38.

[85] B. H. Neumann, Groups covered by permutable subsets. *J. London Math. Soc.* **29** (1954), 236–248.

[86] Peter M. Neumann, A study of some finite permutation groups. DPhil thesis, Oxford, 1966.

[87] Peter M. Neumann and M. R. Vaughan-Lee, An essay on BFC groups. *Proc. London Math. Soc.* (3) **35** (1977), 213–237.

[88] M. Newman, A bound for the number of conjugacy classes in a group. *J. London Math. Soc.* **43** (1968), 108–110.

[89] P. P. Pálfy, A polynomial bound for the orders of primitive solvable groups. *J. Algebra* **77** (1982), 127–137.

[90] P. P. Pálfy, Bounds for linear groups of odd order. Proceedings of the Second International Group Theory Conference (Bressanone, 1989). Rend. Circ. Mat. Palermo (2) Suppl. No. 23 (1990), 253–263.

[91] P. P. Pálfy and L. Pyber, Small groups of automorphisms. *Bull. London Math. Soc.* **30** (1998), no. 4, 386–390.

[92] C. E. Praeger and J. Saxl, On the orders of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980), no. 4, 303–307.

[93] L. Pyber. The number of pairwise non-commuting elements and the index of the centre in a finite group. *J. London Math. Soc. (2)* **35**, (1987), no. 2, 287–295.

[94] L. Pyber, Finite groups have many conjugacy classes. *J. London Math. Soc.* (2) **46** (1992), no. 2, 239–249.

[95] L. Pyber, Asymptotic results for permutation groups, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 11 (ed. L. Finkelstein and W. M. Kantor) Amer. Math. Soc. Providence RI 1993, pp. 197–219.

[96] H. Rademacher, On the partition function $p(n)$. *Proc. London Math. Soc. (2)* **43** (1937), 241–254.

[97] U. Riese and P. Schmid, Real vectors for linear groups and the k(GV)-problem. *J. Algebra* **267** (2003), 725–755.

[98] G. R. Robinson and J. G. Thompson, On Brauer's $k(B)$-problem. *J. Algebra* **184** (1996), no. 3, 1143–1160.

[99] P. Schmid, Signed permutation modules, Singer cycles and class numbers. *J. Group Theory* **14** (2011), no. 2, 175–199.

[100] P. Schmid, The solution of the $k(GV)$ problem. ICP Advanced Texts in Mathematics, 4. Imperial College Press, London, 2007.

[101] L. Scott, Matrices and cohomology. *Ann. of Math.* **105** (1977), 473–492.

[102] S. M. Seager, The rank of a finite primitive solvable permutation group. *J. Algebra* **105** (1987), no. 2, 389–394.

[103] D. Segal and A. Shalev, On groups with bounded conjugacy classes. *Quart. J. Math. Oxford* **50** (1999), 505–516.

[104] Á. Seress, The minimal base size of primitive solvable permutation groups. *J. London Math. Soc.* **53** (1996) 243–255.

[105] D. A. Suprunenko, Matrix groups. Translations of Mathematical Monographs, Vol. 45. American Mathematical Society, Providence, R.I., 1976.

[106] M. Suzuki, Group Theory II, Springer-Verlag, New York, 1986.

[107] G. M. Tracey, Minimal generation of transitive permutation groups. ArXiv: 1504.07506.

[108] P. Turán, An extremal problem in graph theory. *Mat. Fiz. Lapok* **48**, (1941), 436–452.

[109] J. V. Uspensky, Asymptotic formulae for numerical functions which occur in the theory of partitions [Russian]. *Bull. Acad. Sci. URSS (6)* **14** (1920), 199–218.

[110] M. R. Vaughan-Lee, Breadth and commutator subgroups of p-groups. *J. Algebra* **32** (1974) 278–285.

[111] E. P. Vdovin, Regular orbits of solvable linear p'-groups. *Sib. Élektron. Mat. Izv.* **4** (2007), 345–360.

[112] A. Vera López and J. Vera López, Classification of finite groups according to the number of conjugacy classes I and II. *Israel J. Math.* **51** (1985), no. 4, 305–338 and **56** (1986), no. 2, 188–221.

[113] A. Vera López and J. Sangroniz, The finite groups with thirteen and fourteen conjugacy classes. *Math. Nachr.* **280** (2007), no. 5-6, 676–694.

[114] J. Wiegold, Groups with boundedly finite classes of conjugate elements. *Proc. Roy. Soc. London Ser. A* **238** (1956), 389–401.

[115] T. R. Wolf, Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982), 1097–1111.

[116] T. R. Wolf, Large orbits of supersolvable linear groups. *J. Algebra* **215** (1999), 235–247.

[117] Y. Yang, Large character degrees of solvable $3'$-groups. *Proc. Amer. Math. Soc.* **139** (2011), 3171–3173.